FTOS Command Line Interface Reference

Version 7.5.1.0 August 2007

FORCE10™

Copyright 2007 Force10 Networks®

All rights reserved. Printed in the USA. August 2007.

Force10 Networks® reserves the right to change, modify, revise this publication without notice.

Trademarks

Force10 Networks® and E-Series® are registered trademarks of Force10 Networks, Inc. Force10, the Force10 logo, E1200, E600, E600i, E300, C300, EtherScale, TeraScale, and FTOS are trademarks of Force10 Networks, Inc. All other brand and product names are registered trademarks or trademarks of their respective holders.

Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, Force10 Networks reserves the right to make changes to products described in this document without notice. Force10 Networks does not assume any liability that may occur due to the use or application of the product(s) described herein.

USA Federal Communications Commission (FCC) Statement

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC rules. These limits are designated to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy. If it is not installed and used in accordance to the instructions, it may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to take whatever measures necessary to correct the interference at their own expense.

Properly shielded and grounded cables and connectors must be used in order to meet FCC emission limits. Force10 Networks is not responsible for any radio or television interference caused by using other than recommended cables and connectors or by unauthorized changes or modifications in the equipment. Unauthorized changes or modification could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Canadian Department of Communication Statement

The digital apparatus does not exceed the Class A limits for radio noise emissions from digital apparatus set out in the Radio Interference Regulations of the Canadian Department of Communications.

Attention: Le present appareil numerique n' emet pas de perturbations radioelectriques depassant les normes applicables aux appareils numeriques de la Class A prescrites dans le Reglement sur les interferences radioelectriques etabli par le ministere des Communications du Canada.

European Union EMC Directive Conformance Statement

This product is in conformity with the protection requirements of EU Council Directive 89/336/EEC on the approximation of the laws of the Member States relating to electromagnetic compatibility. Force 10 Networks can not accept responsibility for any failure to satisfy the protection requirements resulting from a non-recommended modification of this product, including the fitting of non-Force10 option cards.

This product has been tested and found to comply with the limits for Class A Information Technology Equipment according to CISPR 22/ European Standard EN 55022. The limits for Class A equipment were derived for commercial and industrial environments to provide reasonable protection against interference with licensed communication equipment.

Warning: This device is a Class A product. In a domestic environment, this device can cause radio interference, in which case, the user may be required to take appropriate measures.

VCCI Compliance for Class A Equipment (Japan)

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

This is Class A product based on the standard of the Voluntary Control Council For Interference by Information Technology Equipment (VCCI). If this equipment is used in a domestic environment, radio disturbance may arise. When such trouble occurs, the user may be required to take corrective actions.\

Danger: AC Power cords are for use with Force10 Networks equipment only, do not use Force10 Networks AC Power cords with any unauthorized hardware.

本製品に同梱いたしております電源コードセットは、本製品専用です。本電源コードセットは、本製品以外の製品ならびに他の用途でご使用いただくことは出来ません。製品本体には同梱された電源コードセットを使用し、他製品の電源コードセットを使用しないで下さい。

Feedback on Documentation?
Send email to techpubs@force10networks.com

New Features

Listed below are the new features for FTOS version 7.5.1.0

High Availability

C-Series

- Added robust Debug chapters for both E-Series and C-series—see Chapter 6, E-Series Debugging and Diagnostics, on page 219 and Chapter 5, C-Series Diagnostics and Debugging, on page 183

E-Series

- Added robust Debug chapters for both E-Series and C-series—see Chapter 6, E-Series Debugging and Diagnostics, on page 219 and Chapter 5, C-Series Diagnostics and Debugging, on page 183
- Guaranteed IPC feature—see show processes ipc on page 232 and deprecated the show processes communication command and replaced it with show processes ipc flow-control on page 234

Layer 2

C-Series

- Added support for LACP Slow Mode—see lacp long-timeout on page 523
- Added support for QoS—see Per-Port QoS on page 1219 and Policy-Based QoS on page 1227
- Added Native VLAN support—see portmode hybrid on page 482

E-Series

- Added support to clear the statistics counters in the Resilient Ring Protocol (FRRP)—see clear frrp on page 576
- Added support for LACP Slow Mode—see lacp long-timeout on page 523
- MAC Learning Limit Enhancements—see the mac learning-limit commands beginning on page 560
- Added PBR Exception and Optimization—see the permit on page 771.

Layer 3

C-Series

- Added support for Load Balancing—see hash-algorithm ecmp on page 728 and load-balance (C-Series) on page 742
- Added support for RFC-2328-based Flooding—see the command flood-2328 on page 872

E-Series

- Added support for RFC-2328-based Flooding—see the command flood-2328 on page 872
- Added support for IPv6 IS-IS protocol—see Chapter 41, IPv6 IS-IS Protocol, on page 985.
- Added IPv6 support to SSH—see ssh on page 433
- Added IPv6 support to the telnet command—see telnet on page 160
- Enhanced IS-IS to use BFD services—see bfd all-neighbors (IS-IS) on page 930 and isis bfd all-neighbors on page 935
- IPv6 LSP and SPF Throttling enhancement—see lsp-gen-interval on page 1007 and spf-interval on page 1019
- IPv4 LSP and SPF Throttling enhancement—see lsp-gen-interval on page 964 and spf-interval on page 983
- BGP debug enhancements—see the BGP debug commands in Chapter 42, BGP, on page 1021 and Chapter 43, IPv6 BGP, on page 1127

Management

C-Series

- Added expaned configuration option to AAA Authorization—see aaa authorization on page 394
- Added a interface status commands—see show interfaces status on page 493
- Added a media option to the show inventory command—see show inventory on page 139
- Provide an option to use SSH version 1 or version 2—see ssh on page 433

E-Series

- Added expaned configuration option to AAA Authorization—see aaa authorization on page 394
- Added a interface status commands—see show interfaces status on page 493
- Added a media option to the show inventory command—see show inventory on page 139
- Provide an option to use SSH version 1 or version 2—see ssh on page 433
- SNMP Infrastructure change—see the Important Points to Remember on page 323

Multicast

E-Series

- Added support for IGMPv3—see IGMP Commands on page 1284
- Added support for PIM-SSM—see PIM-SSM on page 1330
- Added Mtrace Originator—see mtrace on page 1281

QoS

E-Series

- Support for WFQ between unicast and multicast—see queue egress on page 1238
- Added support for WRED on Storm Control—see Chapter 16, Storm Control, on page 447
- Added support for Flow Based DSCP Marking—see Chapter 44, Quality of Service, on page 1219

Contents

New Features **3**

Preface
About this Guide **63**

Objectives 63
Audience 63
Conventions 63
Information Symbols 64
Related Documents 65

Chapter 1
CLI Basics **67**

Accessing the Command Line 67
Multiple Configuration Users 68
Navigating the Command Line 68
Obtaining Help 69
Using the Keyword No 71
Filtering show Commands 71
Displaying All Output 72
Filtering Command Output Multiple Times 72
Command Modes 72
EXEC Mode 72
EXEC Privilege Mode 72
CONFIGURATION Mode 73
INTERFACE Mode 73
LINE Mode 74
TRACE-LIST Mode 74
MAC ACCESS LIST Mode 74
IP ACCESS LIST Mode 75
ROUTE-MAP Mode 75
PREFIX-LIST Mode 75
AS-PATH ACL Mode 76
IP COMMUNITY LIST Mode 76
REDIRECT-LIST Mode 76

SPANNING TREE Mode 77
Per-VLAN SPANNING TREE Plus Mode 77
RAPID SPANNING TREE Mode 77
MULTIPLE SPANNING TREE Mode 77
PROTOCOL FVRP Mode 78
ROUTER OSPF Mode 78
ROUTER RIP Mode 78
ROUTER ISIS Mode 79
ROUTER BGP Mode 79
Determining the Chassis Mode 79

Chapter 2
File Management Commands 81

boot config *82*
boot host *82*
boot network *83*
boot system *84*
boot system gateway *85*
cd *85*
change bootflash-image *85*
copy *86*
copy (Streamline Upgrade) *87*
copy running-config startup-config duplicate *88*
delete *88*
dir *89*
download alt-boot-image *89*
download alt-full-image *90*
download alt-system-image *90*
format *91*
logging kernel-coredump *91*
logging kernel-coredump server *93*
pwd *93*
rename *94*
show bootvar *94*
show file *95*
show file-systems *96*
show os-version *97*
show running-config *98*
show version *100*
show startup-config *102*
upgrade *103*

Chapter 3
Control and Monitoring Commands 105

Control and Setup Commands 105
audible cut-off *107*
banner exec *107*
banner login *108*
banner motd *109*
cam-audit linecard *109*
chassis chassis-mode *110*
clear alarms *111*
clear line *111*
configure *111*
debug cpu-traffic-stats *112*
debug ftpserver *113*
disable *113*
do *113*
enable *114*
enable xfp-power-updates *115*
end *116*
epoch *116*
exec-banner *117*
exec-timeout *117*
exit *118*
ftp-server enable *118*
ftp-server topdir *119*
ftp-server username *120*
hostname *120*
ip ftp password *121*
ip ftp source-interface *121*
ip ftp username *122*
ip telnet server enable *123*
ip telnet source-interface *123*
ip tftp source-interface *124*
line *125*
linecard *126*
module power-off *126*
motd-banner *127*
ping *127*
power-off *129*
power-on *129*
reload *130*
reset *130*
send *131*

service timestamps . . . 131
show alarms . . . 132
show chassis . . . 133
show console lp . . . 135
show cpu-traffic-stats . . . 135
show debugging . . . 136
show environment . . . 137
show inventory . . . 139
show linecard . . . 140
show linecard boot-information . . . 142
show memory . . . 144
show processes communication (deprecated) . . . 145
show processes cpu . . . 146
show processes ipc flow-control . . . 148
Important Points to Remember . . . 149
show processes memory . . . 150
show processes switch-utilization . . . 153
show rpm . . . 153
show sfm . . . 155
show switch links . . . 157
show tech-support . . . 158
ssh-peer-rpm . . . 160
telnet . . . 160
telnet-peer-rpm . . . 161
terminal length . . . 162
terminal xml . . . 162
traceroute . . . 163
undebug all . . . 164
upgrade sfm . . . 165
upload nvtrace linecard . . . 165
upload trace-log . . . 166
virtual-ip . . . 167
write . . . 167
Upgrading the FPGA . . . 168
reset . . . 168
restore fpga-flash . . . 169
upgrade primary-fpga-flash . . . 170

Chapter 4
IPv6 Basic Commands . . . 171

clear ipv6 route . . . 172
ipv6 address . . . 172
ipv6 route . . . 173

ipv6 unicast-routing *175*
show ipv6 cam linecard *175*
show ipv6 fib linecard *178*
show ipv6 interface *178*
show ipv6 route *179*
trust ipv6-diffserv *182*

Chapter 5
C-Series
Diagnostics and Debugging 183

Inter-process Communication Commands 183
clear hardware cpu party-bus *184*
clear hardware rpm mac counters *184*
clear hardware mac port-statistics *185*
show hardware cpu party-bus *185*
show hardware rpm mac *187*
RPM Management Port Commands 189
show hardware rpm cpu management *189*
Data Path Debugging 191
show hardware drops *191*
show hardware cpu data-plane *193*
Interface Troubleshooting 195
show hardware interface phy *195*
Advanced ASIC Debugging Information 198
clear hardware unit *198*
show hardware unit *199*
show revision *199*
ACL & System-Flow Debug Commands 200
clear hardware system-flow *200*
show hardware acl *201*
show hardware layer3 qos linecard port-set *202*
show hardware system-flow layer2 linecard port-set *202*
Interface Management Debug Commands 203
debug ifm trace-flags *203*
show software ifm *204*
Layer 2 Debug Commands 205
show software macagent *205*
Trace Logging Commands 206
clear trace hardware *206*
debug cpu-traffic-stats *207*
show command-history *208*
show console lp *208*
show cpu-traffic-stats *209*

show hardware linecard fpga *209*
show hardware rpm fpga *210*
show trace *212*
Offline Diagnostics 213
diag linecard *214*
offline *215*
online *215*
show diag *216*

Chapter 6
E-Series
Debugging and Diagnostics 219

Diagnostics and Monitoring 219
Important Points to Remember 219
dataplane-diag disable loopback *220*
dataplane-diag disable sfm-bringdown *221*
dataplane-diag disable sfm-walk *222*
dataplane-diag disable dfo-reporting *223*
diag sfm *223*
logging coredump kernel disable *224*
logging coredump kernel server *225*
logging coredump linecard *226*
power-off/on sfm *226*
show command-history *228*
show console *230*
reset sfm *230*
show diag sfm *231*
show processes communication (deprecated) *232*
show processes ipc *232*
show processes ipc flow-control *234*
Important Points to Remember 236
show revision *236*
show tech-support *237*
Offline Diagnostics 239
diag linecard *240*
offline *241*
online *241*
show diag *242*
Hardware Information 242
clear hardware btm *243*
clear hardware rpm mac counters *244*
show hardware btm *244*
show hardware fpc forward *246*

show hardware fpc lookup detail 249
show hardware rpm cp 250
show hardware rpm mac counters 252
show hardware rpm rp1/rp2 253
show interfaces link-status 253
show interfaces phy 254
show interfaces transceiver 256
show logging driverlog 257

Chapter 7
sFlow Commands 259

Important Points to Remember 259
sflow collector 260
sflow enable (Global) 261
sflow enable (Interface) 262
sflow extended-gateway enable 262
sflow extended-router enable 263
sflow extended-switch enable 264
sflow polling-interval (Global) 265
sflow polling-interval (Interface) 265
sflow sample-rate (Global) 266
sflow sample-rate (Interface) 267
show sflow 267
show sflow linecard 269

Chapter 8
CAM Profiling 271

CAM Profiling Commands 271
Important Points to Remember 272
cam-profile default microcode 273
cam-profile default microcode chassis 275
cam-profile default microcode linecard 275
cam-profile eg-default 276
cam-profile eg-default microcode default 277
cam-profile ipv4-320k 278
cam-profile ipv4-320k microcode (Configuration) 278
cam-profile ipv4-320k microcode (EXE) 280
cam-profile ipv4-egacl-16k microcode 281
cam-profile ipv4-egacl-16k microcode chassis 282
cam-profile ipv4-egacl-16k microcode linecard 283
cam-profile l2-ipv4-inacl microcode 283
cam-profile unified-default microcode 284
show cam-profile 285

show cam-profile default microcode . . . 287
show cam-profile eg-default microcode . . . 288
show cam-profile ipv4-320k microcode . . . 288
show cam-profile ipv4-egacl-16k microcode . . . 289
show cam-usage . . . 290
CAM IPv4flow Commands . . . 294
Important Points to Remember . . . 294
cam-ipv4flow (EtherScale) . . . 295
cam-ipv4flow (TeraScale) . . . 296
cam ipv4flow chassis all (EtherScale) . . . 297
cam ipv4flow chassis all (TeraScale) . . . 299
cam ipv4flow linecard (EtherScale) . . . 300
cam ipv4flow linecard (TeraScale) . . . 302
show cam-ipv4flow . . . 303

Chapter 9
ACL VLAN Group . . . 307

acl-vlan-group . . . 307
description . . . 308
ip access-group . . . 309
member vlan . . . 309
show acl-vlan-group . . . 310
show config . . . 311
show running config acl-vlan-group . . . 312

Chapter 10
LLDP . . . 313

advertise dot1-tlv . . . 314
advertise dot3-tlv . . . 314
advertise management . . . 315
clear lldp counters . . . 315
clear lldp neighbors . . . 316
debug lldp interface . . . 316
disable . . . 317
hello . . . 318
mode . . . 318
multiplier . . . 319
protocol lldp (Configuration) . . . 319
protocol lldp (Interface) . . . 320
show lldp neighbors . . . 320
show lldp statistics . . . 321
show running-config lldp . . . 322

Chapter 11
SNMP and Syslog Commands 323

SNMP Commands 323
Important Points to Remember 323
show snmp *324*
show snmp engineID *325*
show snmp group *325*
show snmp user *326*
snmp-server community *326*
snmp-server contact *328*
snmp-server enable traps *328*
snmp-server engineID *329*
snmp-server group *330*
snmp-server host *332*
snmp-server location *334*
snmp-server trap-source *334*
snmp-server user *335*
snmp-server view *338*
snmp trap link-status *338*
Syslog Commands 339
clear logging *339*
default logging buffered *340*
default logging console *340*
default logging monitor *341*
default logging trap *341*
logging *341*
logging buffered *342*
logging console *343*
logging facility *343*
logging history *344*
logging history size *345*
logging monitor *346*
logging on *346*
logging source-interface *347*
logging synchronous *347*
logging trap *348*
show logging *349*
terminal monitor *350*

Chapter 12
RMON 353

Important Points to Remember 354
rmon alarm *354*

rmon collection history 355
rmon collection statistics 356
rmon event 356
rmon hc-alarm 357
show rmon 358
show rmon alarms 359
show rmon events 360
show rmon hc-alarm 361
show rmon history 362
show rmon log 363
show rmon statistics 364

Chapter 13
High Availability Commands. 367

redundancy auto-failover-limit 367
redundancy disable-auto-reboot 368
redundancy force-failover 369
redundancy primary 370
redundancy reset-counter 370
redundancy sfm standby 370
redundancy synchronize 371
show redundancy 372

Chapter 14
Time Commands 375

calendar set 376
clock read-calendar 377
clock set 377
clock summer-time date 378
clock summer-time recurring 379
clock timezone 380
clock update-calendar 381
debug ntp 381
ntp authenticate 382
ntp authentication-key 382
ntp broadcast client 383
ntp disable 383
ntp multicast client 383
ntp server 384
ntp source 385
ntp trusted-key 385
ntp update-calendar 386
show calendar 386

show clock *387*
show ntp associations *388*
show ntp status *389*

Chapter 15
Security Commands 391

AAA Accounting 391
aaa accounting *392*
aaa accounting suppress *393*
show accounting *393*
Authorization and Privilege 394
aaa authorization *394*
privilege level (CONFIGURATION mode) *395*
privilege level (LINE mode) *395*
Authentication and Password 396
aaa authentication enable *396*
aaa authentication login *397*
access-class *399*
enable password *399*
enable restricted *400*
enable secret *401*
login authentication *402*
password *402*
password-attributes *403*
service password-encryption *404*
show privilege *405*
show users *405*
timeout login response *406*
username *406*
RADIUS 407
debug radius *408*
ip radius source-interface *408*
radius-server deadtime *409*
radius-server host *409*
radius-server key *410*
radius-server retransmit *411*
radius-server timeout *412*
TACACS+ 412
debug tacacs+ *412*
ip tacacs source-interface *413*
tacacs-server host *413*
tacacs-server key *414*
Port Authentication (802.1x) 415

Important Points to Remember 415
dot1x authentication (Configuration) *416*
dot1x authentication (Interface) *416*
dot1x auth-server *417*
dot1x max-eap-req *417*
dot1x port-contol *418*
dot1x quiet-period *418*
dot1x reauthentication *419*
dot1x reauth-max *419*
dot1x server-timeout *420*
dot1x supplicant-timeout *420*
dot1x tx-period *421*
SSH Server and SCP 421
crypto key generate *422*
debug ip ssh *423*
ip scp topdir *424*
ip ssh authentication-retries *424*
ip ssh connection-rate-limit *425*
ip ssh hostbased-authentication *425*
ip ssh key-size *426*
ip ssh password-authentication *426*
ip ssh pub-key-file *427*
ip ssh rhostsfile *427*
ip ssh rsa-authentication (Config) *428*
ip ssh rsa-authentication (EXEC) *429*
ip ssh server *429*
show crypto *430*
show ip ssh *431*
show ip ssh client-pub-keys *432*
show ip ssh rsa-authentication *432*
ssh *433*
Trace List 434
clear counters ip trace-group *434*
deny *435*
deny tcp *436*
deny udp *437*
ip trace-group *438*
ip trace-list *439*
permit *439*
permit tcp *440*
permit udp *442*
seq *443*
show config *444*

show ip accounting trace-lists 445

Chapter 16
Storm Control 447

Important Points to Remember 447
C-Series 447
E-Series 447
show storm-control broadcast 448
show storm-control unknown-unicast 449
storm-control broadcast (Configuration) 450
storm-control unknown-unicast (Configuration) 451
storm-control broadcast (Interface) 452
storm-control unknown-unicast (Interface) 453

Chapter 17
Interface Commands 455

Basic Interface Commands 455
clear counters 456
clear dampening 458
dampening 458
description 460
duplex (Management) 460
duplex (10/100 Interfaces) 461
flowcontrol 461
Important Points to Remember 462
interface 464
interface loopback 464
interface ManagementEthernet 465
interface null 466
interface port-channel 467
interface range 468
interface range macro (define) 470
interface range macro name 472
interface rate-interval 472
interface vlan 473
ipg (Gigabit Ethernet interfaces) 474
ipg (10 Gigabit Ethernet interfaces) 474
keepalive 475
lfs enable (EtherScale) 475
monitor 476
mtu 478
negotiation auto 480
portmode hybrid 482

show config . . . 483
show config (Bulk Configuration) . . . 484
show interfaces . . . 484
show interfaces configured . . . 490
show interfaces dampening . . . 491
show interfaces description . . . 492
show interfaces linecard . . . 493
show interfaces status . . . 493
show interfaces switchport . . . 494
show range . . . 496
shutdown . . . 496
speed (10/100/1000 Interfaces) . . . 497
speed (Management interface) . . . 498
switchport . . . 498
WAN Port . . . 499
Port Channel-Specific Commands . . . 500
channel-member . . . 500
minimum-links . . . 501
show interfaces port-channel . . . 502
show port-channel-flow . . . 505
Port Mirroring (Deprecated) . . . 507
mirroring source port (deprecated) . . . 507
show run mirroring (deprecated) . . . 507
Time Domain Reflectometer (TDR) . . . 507
Important Points to Remember . . . 508
tdr-cable-test . . . 508
show tdr . . . 509
UDP Broadcast . . . 510
Important Points to Remember . . . 510
debug ip udp-helper . . . 510
ip udp-broadcast-address . . . 511
ip udp-helper udp-port . . . 512
show ip udp-helper . . . 512

Chapter 18
Port Monitoring . . . 515

Important Points to Remember . . . 515
flow-based enable . . . 515
monitor session . . . 516
show config . . . 517
show monitor session . . . 517
show running-config monitor session . . . 518
source . . . 519

Chapter 19
LACP 521

clear lacp counters 521
debug lacp 522
lacp long-timeout 523
lacp port-priority 523
lacp system-priority 524
port-channel mode 524
port-channel-protocol lacp 525
show lacp 525

Chapter 20
SONET 527

ais-shut 528
alarm-report 528
clock source 530
debug ppp 530
delay triggers 531
down-when-looped 532
encap 532
flag 533
framing 533
interface sonet 534
keepalive 534
loopback 535
ppp authentication 536
ppp chap hostname 537
ppp chap password 537
ppp chap rem-hostname 538
ppp chap rem-password 538
ppp next-hop 539
ppp pap hostname 540
ppp pap password 540
ppp pap rem-hostname 541
ppp pap rem-password 541
scramble-atm 542
show controllers 543
show interfaces 545
speed 547

Chapter 21
Layer 2 Protocol Tunneling 549

Important Points to Remember 549

debug protocol-tunnel . . . 550
protocol-tunnel . . . 550
protocol-tunnel enable . . . 551
protocol-tunnel rate-limit . . . 552
show protocol-tunnel . . . 553

Chapter 22
Layer 2 . . . 555

MAC Addressing . . . 555
clear mac-address-table dynamic . . . 556
mac-address-table aging-time . . . 556
mac-address-table static . . . 557
mac-address-table station-move . . . 558
mac-address-table station-move refresh-arp . . . 558
mac accounting destination . . . 559
mac cam fib-partition . . . 559
mac learning-limit . . . 560
mac learning limit dynamic | no-station-move . . . 561
mac learning-limit learn-limit-violation . . . 562
mac learning-limit station-move-violation . . . 562
mac learning-limit reset . . . 563
show mac-address-table . . . 564
show mac-address-table aging-time . . . 566
show mac accounting destination . . . 566
show mac cam . . . 567
show mac learning-limit . . . 568
Virtual LANs . . . 569
default vlan-id . . . 570
name . . . 570
show vlan . . . 571
tagged . . . 572
track ip . . . 573
untagged . . . 574

Chapter 23
Resilient Ring Protocol . . . 575

Important Points to Remember . . . 575
clear frrp . . . 576
debug frrp . . . 577
description . . . 577
disable . . . 578
interface . . . 578
member-vlan . . . 580

mode 580
protocol frrp 581
show frrp 581
timer 583

Chapter 24
FVRP 585

Important Points to Remember 585
disable 586
fvrp access 586
fvrp aware 587
fvrp control-vlan 588
fvrp core 588
fvrp core region 589
fvrp disable 589
fvrp domain 590
fvrp group 591
fvrp hello-time 591
fvrp preempt 592
fvrp priority (for a VLAN) 592
fvrp priority (for an interface) 593
fvrp uplink 594
protocol fvrp 594
show config 595
show fvrp 595

Chapter 25
VLAN-Stack VLANs 599

Important Points to Remember 599
member 600
vlan-stack access 600
vlan-stack compatible 601
vlan-stack protocol-type 602
vlan-stack trunk 603

Chapter 26
Access Control List 605

Standard IP ACLs 605
deny 606
ip access-list standard 607
permit 608
remark 609
resequence access-list 610

resequence prefix-list ipv4 611
seq 611
Extended IP ACLs 613
deny 613
deny arp 615
deny ether-type 616
deny icmp 618
deny tcp 621
deny udp 623
ip access-list extended 625
permit 626
permit arp 628
permit ether-type 629
permit icmp 631
permit tcp 632
permit udp 635
resequence access-list 637
resequence prefix-list ipv4 638
seq arp 638
seq ether-type 640
seq 642
Common IP ACL Commands 644
access-class 644
clear counters ip access-group 645
ip access-group 645
show config 646
show ip accounting access-list 646
Standard MAC ACLs 647
deny 648
mac access-list standard 649
permit 649
seq 650
Extended MAC ACLs 651
deny 651
mac access-list extended 653
permit 654
seq 655
Common MAC Access List Commands 656
clear counters mac access-group 657
mac access-group 657
show mac accounting access-list 658
IP Prefix List Commands 658
clear ip prefix-list 659

deny 659
ip prefix-list 660
permit 660
seq 661
show config 662
show ip prefix-list detail 662
show ip prefix-list summary 663
Route Map Commands 664
continue 664
Match clause with Continue clause 665
Set clause with Continue clause 665
match as-path 666
match community 666
match interface 667
match ip address 667
match ip next-hop 668
match ip route-source 669
match metric 669
match origin 670
match route-type 670
match tag 671
route-map 672
set as-path 673
set automatic-tag 673
set comm-list delete 674
set community 675
set level 676
set local-preference 676
set metric 677
set metric-type 677
set next-hop 678
set origin 679
set tag 679
set weight 680
show config 680
show route-map 681
AS-Path Commands 681
deny 682
ip as-path access-list 682
permit 683
show config 684
show ip as-path-access-lists 685
IP Community List Commands 685

deny 686
ip community-list 687
permit 687
show config 688
show ip community-lists 689

Chapter 27
IPv6 Access Control Lists 691

Important Points to Remember 691
IPv6 Extended ACLs 691
clear counters ipv6 access-group 692
deny 692
deny icmp 693
deny tcp 695
deny udp 697
ipv6 access-group 699
ipv6 access-list 700
permit 701
permit icmp 701
permit tcp 703
permit udp 705
remark 707
resequence access-list 708
resequence prefix-list ipv6 708
seq 709
show config 711
show ipv6 accounting access-list 712
show running-config acl 713
Route Map Commands 713
match ipv6 address 714
match ipv6 next-hop 714
match ipv6 route-source 715
route-map 715
set ipv6 next-hop 716
show config 716
show route-map 717

Chapter 28
IP Routing Commands 719

arp 720
arp timeout 721
clear arp-cache 721
clear host 722

clear ip fib linecard . . . 723
clear ip route . . . 723
clear tcp statistics . . . 724
debug arp . . . 724
debug ip dhcp . . . 725
debug ip icmp . . . 726
debug ip packet . . . 727
hash-algorithm ecmp . . . 728
hash-algorithm . . . 729
ip address . . . 731
ip directed-broadcast . . . 732
ip domain-list . . . 732
ip domain-lookup . . . 733
ip domain-name . . . 734
ip fib download-igp-only . . . 734
ip helper-address . . . 735
ip helper-address hop-count disable . . . 735
ip host . . . 736
ip max-frag-count . . . 736
ip mtu . . . 737
ip name-server . . . 738
ip proxy-arp . . . 739
ip redirects . . . 739
ip route . . . 740
ip source-route . . . 741
ip unreachables . . . 741
ip vlan-flooding . . . 742
load-balance . . . 742
load-balance . . . 744
management route . . . 745
show arp . . . 747
show hosts . . . 749
show ip cam . . . 750
show ip fib linecard . . . 753
show ip flow . . . 754
show ip interface . . . 755
show ip management-route . . . 757
show ip protocols . . . 758
show ip route . . . 758
show ip route list . . . 760
show ip route summary . . . 761
show ip traffic . . . 762
show protocol-termination-table . . . 764

show tcp statistics 765

Chapter 29
Policy-based Routing 769

ip redirect-group 770
ip redirect-list 771
permit 771
redirect 773
seq 774
show cam pbr 775
show ip redirect-list 777

Chapter 30
Far-End Failure Detection 779

debug fefd 779
fefd 780
fefd-global 781
fefd disable 781
fefd interval 782
fefd-global interval 782
fefd reset 783
show fefd 783

Chapter 31
VRRP Commands 785

advertise-interval 785
authentication-type 786
clear counters vrrp 787
debug vrrp 787
description 788
disable 788
hold-time 789
preempt 789
priority 790
show config 790
show vrrp 791
track 793
virtual-address 794
vrrp-group 795

Chapter 32
Spanning Tree Protocol 797

bridge-priority 797

debug spanning-tree 798
disable 798
forward-delay 799
hello-time 799
max-age 800
protocol spanning-tree 800
show config 801
show spanning-tree 0 801
spanning-tree 803

Chapter 33
PVST+ **805**

disable 805
protocol spanning-tree pvst 806
show spanning-tree pvst 806
spanning-tree pvst 809
tc-flush-standard 811
vlan bridge-priority 811
vlan forward-delay 812
vlan hello-time 812
vlan max-age 813

Chapter 34
RSTP **815**

bridge-priority 815
debug spanning-tree rstp 816
disable 817
forward-delay 817
hello-time 818
max-age 818
protocol spanning-tree rstp 819
show config 820
show spanning-tree rstp 820
spanning-tree rstp 822
tc-flush-standard 823

Chapter 35
MSTP **825**

debug spanning-tree mstp 825
disable 826
forward-delay 827
hello-time 827
max-age 828

max-hops 828
msti 829
name 830
protocol spanning-tree mstp 830
revision 831
show config 832
show spanning-tree mst configuration 832
show spanning-tree msti 833
spanning-tree 835
spanning-tree msti 836
spanning-tree mstp edge-port 837
tc-flush-standard 837

Chapter 36
Router Information Protocol 839

auto-summary 840
clear ip rip 840
debug ip rip 841
default-information originate 841
default-metric 842
distance 843
distribute-list in 843
distribute-list out 844
ip poison-reverse 845
ip rip receive version 845
ip rip send version 846
ip split-horizon 847
maximum-paths 847
neighbor 848
network 848
offset-list 849
output-delay 850
passive-interface 850
redistribute 851
redistribute isis 852
redistribute ospf 852
router rip 853
show config 854
show ip rip database 854
timers basic 855
version 856

Chapter 37
OSPF 859

area default-cost 861
area nssa 861
area range 862
area stub 862
area virtual-link 863
auto-cost 864
clear ip ospf 865
clear ip ospf statistics 865
debug ip ospf 866
default-information originate 867
default-metric 868
distance 869
distance ospf 869
distribute-list in 870
distribute-list out 871
enable inverse mask 871
flood-2328 872
graceful-restart grace-period 872
graceful-restart helper-reject 873
graceful-restart mode 873
graceful-restart role 873
ip ospf auth-change-wait-time 874
ip ospf authentication-key 874
ip ospf cost 875
ip ospf dead-interval 875
ip ospf hello-interval 876
ip ospf message-digest-key 876
ip ospf mtu-ignore 877
ip ospf network 878
ip ospf priority 878
ip ospf retransmit-interval 879
ip ospf transmit-delay 879
log-adjacency-changes 880
maximum-paths 880
network area 880
passive-interface 881
redistribute 883
redistribute bgp 884
redistribute isis 884
router-id 885
router ospf 886

show config 887
show ip ospf 887
show ip ospf asbr 888
show ip ospf database 889
show ip ospf database asbr-summary 890
show ip ospf database external 892
show ip ospf database network 893
show ip ospf database nssa-external 895
show ip ospf database opaque-area 896
show ip ospf database opaque-as 897
show ip ospf database opaque-link 898
show ip ospf database router 898
show ip ospf database summary 900
show ip ospf interface 902
show ip ospf neighbor 904
show ip ospf route 904
show ip ospf statistics 905
show ip ospf topology 909
show ip ospf virtual-links 909
summary-address 910
timers spf 911

Chapter 38
IPv6 OSPFv3 . . . . . **913**

clear ipv6 ospf process 914
debug ipv6 ospf packet 914
default-information originate 915
ipv6 ospf area 916
ipv6 ospf cost 917
ipv6 ospf dead-interval 918
ipv6 ospf hello-interval 918
ipv6 ospf priority 919
ipv6 router ospf 920
passive-interface 920
redistribute 921
router-id 922
show ipv6 ospf database 923
show ipv6 ospf interface 924
show ipv6 ospf neighbor 925

Chapter 39
Bidirectional Forwarding Detection **927**

bfd enable (Configuration) 928

bfd enable (Interface) 928
bfd interval 929
bfd all-neighbors (IS-IS) 930
bfd all-neighbors (OSPF) 931
bfd neighbor 931
bfd protocol-liveness 932
clear bfd counters 933
debug bfd 933
ip route bfd 934
isis bfd all-neighbors 935
show bfd counters 936
show bfd neighbors 937

Chapter 40
IS-IS Protocol 941

advertise 943
area-password 944
clear config 944
clear isis 945
clns host 945
debug isis 946
debug isis adj-packets 946
debug isis local-updates 947
debug isis snp-packets 948
debug isis spf-triggers 948
debug isis update-packets 949
default-information originate 949
distance 950
distribute-list in 951
distribute-list out 952
distribute-list redistributed-override 953
domain-password 953
hello padding 954
hostname dynamic 955
ignore-lsp-errors 955
ip router isis 956
isis circuit-type 956
isis csnp-interval 957
isis hello-interval 958
isis hello-multiplier 959
isis hello padding 959
isis metric 960
isis network point-to-point 961

isis password 961
isis priority 962
is-type 963
log-adjacency-changes 963
lsp-gen-interval 964
lsp-mtu 965
lsp-refresh-interval 965
max-area-addresses 966
max-lsp-lifetime 967
maximum-paths 967
metric-style 968
net 969
passive-interface 969
redistribute 970
redistribute bgp 972
redistribute ospf 973
router isis 974
set-overload-bit 975
show config 976
show isis database 976
show isis hostname 978
show isis interface 978
show isis neighbors 979
show isis protocol 980
show isis traffic 981
spf-interval 983

Chapter 41
IPv6 IS-IS Protocol 985

address family ipv6 unicast 986
adjacency-check 987
advertise 988
area-password 988
clear config 989
clear isis 990
clns host 990
debug isis 991
debug isis adj-packets 992
debug isis local-updates 992
debug isis snp-packets 993
debug isis spf-triggers 994
debug isis update-packets 994
default-information originate 995

domain-password . . . 996
hello padding . . . 996
hostname dynamic . . . 997
ignore-lsp-errors . . . 998
isis circuit-type . . . 998
isis csnp-interval . . . 999
isis hello-interval . . . 1000
isis hello-multiplier . . . 1001
isis hello padding . . . 1002
isis ipv6 metric . . . 1003
isis network point-to-point . . . 1003
isis password . . . 1004
isis priority . . . 1005
is-type . . . 1006
log-adjacency-changes . . . 1006
lsp-gen-interval . . . 1007
lsp-mtu . . . 1008
lsp-refresh-interval . . . 1009
max-area-addresses . . . 1010
max-lsp-lifetime . . . 1010
maximum-paths . . . 1011
net . . . 1012
passive-interface . . . 1012
ipv6 router isis . . . 1013
set-overload-bit . . . 1014
show config . . . 1015
show isis database detail . . . 1015
show isis hostname . . . 1016
show isis interface . . . 1016
show isis neighbors . . . 1017
show isis protocol . . . 1018
spf-interval . . . 1019

Chapter 42
BGP . . . 1021

BGP Commands . . . 1021
aggregate-address . . . 1024
bgp always-compare-med . . . 1025
bgp bestpath as-path ignore . . . 1025
bgp bestpath med confed . . . 1026
bgp bestpath med missing-as-best . . . 1026
bgp client-to-client reflection . . . 1027
bgp cluster-id . . . 1027

bgp confederation identifier 1028
bgp confederation peers 1029
bgp dampening 1029
bgp default local-preference 1030
bgp enforce-first-as 1031
bgp fast-external-fallover 1032
bgp graceful-restart 1032
bgp log-neighbor-changes 1033
bgp non-deterministic-med 1034
bgp recursive-bgp-next-hop 1034
bgp router-id 1035
bgp soft-reconfig-backup 1035
capture bgp-pdu neighbor (ipv4) 1036
capture bgp-pdu max-buffer-size 1037
clear ip bgp 1037
clear ip bgp peer-group 1038
clear ip bgp dampening 1039
clear ip bgp flap-statistics 1039
debug ip bgp 1040
debug ip bgp dampening 1041
debug ip bgp events 1042
debug ip bgp keepalives 1042
debug ip bgp notifications 1043
debug ip bgp soft-reconfiguration 1043
debug ip bgp updates 1044
default-metric 1045
distance bgp 1045
maximum-paths 1046
neighbor activate 1047
neighbor advertisement-interval 1047
neighbor default-originate 1048
neighbor description 1049
neighbor distribute-list 1049
neighbor ebgp-multihop 1050
neighbor fall-over 1051
neighbor filter-list 1051
neighbor graceful-restart 1052
neighbor maximum-prefix 1053
neighbor next-hop-self 1054
neighbor password 1054
neighbor peer-group (assigning peers) 1055
neighbor peer-group (creating group) 1057
neighbor peer-group passive 1057

neighbor remote-as *1058*
neighbor remove-private-as *1059*
neighbor route-map *1059*
neighbor route-reflector-client *1060*
neighbor send-community *1061*
neighbor shutdown *1061*
neighbor soft-reconfiguration inbound *1063*
neighbor subnet *1063*
neighbor timers *1064*
neighbor update-source *1065*
neighbor weight *1066*
network *1066*
network backdoor *1067*
redistribute *1068*
redistribute isis *1069*
redistribute ospf *1070*
router bgp *1071*
show capture bgp-pdu neighbor (ipv4) *1071*
show config *1072*
show ip bgp *1073*
show ip bgp cluster-list *1075*
show ip bgp community *1076*
show ip bgp community-list *1078*
show ip bgp dampened-paths *1079*
show ip bgp detail *1079*
show ip bgp filter-list *1081*
show ip bgp flap-statistics *1082*
show ip bgp inconsistent-as *1084*
show ip bgp neighbors *1085*
show ip bgp next-hop *1089*
show ip bgp paths *1089*
show ip bgp paths as-path *1091*
show ip bgp paths community *1092*
show ip bgp peer-group *1093*
show ip bgp regexp *1095*
show ip bgp summary *1096*
MBGP Commands 1098
address family *1099*
aggregate-address *1100*
bgp dampening *1101*
clear ip bgp ipv4 multicast *1102*
clear ip bgp dampening *1102*
clear ip bgp flap-statistics *1103*

debug ip bgp dampening *1103*
debug ip bgp peer-group updates *1104*
debug ip bgp updates *1104*
distance bgp *1105*
neighbor activate *1106*
neighbor advertisement-interval *1106*
neighbor default-originate *1107*
neighbor distribute-list *1108*
neighbor filter-list *1108*
neighbor maximum-prefix *1109*
neighbor next-hop-self *1110*
neighbor remove-private-AS *1111*
neighbor route-map *1111*
neighbor route-reflector-client *1112*
network *1113*
redistribute *1114*
redistribute ospf *1115*
show ip bgp ipv4 multicast *1115*
show ip bgp cluster-list *1117*
show ip bgp community *1117*
show ip bgp community-list *1118*
show ip bgp dampened-paths *1118*
show ip bgp filter-list *1119*
show ip bgp flap-statistics *1119*
show ip bgp inconsistent-as *1120*
show ip bgp ipv4 multicast neighbors *1120*
show ip bgp peer-group *1123*
show ip bgp summary *1124*

Chapter 43
IPv6 BGP 1127

IPv6 BGP Commands 1127
aggregate-address *1129*
bgp always-compare-med *1131*
bgp bestpath as-path ignore *1131*
bgp bestpath med confed *1132*
bgp bestpath med misssing-as-best *1132*
bgp client-to-client reflection *1133*
bgp cluster-id *1133*
bgp confederation identifier *1134*
bgp confederation peers *1135*
bgp dampening *1136*
bgp default local-preference *1137*

bgp fast-external-fallover 1137
bgp graceful-restart 1138
bgp log-neighbor-changes 1139
bgp non-deterministic-med 1139
bgp router-id 1140
capture bgp-pdu neighbor (ipv6) 1141
capture bgp-pdu max-buffer-size 1141
clear ip bgp * (asterisk) 1142
clear ip bgp as-number 1143
clear ip bgp ipv6-address 1144
clear ip bgp peer-group 1145
clear ip bgp ipv6 dampening 1145
clear ip bgp ipv6 flap-statistics 1146
debug ip bgp 1147
debug ip bgp ipv6 dampening 1148
debug ip bgp events 1148
debug ip bgp keepalives 1149
debug ip bgp notifications 1150
debug ip bgp updates 1150
default-metric 1151
distance bgp 1152
maximum-paths 1153
neighbor activate 1153
neighbor advertisement-interval 1154
neighbor default-originate 1155
neighbor description 1156
neighbor distribute-list 1156
neighbor ebgp-multihop 1157
neighbor fall-over 1158
neighbor filter-list 1159
neighbor maximum-prefix 1159
neighbor next-hop-self 1160
neighbor password 1161
neighbor peer-group (assigning peers) 1162
neighbor peer-group (creating group) 1163
neighbor peer-group passive 1164
neighbor remote-as 1164
neighbor remove-private-as 1165
neighbor route-map 1166
neighbor route-reflector-client 1167
neighbor send-community 1168
neighbor shutdown 1168
neighbor subnet 1169

neighbor timers *1170*
neighbor update-source *1171*
neighbor weight *1171*
network *1172*
network backdoor *1173*
redistribute *1174*
redistribute ospf *1175*
router bgp *1176*
show capture bgp-pdu neighbor (ipv6) *1176*
show config *1177*
show ip bgp ipv6 . . . . . *1178*
show ip bgp cluster-list *1178*
show ip bgp community *1179*
show ip bgp community-list *1179*
show ip bgp dampened-paths *1180*
show ip bgp filter-list *1180*
show ip bgp ipv6 flap-statistics *1181*
show ip bgp inconsistent-as *1182*
show ip bgp neighbors *1182*
show ip bgp next-hop *1183*
show ip bgp paths *1184*
show ip bgp paths as-path *1185*
show ip bgp paths community *1185*
show ip bgp peer-group *1185*
show ip bgp regexp *1186*
show ip bgp summary *1187*
timers bgp *1188*
IPv6 MBGP Commands 1189
address family *1190*
aggregate-address *1190*
bgp dampening *1192*
clear ip bgp ipv6 unicast *1192*
clear ip bgp ipv6 unicast dampening *1193*
clear ip bgp ipv6 unicast flap-statistics *1194*
debug ip bgp ipv6 unicast dampening *1194*
debug ip bgp ipv6 unicast peer-group updates *1195*
debug ip bgp ipv6 unicast updates *1196*
distance bgp *1196*
neighbor activate *1197*
neighbor advertisement-interval *1198*
neighbor default-originate *1199*
neighbor distribute-list *1199*
neighbor filter-list *1200*

neighbor maximum-prefix *1201*
neighbor next-hop-self *1202*
neighbor remove-private-AS *1202*
neighbor route-map *1203*
neighbor route-reflector-client *1204*
network *1204*
redistribute *1205*
show ip bgp ipv6 unicast *1206*
show ip bgp ipv6 unicast cluster-list *1208*
show ip bgp ipv6 unicast community *1208*
show ip bgp ipv6 unicast community-list *1209*
show ip bgp ipv6 unicast dampened-paths *1210*
show ip bgp ipv6 unicast detail *1210*
show ip bgp ipv6 unicast filter-list *1211*
show ip bgp ipv6 unicast flap-statistics *1212*
show ip bgp ipv6 unicast inconsistent-as *1213*
show ip bgp ipv6 unicast neighbors *1213*
show ip bgp ipv6 unicast peer-group *1216*
show ip bgp ipv6 unicast summary *1217*

Chapter 44
Quality of Service. 1219

Per-Port QoS 1219
dot1p-priority *1219*
rate limit *1220*
rate police *1221*
C-Series 1222
E-Series 1222
rate shape *1223*
service-class dynamic dot1p *1223*
show interfaces rate *1224*
strict-priority queue *1226*
Policy-Based QoS 1227
bandwidth-percentage *1228*
class-map *1228*
clear qos statistics *1229*
E-Series Only 1230
match ip access-group *1230*
match ip dscp *1231*
match ip precedence *1232*
match mac access-group *1233*
match mac dot1p *1233*
policy-aggregate *1234*

C-Series . . . 1234
E-Series . . . 1234
policy-map-input . . . *1235*
policy-map-output . . . *1236*
qos-policy-input . . . *1236*
qos-policy-name . . . *1237*
qos-policy-output . . . *1237*
queue egress . . . *1238*
Important Points to Remember—multicast-bandwidth option . . . 1239
queue ingress . . . *1240*
rate-limit . . . *1241*
rate-police . . . *1241*
rate-shape . . . *1242*
service-policy input . . . *1243*
service-policy output . . . *1243*
service-queue . . . *1244*
set . . . *1245*
C-Series . . . 1245
E-Series . . . 1245
show cam layer2-qos . . . *1245*
show cam layer3-qos . . . *1247*
show qos class-map . . . *1248*
show qos policy-map . . . *1249*
show qos policy-map-input . . . *1251*
show qos policy-map-output . . . *1252*
show qos qos-policy-input . . . *1253*
show qos qos-policy-output . . . *1253*
show qos statistics . . . *1254*
E-Series . . . 1255
show qos wred-profile . . . *1257*
test cam-usage . . . *1258*
threshold . . . *1260*
trust . . . *1261*
E-Series . . . 1261
wred . . . *1262*
wred-profile . . . *1263*
Queue Level Debugging . . . 1264
clear queue statistics egress . . . *1264*
clear queue statistics ingress . . . *1265*
show queue statistics egress . . . *1266*
show queue statistics ingress . . . *1270*

Chapter 45
Multicast 1277

Multicast Commands 1277
clear ip mroute *1278*
ip mroute *1278*
ip multicast-lag-hashing *1279*
ip multicast-routing *1280*
mtrace *1281*
show ip mroute *1281*
show ip rpf *1283*
IGMP Commands 1284
Important Points to Remember 1284
clear ip igmp groups *1285*
debug ip igmp *1285*
ip igmp immediate-leave *1286*
ip igmp last-member-query-interval *1286*
ip igmp querier-timeout *1287*
ip igmp query-interval *1287*
ip igmp query-max-resp-time *1288*
ip igmp static-group *1288*
Command Limitations 1289
ip igmp version *1289*
show ip igmp groups *1290*
show ip igmp interface *1291*
IGMP Snooping Commands 1292
Important Points to Remember for IGMP Snooping 1292
Important Points to Remember for IGMP Querier 1293
debug ip igmp *1293*
ip igmp snooping enable *1294*
ip igmp snooping fast-leave *1295*
ip igmp snooping flood *1295*
ip igmp snooping last-member-query-interval *1296*
ip igmp snooping mrouter *1296*
ip igmp snooping querier *1297*
show ip igmp snooping mrouter *1297*

Chapter 46
IPv6 Multicast 1299

IPv6 Multicast Commands 1299
clear ipv6 mroute *1300*
show ipv6 mroute *1300*
show ipv6 mroute mld *1303*
show ipv6 mroute summary *1304*

MLD Commands 1304
clear ipv6 mld groups *1305*
debug ipv6 mld *1306*
ipv6 mld explicit-tracking *1306*
ipv6 mld last-member-query-interval *1307*
ipv6 mld querier-timeout *1307*
ipv6 mld query-interval *1308*
ipv6 mld query-max-resp-time *1308*
ipv6 mld static-group *1309*
ipv6 mld version *1310*
show ipv6 mld interface *1310*
MLD Snooping Commands 1311
ipv6 mld snooping enable *1312*
ipv6 mld snooping flood *1312*
ipv6 mld snooping *1313*
ipv6 mld snooping explicit-tracking *1313*
ipv6 mld snooping mrouter *1314*
ipv6 mld snooping querier *1315*
show ipv6 mld snooping groups *1315*
show ipv6 mld snooping mrouter *1316*

Chapter 47
Protocol Independent Multicast 1317

PIM Sparse-Mode 1317
clear ip pim rp-mapping *1318*
clear ip pim tib *1318*
debug ip pim *1318*
Ip pim bsr-border *1319*
Ip pim bsr-candidate *1320*
ip pim dr-priority *1320*
ip pim query-interval *1321*
ip pim rp-address *1321*
ip pim rp-candidate *1322*
ip pim sparse-mode *1323*
ip pim spt-threshold *1324*
show ip pim bsr-router *1324*
show ip pim interface *1325*
show ip pim neighbor *1326*
show ip pim rp *1327*
show ip pim tib *1328*
PIM-SSM 1330
ip pim ssm-range *1330*
show ip pim ssm-range *1331*

PIM Dense-Mode 1332
ip pim dense-mode *1332*

Chapter 48
IPv6 Protocol Independent Multicast 1333

clear ipv6 pim tib *1334*
debug ipv6 pim *1334*
ipv6 pim bsr-candidate *1335*
ipv6 pim dr-priority *1336*
ipv6 pim query-interval *1336*
ipv6 pim rp-address *1337*
ipv6 pim rp-candidate *1338*
ipv6 pim sparse-mode *1338*
ipv6 pim spt-threshold *1339*
ipv6 pim ssm-range *1339*
show ipv6 pim bsr-router *1340*
show ipv6 pim interface *1341*
show ipv6 pim neighbor *1342*
show ipv6 pim rp *1342*
show ipv6 pim tib *1343*

Chapter 49
MSDP 1345

clear ip msdp peer *1345*
clear ip msdp sa-cache *1346*
debug ip msdp *1346*
ip msdp cache-rejected-sa *1347*
ip msdp default-peer *1348*
ip msdp log-adjacency-changes *1348*
ip msdp mesh-group *1349*
ip msdp originator-id *1349*
ip msdp peer *1350*
ip msdp sa-limit *1352*
ip msdp shutdown *1352*
ip multicast-msdp *1353*
show ip msdp *1353*
show ip msdp sa-cache rejected-sa *1355*

Chapter 50
NDP and RAD 1357

Neighbor Discovery Protocol 1357
clear ipv6 neighbors *1357*
ipv6 neighbor *1358*

show ipv6 neighbors *1359*
Router Advertisement Daemon 1360
ipv6 nd managed-config-flag *1361*
ipv6 nd max-ra-interval *1361*
ipv6 nd other-config-flag *1362*
ipv6 nd prefix *1362*
ipv6 nd ra-lifetime *1363*
ipv6 nd reachable-time *1363*
ipv6 nd suppress-ra *1364*

Chapter 51
Service Agent 1365

admin-email *1366*
call-home *1366*
debug call-home *1367*
domain-name *1368*
enable *1369*
enable-all *1369*
encrypt (TeraScale only) *1370*
frequency *1371*
keyadd (TeraScale only) *1371*
recipient *1372*
server *1373*
show configuration *1374*
show debugging *1374*
show keys (TeraScale only) *1375*
smtp *1375*

Chapter 52
Power Over Ethernet 1377

power inline *1377*
show hardware linecard poe-status *1378*
show power detail *1379*
show power inline *1380*
show power supply *1380*

Chapter 53
BOOT_USER 1383

boot change *1384*
boot messages *1385*
boot selection *1385*
default-gateway *1386*
delete *1386*

dir *1387*
enable *1388*
format *1388*
ignore enable-password *1388*
interface management ethernet ip address *1389*
interface management port config *1389*
reload *1390*
rename *1390*
show boot selection *1391*
show bootflash *1391*
show bootvar *1392*
show default-gateway *1393*
show interfaces management ethernet *1393*

Appendix A
ICMP Message Types **1395**

Appendix B
SNMP Traps **1397**

Index **1403**

Command Index **1415**

List of Figures

Figure 1 Login Example . . . 67
Figure 2 Configuration Mode User Alert . . . 68
Figure 3 Partial Keyword Example . . . 70
Figure 4 copy running-config scp: Command Example . . . 87
Figure 5 dir Command Example for the Internal Flash . . . 89
Figure 6 pwd Command Example . . . 94
Figure 7 show bootvar Command Output . . . 95
Figure 8 show file Command Example (Partial) . . . 96
Figure 9 show file-system Command Output . . . 96
Figure 10 show os-version Command Example (E-Series) . . . 98
Figure 11 show os-version Command Example (C-Series) . . . 98
Figure 12 show running-config Command Example (partial) . . . 100
Figure 13 show version Command Output . . . 101
Figure 14 show startup-config Command Output (partial) . . . 102
Figure 15 banner incoming Command Example . . . 108
Figure 16 chassis chassis-mode Command Options. . . . 110
Figure 17 configure Command Example . . . 112
Figure 18 do Command Example . . . 114
Figure 19 enable Command Example . . . 115
Figure 20 end Command Example . . . 116
Figure 21 Screenshot of Prompt After the FTOS Times Out . . . 118
Figure 22 exit Command Example . . . 118
Figure 23 Example of Logging on to an FTP Server . . . 119
Figure 24 ping (IPv4) Command Example . . . 128
Figure 25 ping (IPv6) Command Example . . . 128
Figure 26 show alarms Command Example . . . 133
Figure 27 show chassis brief Command Example . . . 134
Figure 28 show cpu-traffic-stats Command Example . . . 136
Figure 29 show debugging Command Example . . . 137
Figure 30 show environment Command Example for the E1200 . . . 138
Figure 31 show environment fan Command Example on the E600 . . . 138
Figure 32 show environment fan Command Example on the E300 . . . 139
Figure 33 show inventory media (partial) Command Example . . . 139
Figure 34 show inventory Command Example . . . 140

Figure 35 show linecard Command Example 141
Figure 36 show linecard brief Command Example 142
Figure 37 show linecard boot-information Command 143
Figure 38 show memory Command Example 145
Figure 39 show processes cpu Command Example (Partial) 147
Figure 40 show processes cpu rp1 Command Example 147
Figure 41 show processes cpu rp2 Command Example 148
Figure 42 show processes ipc flow-control rp Command Example 149
Figure 43 show processes ipc flow-control lp Command Example 149
Figure 44 show processes memory (partial) Command Example 151
Figure 45 show processes memory rp1 Command Example 151
Figure 46 show processes memory rp2 Command Example 152
Figure 47 show processes switch-utilization Command Example 153
Figure 48 show rpm Command Example 154
Figure 49 show sfm Command Example (Partial) 156
Figure 50 show sfm all Command Example 157
Figure 51 partial output of the show tech-support Command Example 159
Figure 52 traceroute (IPv4) Command Example 164
Figure 53 Traceroute (IPv6) Command Example 164
Figure 54 upgrade sfm autoreset Command Example 165
Figure 55 restore fpga-flash Command Example 169
Figure 56 upgrade primary-fpga-flash Command Example 170
Figure 57 ipv6 route command 174
Figure 58 show ipv6 cam linecard fib Command 176
Figure 59 show ipv6 cam linecard Command 177
Figure 60 show ipv6 interface Command 179
Figure 61 show ipv6 route Command Example 180
Figure 62 show ipv6 route summary Command Example 180
Figure 63 show hardware linecard Command Example 186
Figure 64 show hardware rpm mac counters Command Example 187
Figure 65 show hardware rpm mac port-statistics Command Example 188
Figure 66 show hardware rpm Command Example 190
Figure 67 show hardware drops Command Example 192
Figure 68 show hardware drops unit Command Example 192
Figure 69 show hardware drops unit port Command Example 193
Figure 70 show hardware linecard Command Example 194
Figure 71 show hardware rpm Command Example 194
Figure 72 show hardware interface Command Example 196
Figure 73 Auto-negotiation Mismatch Example 197
Figure 74 show revision command Example 200
Figure 75 show hardware rpm fpga registers Command Example 211
Figure 76 show hardware rpm fpga stats Command Example 212
Figure 77 show trace Command Example 213

Figure 78 show diag sfm command Example . . . 221
Figure 79 power-off sfm command with data traffic warning message . . . 227
Figure 80 power-off sfm command with switch fabric down warning message . . . 227
Figure 81 show sfm all command Example . . . 228
Figure 82 show command-history . . . 229
Figure 83 show console lp 0 command Example . . . 230
Figure 84 reset sfm command with warning message . . . 231
Figure 85 reset sfm error message . . . 231
Figure 86 show diag sfm command Example . . . 232
Figure 87 show processes ipc recv-stats Command Example . . . 233
Figure 88 show processes ipc send-stats Command Example . . . 234
Figure 89 show processes ipc flow-control rp Command Example . . . 235
Figure 90 show processes ipc flow-control lp Command Example . . . 235
Figure 91 show revision command Example (partial) . . . 237
Figure 92 partial output of the show tech-support Command Example . . . 238
Figure 93 show hardware fpc forward drops Command Example . . . 247
Figure 94 show hardware fpc forward counters Command Example . . . 248
Figure 95 show hardware rpm command Examples . . . 251
Figure 96 show hardware rpm mac counters Command Example . . . 252
Figure 97 show interfaces tengigabitethernet Command Example . . . 254
Figure 98 show interfaces gigabitethernet phy Command Example (Partial) . . . 255
Figure 99 show interfaces gigabitethernet transceiver Command Example . . . 257
Figure 100 show sflow Command Example . . . 268
Figure 101 show sflow linecard Command Example . . . 269
Figure 102 show cam-profile summary command . . . 286
Figure 103 show cam-profile command . . . 286
Figure 104 show cam-profile default microcode command . . . 287
Figure 105 show cam-usage Command . . . 292
Figure 106 show cam-usage acl Command . . . 292
Figure 107 show cam-usage router Command . . . 293
Figure 108 show cam-usage switch . . . 293
Figure 109 show cam-ipv4flow (EtherScale) Command . . . 304
Figure 110 show cam-ipv4flow (TeraScale) Command . . . 305
Figure 111 show acl-vlan-group command example . . . 310
Figure 112 show acl-vlan-group group1 command example 311
Figure 113 show config command example 311
Figure 114 show running-config acl-vlan-group command example . . . 312
Figure 115 show snmp Command Example . . . 324
Figure 116 show snmp engineID Command . . . 325
Figure 117 show snmp group Command Example . . . 325
Figure 118 show snmp user Command Example . . . 326
Figure 119 show logging Command Example (Partial) . . . 350
Figure 120 show logging history Command Example . . . 350

Figure 121 show rmon Command Example 358
Figure 122 show rmon alarms index Command Example 359
Figure 123 show rmon alarms brief Command Example 359
Figure 124 show rmon event index Command Example 360
Figure 125 show rmon event brief Command Example 360
Figure 126 show rmon hc-alarm brief Command Example 361
Figure 127 show rmon hc-alarm index Command Example 361
Figure 128 show rmon history index Command Example 362
Figure 129 show rmon history brief Command Example 362
Figure 130 show rmon log index Command Example 363
Figure 131 show rmon log brief Command Example 363
Figure 132 show rmon statistics index Command Example 364
Figure 133 show rmon statistics brief Command Example 365
Figure 134 redundancy force-failover rpm Command Example 369
Figure 135 redundancy force-failover sfm (E-Series Only) Command Example 369
Figure 136 show redundancy Command Example 372
Figure 137 calendar set Command Example 376
Figure 138 clock set Command Example 377
Figure 139 show calendar Command Example 387
Figure 140 show clock Command Example 387
Figure 141 show ntp associations Command Example 388
Figure 142 show ntp status Command Example 389
Figure 143 show accounting command 393
Figure 144 show privilege Command Output 405
Figure 145 show users Command Example 405
Figure 146 crypto key generate rsa1 command example 423
Figure 147 show crypto command examples 431
Figure 148 show ip ssh Command Example 431
Figure 149 show ip ssh client-pub-keys command 432
Figure 150 show ip ssh rsa-authentication command 433
Figure 151 ip trace-list Command Example 439
Figure 152 show config Command Example in TRACE LIST Mode 445
Figure 153 show ip accounting trace-lists Command Example 445
Figure 154 show storm-control broadcast command Example (E-Series) 449
Figure 155 show storm-control broadcast command Example (C-Series) 449
Figure 156 show storm-control unknown-unicast command Example (E-Series) 450
Figure 157 show storm-control unknown-unicast command Example (C-Series) 450
Figure 158 clear counters Command Example 457
Figure 159 show running config (partial) 463
Figure 160 interface Command Example 464
Figure 161 interface loopback Command Example 465
Figure 162 interface ManagementEthernet Command Example 465
Figure 163 interface null Command Example 466

Figure 164 interface port-channel Command Example . . . 467
Figure 165 Bulk Configuration Warning Message . . . 469
Figure 166 Interface Range prompt with Multiple Ports . . . 469
Figure 167 Interface Range prompt Overlapping Port Ranges . . . 469
Figure 168 Single range Bulk Configuration . . . 469
Figure 169 Multiple range Bulk Configuration Gigabit Ethernet and Ten Gigabit Ethernet . . . 470
Figure 170 Multiple range Bulk Configuration with SONET, VLAN, and port-channel . . . 470
Figure 171 define interface-range macro test command . . . 471
Figure 172 run interface-range macro test . . . 472
Figure 173 interface vlan Command Example . . . 473
Figure 174 monitor Command Example of a Single Interface . . . 477
Figure 175 monitor Command Example of All Interfaces on a Line Card . . . 477
Figure 176 negotiation auto master/slave example . . . 480
Figure 177 View auto negotiation master/slave setting (partial) . . . 481
Figure 178 portmode hybrid configuration example . . . 482
Figure 179 View the Tagged Hybrid Interface . . . 483
Figure 180 Unconfigure the hybrid port . . . 483
Figure 181 show config Command Example for the INTERFACE mode . . . 483
Figure 182 show config (Bulk Configuration) Command Example . . . 484
Figure 183 show interfaces Command Example (EtherScale) . . . 485
Figure 184 show interfaces Command Example (TeraScale) . . . 488
Figure 185 show interfaces description Command Example . . . 492
Figure 186 show interfaces status Command Example . . . 494
Figure 187 show interfaces switchport Command Example . . . 495
Figure 188 show range Command Example . . . 496
Figure 189 wanport command with shutdown command . . . 499
Figure 190 show interfaces port-channel Command Example . . . 503
Figure 191 show interfaces port-channel brief Command Example . . . 504
Figure 192 show port-channel-flow Command for MAC . . . 506
Figure 193 show port-channel-flow Command for TCP . . . 506
Figure 194 show tdr gigabitethernet Command Example . . . 509
Figure 195 Debug Output Example . . . 511
Figure 196 show ip udp-helper command Example . . . 513
Figure 197 show lacp *port-channel-number* command . . . 526
Figure 198 show lacp sys-id command Example . . . 526
Figure 199 show lacp counter command Example . . . 526
Figure 200 interface sonet Command Example . . . 534
Figure 201 show controllers sonet Command Example . . . 543
Figure 202 show controllers tengigabitethernet Command Example . . . 544
Figure 203 show interfaces sonet with PPP Encapsulation Command Example . . . 546
Figure 204 show protocol-tunnel command example . . . 553
Figure 205 show protocol-tunnel command example for a specific VLAN . . . 553
Figure 206 show mac-address-table . . . 565

Figure 207 show mac-address-table count . . . 565
Figure 208 show mac-address-table aging-time . . . 566
Figure 209 show mac accounting destination . . . 567
Figure 210 show mac cam . . . 568
Figure 211 show mac learning-limit . . . 569
Figure 212 show vlan . . . 571
Figure 213 show vlan brief . . . 572
Figure 214 clear frrp command examples . . . 576
Figure 215 show frrp summary command . . . 582
Figure 216 show frrp ring-id command . . . 582
Figure 217 show frrp ring-id summary command . . . 582
Figure 218 Configuring an FVRP Region Name Example . . . 587
Figure 219 show config Command Example . . . 595
Figure 220 show fvrp Command Example . . . 596
Figure 221 show fvrp region Command Example . . . 597
Figure 222 show vlan Command Example with VLAN-Stack VLANs . . . 601
Figure 223 vlan-stack protocol-type command example . . . 602
Figure 224 VLAN-Stack Tag . . . 602
Figure 225 ip access-list standard Command Example . . . 607
Figure 226 ip access-list extended Command Example . . . 626
Figure 227 show config Command Example . . . 646
Figure 228 show ip accounting access-lists Command Example (Partial) . . . 647
Figure 229 mac-access-list standard Command Example . . . 649
Figure 230 mac-access-list extended Command Example . . . 653
Figure 231 show mac accounting access-list Command Example . . . 658
Figure 232 show config Command Example . . . 662
Figure 233 show ip prefix-list detail Command Example . . . 663
Figure 234 show ip prefix-list summary Command Example . . . 663
Figure 235 route-map Command Example . . . 672
Figure 236 show config Command Example . . . 680
Figure 237 show route-map Command Example . . . 681
Figure 238 ip as-path access-list Command Example . . . 683
Figure 239 show config Command Example in AS-PATH ACL mode . . . 684
Figure 240 show ip as-path-access-lists Command Example . . . 685
Figure 241 ip community-list Command Example . . . 687
Figure 242 show config Command Example in COMMUNITY-LIST mode . . . 689
Figure 243 show ip community-lists Command Example . . . 689
Figure 244 ipv6 access-group Command Example . . . 700
Figure 245 show config Command Example . . . 711
Figure 246 show ipv6 accounting access-lists Command Example) . . . 712
Figure 247 show running-config acl Command Example . . . 713
Figure 248 route-map Command Example . . . 716
Figure 249 show config Command Example . . . 717

Figure 250 show route-map Command Example . . . 717
Figure 251 debug ip icmp Command Example (Partial) . . . 726
Figure 252 debug ip packet Command Example (Partial) . . . 727
Figure 253 show arp Command Example (Partial) . . . 748
Figure 254 show arp cpu cp Command Example . . . 748
Figure 255 show arp summary Command Example . . . 748
Figure 256 show hosts Command Example . . . 749
Figure 257 show ip cam Command Example . . . 751
Figure 258 show ip cam summary Command Example . . . 752
Figure 259 show ip fib linecard Command Example . . . 753
Figure 260 show ip flow Command . . . 755
Figure 261 show ip interface Command Example . . . 756
Figure 262 show ip interface brief Command Example (Partial) . . . 757
Figure 263 show ip management route Command Example . . . 758
Figure 264 show ip protocols Command Example . . . 758
Figure 265 show ip route all Command Example . . . 759
Figure 266 show ip route summary Command Example . . . 761
Figure 267 show ip traffic Command Example (partial) . . . 762
Figure 268 show tcp statistics cp Command Example . . . 766
Figure 269 show cam pbr interface vlan Command . . . 776
Figure 270 show cam pbr linecard 2 port-set 0 Command . . . 776
Figure 271 show ip redirect-list Command Example . . . 777
Figure 272 show fefd Command Example . . . 784
Figure 273 show config Command Example . . . 790
Figure 274 show vrrp brief Command Example . . . 791
Figure 275 show vrrp Command Example . . . 792
Figure 276 protocol spanning-tree . . . 800
Figure 277 show config command for the SPANNING TREE mode . . . 801
Figure 278 show spanning-tree . . . 802
Figure 279 show spanning-tree brief . . . 803
Figure 280 show spanning-tree pvst brief command . . . 807
Figure 281 show spanning-tree pvst vlan command . . . 808
Figure 282 show spanning-tree pvst command with EDS and LBK . . . 808
Figure 283 show spanning-tree pvst with EDS and PVID . . . 809
Figure 284 spanning-tree pvst command . . . 810
Figure 285 protocol spanning-tree rstp command . . . 819
Figure 286 show config command for the RSTP mode . . . 820
Figure 287 show spanning-tree rstp brief command . . . 821
Figure 288 show spanning-tree rstp with EDS and LBK . . . 821
Figure 289 spanning-tree rstp edge-port command . . . 823
Figure 290 protocol spanning-tree mstp . . . 831
Figure 291 show config command for the MULTIPLE SPANNING TREE mode . . . 832
Figure 292 show spanning-tree mst configuration . . . 832

Figure 293 show spanning-tree msti *instance-number* *834*
Figure 294 show spanning-tree msti with EDS and LBK 835
Figure 295 router rip Command Example 853
Figure 296 show config Command Example in ROUTER RIP Mode 854
Figure 297 show ip rip database Command Example (partial) 855
Figure 298 debug ip ospf Output 866
Figure 299 router-id Command Examples 886
Figure 300 router ospf Command Example 886
Figure 301 show config Command Example 887
Figure 302 show ip ospf Command Example 887
Figure 303 show ip ospf asbr Command Example 889
Figure 304 show ip ospf database Command Example 889
Figure 305 show ip ospf database asbr-summary Command Example (Partial) 891
Figure 306 show ip ospf database external Command Example 892
Figure 307 show ip ospf database network Command Example 894
Figure 308 show ip ospf database opaque-area Command Example (Partial) 896
Figure 309 show ip ospf database router Command Example (Partial) 899
Figure 310 show ip ospf database summary Command Example 901
Figure 311 show ip ospf interface Command Example 903
Figure 312 show ip ospf neighbor Command Example 904
Figure 313 show ip ospf route Command Example 905
Figure 314 show ip ospf statistics global Command Example 906
Figure 315 show ip ospf statistics Command Example 908
Figure 316 show ip ospf topology Command Example 909
Figure 317 show ip ospf virtual-links Command Example 910
Figure 318 debug ipv6 ospf packet Command Example 915
Figure 319 show ipv6 ospf database database-summary Command 924
Figure 320 show ipv6 ospf neighbor Command Example 926
Figure 321 show bfd neighbors Command 938
Figure 322 show bfd neighbors detail Command 938
Figure 323 redistribute bgp Command Example 973
Figure 324 show config Command Example 976
Figure 325 show isis database Command Example 977
Figure 326 show isis hostname Command Example 978
Figure 327 show isis interface Command Example (Partial) 979
Figure 328 show isis neighbors Command Example 980
Figure 329 show isis protocol Command Example 981
Figure 330 show isis traffic Command Example 982
Figure 331 show isis hostname Command Example 1016
Figure 332 show isis neighbors Command Example 1018
Figure 333 show isis protocol Command Example 1019
Figure 334 redistribute isis Command Example 1070
Figure 335 router bgp Command Example 1071

Figure 336 show capture bgp-pdu neighbor Command Example 1072
Figure 337 show config Command Example 1073
Figure 338 show ip bgp Command Example (Partial) 1074
Figure 339 show ip bgp cluster-list Command Example (Partial) 1075
Figure 340 show ip bgp community Command Example (Partial) 1077
Figure 341 show ip bgp community-list Command Example 1078
Figure 342 show ip bgp dampened-paths Command Example 1079
Figure 343 show ip bgp filter-list Command Example 1081
Figure 344 show ip bgp flap-statistics Command Example 1083
Figure 345 show ip bgp inconsistent-as Command Example (Partial) 1084
Figure 346 show ip bgp neighbors Command Example (Partial) 1086
Figure 347 show ip bgp neighbors advertised-routes Command Example 1086
Figure 348 show ip bgp neighbors received-routes Command Example 1087
Figure 349 show ip bgp neighbors denied-routes Command Example 1087
Figure 350 show ip bgp next-hop Command Example 1089
Figure 351 show ip bgp paths Command Example (Partial) 1090
Figure 352 show ip bgp paths as-path Command Example (partial) 1091
Figure 353 show ip bgp paths community Command Example (partial) 1092
Figure 354 show ip bgp peer-group Command Example (Partial) 1094
Figure 355 show ip bgp regexp Command Example (Partial) 1095
Figure 356 show ip bgp summary Command Example 1096
Figure 357 show ip bgp Command Example 1116
Figure 358 show ip bgp neighbors Command Example 1121
Figure 359 show ip bgp summary Command Example 1124
Figure 360 show config Command Example (Partial) 1177
Figure 361 show ip bgp next-hop Command Example 1184
Figure 362 show ip bgp peer-group Command Example 1186
Figure 363 show ip bgp summary Command Example 1188
Figure 364 show ip bgp ipv6 unicast Example 1207
Figure 365 show ip bgp ipv6 unicast detail Command Example (Partial) 1210
Figure 366 show ip bgp ipv6 unicast flap-statistics command Example 1212
Figure 367 show ip bgp ipv6 unicast neighbors Command Example (Partial) 1214
Figure 368 show ip bgp summary Command Example 1217
Figure 369 show interfaces rate limit Command Example 1224
Figure 370 show interfaces rate police Command Example 1225
Figure 371 show cam layer2-qos interface 1246
Figure 372 show cam layer2-qos linecard 1246
Figure 373 show cam layer3-qos linecard interface Command 1247
Figure 374 show cam layer3-qos linecard port-set Command 1248
Figure 375 show cam layer3-qos linecard interface Command without Trust 1248
Figure 376 show cam layer3-qos summary Command 1248
Figure 377 show qos class-map Command 1249
Figure 378 show qos policy-map detail (IPv4) Command 1250

Figure 379 show qos policy-map detail (IPv6) Command 1251
Figure 380 show qos policy-map summary (IPv4) Command 1251
Figure 381 show qos policy-map-input (IPv4) Command 1252
Figure 382 show qos policy-map-input (IPv6) Command 1252
Figure 383 show qos policy-map-output 1253
Figure 384 show qos qos-policy-input Command 1253
Figure 385 show qos qos-policy-output Command 1254
Figure 386 show qos statistics Command (ED and EE Series) 1255
Figure 387 show qos statistics Command (EFSeries) 1256
Figure 388 show qos statistics wred-profile Command (ED, EE, and EF Series) 1257
Figure 389 show qos wred-profile Command 1258
Figure 390 test cam-usage service-policy input policy-map linecard all Example Command . . . 1259
Figure 391 show queue statistics egress Command (TeraScale) 1267
Figure 392 show queue statistics egress multicast Command (EtherScale) 1268
Figure 393 show queue statistics egress brief Command 1269
Figure 394 show queue statistics ingress Command (EtherScale) Partial 1272
Figure 395 show queue statistics ingress Multicast Command (EtherScale) 1274
Figure 396 show queue statistics ingress brief Command 1275
Figure 397 show ip mroute static Command Example 1282
Figure 398 show ip mroute Command Example 1282
Figure 399 show ip rpf Command Example 1283
Figure 400 show ip igmp groups Command Example 1290
Figure 401 show ip igmp interface Command Example 1292
Figure 402 show ipv6 mroute command Example 1301
Figure 403 show ipv6 mroute active command Example 1302
Figure 404 show ipv6 mroute count group command Examples 1302
Figure 405 show ipv6 mroute count source command Examples 1302
Figure 406 show ipv6 mroute mld all command Example 1303
Figure 407 show ip pim bsr-router Command Example 1325
Figure 408 show ip pim interface Command Example 1325
Figure 409 show ip pim neighbor Command Example 1326
Figure 410 show ip pim rp mapping Command Example 1 1328
Figure 411 show ip pim rp mapping Command Example 2 1328
Figure 412 show ip pim rp group-address Command Example 3 1328
Figure 413 show ip pim tib Command Example 1329

List of Tables

Table 1 Information Symbols . . . 64
Table 2 Command Prompt and Corresponding Command Mode . . . 68
Table 3 Short-cut Keys and their Actions . . . 70
Table 4 Interface prompts . . . 73
Table 5 show file-systems Command Output Fields . . . 96
Table 6 show version Command Fields . . . 101
Table 7 show linecard Command Example Information . . . 141
Table 8 show linecard boot-information output definitions . . . 143
Table 9 show memory Command Example Information . . . 145
Table 10 show processes memory rp1/rp2 . . . 152
Table 11 show rpm Command Example Information . . . 154
Table 12 show sfm Command Output Fields . . . 156
Table 13 show ipv6 route Command Example Fields . . . 181
Table 14 IPv6 -Diffserv Mapping . . . 182
Table 15 show hardware rpm mac counters Output Description . . . 188
Table 16 show hardware rpm number mac Output Description . . . 196
Table 17 show processes ipc flow-control Display Definitions . . . 235
Table 18 show hardware rpm mac counters Command Example Information . . . 252
Table 19 Lines in show interfaces tengigabitethernet Command Example . . . 254
Table 20 Lines in show interfaces gigabitethernet Command Example . . . 255
Table 21 show redundancy Command Example Fields . . . 372
Table 22 show ntp associations Command Fields . . . 388
Table 23 show ntp status Command Example Information . . . 389
Table 24 show users Command Example Fields . . . 406
Table 25 Negotiated Flow Control Values . . . 463
Table 26 monitor Command Menu Options . . . 478
Table 27 Difference between Link MTU and IP MTU . . . 479
Table 28 Auto Negotiation and Link Speed Combinations . . . 481
Table 29 Lines in show interfaces Command Example (EtherScale) . . . 486
Table 30 Lines in show interfaces Command Example (TeraScale) . . . 488
Table 31 show interfaces description Command Example Fields . . . 493
Table 32 Items in show interfaces switchport Command Example . . . 496
Table 33 show interfaces port-channel Command Example Fields . . . 503
Table 34 show interfaces port-channel brief Command Example Fields . . . 504

Table 35 TDR Test Status . . . 509
Table 36 LACP Modes . . . 525
Table 37 Alarm Definitions . . . 529
Table 38 Lines in show controllers interface Command Example . . . 544
Table 39 Fields in the show interfaces sonet with PPP Encapsulation . . . 546
Table 40 show mac-address-table Information . . . 565
Table 41 show mac-address-table count Information . . . 565
Table 42 show mac cam Information . . . 568
Table 43 show vlan Information . . . 571
Table 44 show frvp Command Example Fields . . . 596
Table 45 ICMP Message Type Keywords . . . 619
Table 46 show ip accounting access-lists Command Example Field . . . 647
Table 47 ICMP Message Type Keywords . . . 694
Table 48 show ip accounting access-lists Command Example Field . . . 712
Table 49 debug ip packet Command Example Fields . . . 728
Table 50 Difference between Link MTU and IP MTU . . . 738
Table 51 Configurations of the load-balance Command . . . 745
Table 52 show arp Command Example Fields . . . 748
Table 53 show arp summary Command Example Fields . . . 749
Table 54 show hosts Command Example Fields . . . 749
Table 55 show ip cam Command Example Fields . . . 751
Table 56 show ip cam summary Command Example Fields . . . 752
Table 57 show ip fib linecard Command Example Fields . . . 753
Table 58 show ip interface Command Example Items . . . 756
Table 59 show ip interface brief Column Headings . . . 757
Table 60 show ip route all Command Example Fields . . . 760
Table 61 show ip route summary Column Headings . . . 761
Table 62 show ip traffic output definitions . . . 763
Table 63 F10 Monitoring MIB . . . 763
Table 64 show tcp statistics cp Command Example Fields . . . 766
Table 65 show fefd display details . . . 784
Table 66 show vrrp brief Command Example Items . . . 791
Table 67 show vrrp Command Example Items . . . 792
Table 68 Fields in show ip rip database Command Output . . . 855
Table 69 debug ip ospf Output Fields . . . 866
Table 70 show ip ospf Command Example . . . 888
Table 71 show ip ospf database Command Example Fields . . . 890
Table 72 show ip ospf database asbr-summary Command Example fields . . . 891
Table 73 show ip ospf database external Command Example Fields . . . 893
Table 74 show ip ospf database network Command Example fields . . . 895
Table 75 show ip ospf database opaque-area Command Example Fields . . . 897
Table 76 show ip ospf database router Command Example Fields . . . 899
Table 77 show ip ospf database summary Command Example Fields . . . 901

Table 78 show ip ospf interface Command Example Fields . . . 903
Table 79 show ip ospf neighbor Command Example Fields . . . 904
Table 80 show ip ospf statistics global Command Example Fields . . . 907
Table 81 show ip ospf statistics global Error Definitions . . . 907
Table 82 show ip ospf virtual-links Command Example Fields . . . 910
Table 83 debug ip ospf Output Fields . . . 915
Table 84 show isis database Command Example Fields . . . 977
Table 85 show isis neighbors Command Example Fields . . . 980
Table 86 show isis traffic Command Example Fields . . . 982
Table 87 show isis neighbors Command Example Fields . . . 1018
Table 88 show ip bgp Command Example Fields . . . 1074
Table 89 show ip bgp cluster-list Command Fields . . . 1075
Table 90 show ip bgp community Command Example Fields . . . 1077
Table 91 show ip bgp community-list Command Example Fields . . . 1078
Table 92 show ip bgp dampened-paths Command Example . . . 1079
Table 93 show ip bgp filter-list Command Fields . . . 1082
Table 94 show ip bgp flap-statistics Command Example Fields . . . 1083
Table 95 show ip bgp inconsistent-as Command Example Fields . . . 1084
Table 96 show ip bgp neighbors Command Fields . . . 1087
Table 97 show ip bgp next-hop Command Fields . . . 1089
Table 98 show ip bgp paths Command Fields . . . 1090
Table 99 show ip bgp paths community Command Fields . . . 1091
Table 100 show ip bgp paths community Command Fields . . . 1093
Table 101 show ip bgp peer-group Command Fields . . . 1094
Table 102 show ip bgp regexp Command Example Fields . . . 1096
Table 103 show ip bgp summary Command Fields . . . 1097
Table 104 show ip bgp Command Example Fields . . . 1116
Table 105 show ip bgp neighbors Command Fields . . . 1122
Table 106 show ip bgp summary Command Fields . . . 1124
Table 107 show ip bgp Command Example Fields . . . 1207
Table 108 show ip bgp neighbors Command Fields . . . 1215
Table 109 show ip bgp summary Command Fields . . . 1217
Table 110 show interfaces Command Example Fields . . . 1225
Table 111 show interfaces police Command Example Fields . . . 1225
Table 112 show qos statistics Command Example Fields (ED and EE Series) . . . 1255
Table 113 show qos statistics Command Example Fields (EF Series) . . . 1256
Table 114 show qos statistics wred-profile Command Example Fields (ED, EE, and EF Series) 1257
Table 115 test cam-usage Command Example Fields . . . 1259
Table 116 Pre-defined WRED Profile Threshold Values . . . 1260
Table 117 Standard Default DSCP Mapping Table . . . 1262
Table 118 Numbering Conventions for show queue egress statistics Output . . . 1267
Table 119 show queue statistics egress Command Fields . . . 1267
Table 120 show queue statistics egress multicast Command Fields . . . 1268

Table 121 show queue statistics egress brief Command Fields 1269
Table 122 Numbering Conventions for show queue statistics ingress Output 1271
Table 123 show queue statistics Command Fields 1273
Table 124 show queue statistics ingress Multicast Command Fields 1274
Table 125 show queue statistics ingress brief Command Fields 1275
Table 126 show ip mroute Command Example Fields 1283
Table 127 show ip igmp groups Command Example Fields 1291
Table 128 show ip pim interface Command Example Fields 1325
Table 129 show ip pim neighbor Command Example Fields 1327
Table 130 show ip pim tib Command Example Fields 1329

Preface About this Guide

This document provides information on the FTOS Command Line Interface (CLI). It includes some information on the protocols and features found in FTOS and on the E-Series. This chapter includes:

- Objectives on page 63
- Audience on page 63
- Conventions on page 63
- Related Documents on page 65

Objectives

This document is intended as a reference guide for the FTOS command line interface (CLI) commands, with detailed syntax statements, along with usage information and sample output.

For details on when to use the commands, refer to the *FTOS Configuration Guide*. Appendix G in that guide contains a list of the RFCs and MIBs (management information base files) supported in E-Series systems. Also, syntax statements in this guide and related instructions in that guide cite the relevant RFCs.

Audience

This document is intended for system administrators who are responsible for configuring or maintaining networks. This guide assumes you are knowledgeable in Layer 2 and Layer 3 networking technologies.

Conventions

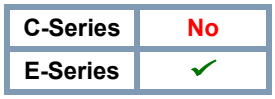
This document uses the following conventions to describe command syntax:

Convention	Description
keyword	Keywords are in bold and should be entered in the CLI as listed.
parameter	Parameters are in italics and require a number or word to be entered in the CLI.
{X}	Keywords and parameters within braces must be entered in the CLI.
[X]	Keywords and parameters within brackets are optional.
x | y	Keywords and parameters separated by bar require you to choose one.

Information Symbols

Table 1 describes symbols contained in this guide.

Table 1 Information Symbols

Symbol	Warning	Description
	Danger	This symbol warns you that improper handling and installation could result in bodily injury. Before you work on this equipment, be aware of electrical hazards and take appropriate safety precautions.
	Caution	This symbol informs you that improper handling and installation could result in equipment damage or loss of data.
	Warning	This symbol informs you that improper handling could reduce your component or system performance.
	Note	This symbol informs you of important operational information.
	C-Series Only	This symbol informs you that a major feature or protocol is supported on the C-Series only.
	C-Series Only	This symbol informs you that a command is supported on the C-Series only.
	E-Series Only	This symbol informs you that a major feature or protocol is supported on the E-Series only.
	E-Series Only	This symbol informs you that a command is supported on the E-Series only.

Related Documents

For more information about the system, refer to the following documents:

- *FTOS Configuration Guide*
- *Installing and Maintaining the E-1200 System*
- *Installing and Maintaining the E-600 System*
- *Installing and Maintaining the E-600i System*
- *Installing and Maintaining the E-300 System*
- *Installing and Maintaining the C-300 System*
- *Release Notes for the E-Series and FTOS*

Chapter 1 CLI Basics

This chapter describes the command structure and command modes. FTOS commands are a text-based interface that allows you to use launch commands, change the command modes, and configure interfaces and protocols.

This chapter covers the following topics:

- Accessing the Command Line on page 67
- Navigating the Command Line on page 68
- Obtaining Help on page 69
- Using the Keyword No on page 71
- Filtering show Commands on page 71
- Command Modes on page 72
- Determining the Chassis Mode on page 79

Accessing the Command Line

When the E-Series successfully boots, you enter the command line in the EXEC mode and *not* prompted to log in. You can access the E-Series commands through a serial console port or a Telnet session. When you Telnet into the E-Series, you are prompted to enter a login name and password.

Figure 1 is an example of a successful Telnet login session.

```
telnet 172.31.1.53
Trying 172.31.1.53...
Connected to 172.31.1.53.
Escape character is '^]'.
Login: username
Password:
Force10>
```

Figure 1 Login Example

Once you log into the E-Series, the prompt provides you with current command-level information (refer to Table 2).

Multiple Configuration Users

When a user enters the CONFIGURATION mode and another user(s) is already in that configuration mode, FTOS generates the following alert warning message:

```
Force10#conf

% Warning: The following users are currently configuring the system:

User "" on line console0
User "admin" on line vty0 ( 123.12.1.123 )
User "admin" on line vty1 ( 123.12.1.123 )
User "Irene" on line vty3 ( 123.12.1.321 )

Force10(conf)#Force10#
```

Figure 2 Configuration Mode User Alert

When another user enters the configuration mode, for example “admin” on vty2, FTOS sends a message:

```
% Warning: User "admin" on line vty2 "172.16.1.210" is in configuration
```

Navigating the Command Line

The command line prompt changes as you move up and down the levels of the command structure. Table 2 lists the current prompts and their corresponding command levels. Starting with the Configuration mode, the command prompt adds the appropriate modifier to further identify the mode. The FTOS command modes are explained in the Command Modes section.

Table 2 Command Prompt and Corresponding Command Mode

Prompt	CLI Command Mode
Force10>	EXEC
Force10#	EXEC privilege
Force10(conf)#	CONFIGURATION
Force10(conf-if)# Force10(conf-if-gi-0/0)# Force10(conf-if-te-0/0)# Force10(conf-if-lo-0)# Force10(conf-if-nu-0)# Force10(conf-if-po-0)# Force10(conf-if-vl-0)# Force10(conf-if-so-0/0)# Force10(conf-if-ma-0/0)# Force10(conf-if-range)#	INTERFACE

Table 2 Command Prompt and Corresponding Command Mode (continued)

Prompt	CLI Command Mode
Force10(config-line-aux)# Force10(config-line-console)# Force10(config-line-vty)#	LINE
Force10(config-span)#	STP
Force10(config-mstp)#	MULTIPLE SPANNING TREE
Force10(config-pvst)#	Per-VLAN SPANNING TREE Plus
Force10(config-rstp)#	RAPID SPANNING TREE
Force10(config-fvrp)#	PROTOCOL FVRP
Force10(config-ext-macl)# Force10(config-std-macl)#	MAC ACCESS LIST
Force10(config-ext-nacl)# Force10(config-std-nacl)#	IP ACCESS LIST
Force10(config-route-map)#	ROUTE-MAP
Force10(conf-nprefixl)#	PREFIX-LIST
Force10(conf-trace-acl)#	TRACE-LIST
Force10(conf-router_rip)#	ROUTER RIP
Force10(conf-redirect-list)#	REDIRECT
Force10(conf-router_ospf)#	ROUTER OSPF
Force10(conf-router_isis)#	ROUTER ISIS
Force10(conf-router_bgp)#	ROUTER BGP

Obtaining Help

As soon as you are in a command mode there are several ways to access help.

- To obtain a list of keywords at any command mode, do the following:

  Enter a **?** at the prompt or after a keyword. There must always be a space before the **?**.

- To obtain a list of keywords with a brief functional description, do the following:

  Enter **help** at the prompt.

- To obtain a list of available options, do the following:

  Type a keyword followed by a space and a **?**

- Type a partial keyword followed by a **?**

  A display of keywords beginning with the partial keyword is listed.

Figure 3 illustrates the results of entering **ip ?** at the prompt.

```
Force10(conf)#ip ?
access-list             Named access-list
as-path                 BGP autonomous system path filter
community-list          Add a community list entry
domain-list             Domain name to complete unqualified host name
domain-lookup           Enable IP Domain Name System hostname translation
domain-name             Define the default domain name
fib                     FIB configuration commands
ftp                     FTP configuration commands
host                    Add an entry to the ip hostname table
max-frag-count          Max. fragmented packets allowed in IP re-assembly
multicast-routing       Enable IP multicast forwarding
name-server             Specify addess of name server to use
pim                     Protocol Independent Multicast
prefix-list             Build a prefix list
radius                  Interface configuration for RADIUS
redirect-list           Named redirect-list
route                   Establish static routes
scp                     SCP configuration commands
source-route            Process packets with source routing header options
ssh                     SSH configuration commands
tacacs                  Interface configuration for TACACS+
telnet                  Specify telnet options
tftp                    TFTP configuration commands
trace-group             Named trace-list
trace-list              Named trace-list
Force10(conf)#ip
```

Figure 3 Partial Keyword Example

When entering commands, you can take advantage of the following timesaving features:

- The commands are not case sensitive.
- You can enter partial (truncated) command keywords. For example, you can type **conf** for the **configure terminal** command.
- Use the TAB key to complete keywords in commands.
- Use the up arrow key to display the last enabled command.
- Use either the Backspace key or the Delete (Del) key to erase the previous character.

Use the left and right arrow keys to navigate left or right in the FTOS command line. Table 3 defines the key combinations valid at the FTOS command line.

Table 3 Short-cut Keys and their Actions

Key Combinations	Action
CNTL-A	Moves the cursor to the beginning of the command line.
CNTL-B	Moves the cursor back one character.
CNTL-D	Deletes character at cursor.
CNTL-E	Moves the cursor to the end of the line.
CNTL-F	Moves the cursor forward one character.

Table 3 Short-cut Keys and their Actions (continued)

Key Combinations	Action
CNTL-I	Completes a keyword.
CNTL-K	Deletes all characters from the cursor to the end of the command line.
CNTL-L	Re-enters the previous command.
CNTL-N	Return to more recent commands in the history buffer after recalling commands with Ctrl-P or the up arrow key
CNTL-P	Recalls commands, beginning with the last command
CNTL-R	Re-enters the previous command.
CNTL-U	Deletes the line.
CNTL-W	Deletes the previous word.
CNTL-X	Deletes the line.
CNTL-Z	Ends continuous scrolling of command outputs.
Esc B	Moves the cursor back one word.
Esc F	Moves the cursor forward one word.
Esc D	Deletes all characters from the cursor to the end of the word.

Using the Keyword No

To disable, delete, or return to default values, use the no form of the commands. For most commands, if you type the keyword **no** in front of the command, you will disable that command or delete it from the running configuration. In this document, the no form of the command is discussed in the Command Syntax portion of the command description.

Filtering show Commands

You can filter the display output of a show command to find specific information, to display certain information only, or to begin the command output at the first instance of a regular expression or phrase.

After you execute the show command, add a pipe (|) followed by one of the parameters listed below and a regular expression, the resulting output either excludes or includes those parameters.

- **display** — display additional configuration information
- **except**— display only text that does not match the pattern (or regular expression)

- **find** — search for the first occurrence of a pattern
- **grep** — display text that matches a pattern
- **no-more** — do not paginate the display output

Note: FTOS accepts a space before or after the pipe, no space before or after the pipe, or any combination. For example:

Force10#*command*|grep gigabit |**except** *regular-expression* | **find** *regular-expression*

Displaying All Output

To display the output all at once (not one screen at a time), use the **no-more** after the pipe. This is similar to the **terminal length** *screen-length* command except that the **no-more** option affects the output of just the specified command.For example:

```
Force10#show running-config|no-more
```

Filtering Command Output Multiple Times

You can filter a single command output multiple times. For example:

Force10# *command* | **grep** *regular-expression* | **except** *regular-expression* | **grep** *other-regular-expression* | **find** *regular-expression* | **no-more**

Command Modes

To navigate to various CLI modes, you need to use specific commands to launch each mode. Navigation to these modes is discussed in the following sections.

EXEC Mode

When you initially log in to the E-Series, by default, you are logged into the EXEC mode. This mode allows you to view settings and to enter the EXEC privilege mode to configure the device. The > prompt is displayed while you are logged into the EXEC mode.

The launch command to enter EXEC privilege mode is **enable**. When you use the **enable** command you must provide a password.

EXEC Privilege Mode

The EXEC privilege mode allows you to access all interface and other settings also accessible in EXEC mode, and to clear ARP entries and IP addresses. In addition, you can configure interfaces, routes, and protocols on the E-Series. While you are logged in to the EXEC privilege mode, the # prompt is displayed.

CONFIGURATION Mode

While in the EXEC privilege mode, use the **configure** command to enter the CONFIGURATION mode and configure interfaces and routing protocols.

To enter the CONFIGURATION mode:

1. Verify that you are logged in to the EXEC privilege mode.
2. Enter the **configure** command. The prompt changes to include (conf).

From this mode, you can enter INTERFACE by using the **interface** command.

INTERFACE Mode

While in the CONFIGURATION mode, use the **interface** command to enter the INTERFACE and configure interfaces or IP services on those interfaces. An interface can be physical (for example, a Gigabit Ethernet port) or virtual (for example, the Null interface).

To enter INTERFACE mode:

1. Verify that you are logged into the CONFIGURATION mode.
2. Enter the **interface** command. You must include an interface type and number that is available on the E-Series.The prompt changes to include the interface and port/slot/number as outline in Table 4.

Table 4 Interface prompts

Prompt	Interface Type
Force10(conf-if)#	INTERFACE Mode
Force10(conf-if-gi-0/0)#	Gigabit Ethernet Interface followed by slot/port information.
Force10(conf-if-te-0/0)#	Ten Gigabit Ethernet Interface followed by slot/port information.
Force10(conf-if-lo-0)#	Loopback Interface number. Range 0 to 16833
Force10(conf-if-nu-0)#	Null Interface followed by zero
Force10(conf-if-po-0)#	Port-channel Interface number. Range 1 to 255 TeraScale; Range 1 to 32 EtherScale
Force10(conf-if-vl-0)#	VLAN Interface followed by VLAN identifier. Range 1 to 4094.
Force10(conf-if-so-0/0)#	SONET Interface followed by slot/port information.
Force10(conf-if-ma-0/0)#	Management Ethernet Interface followed by slot/port information.
Force10(conf-if-range)#	Configure Interface Range for bulk configuration (see interface range).

LINE Mode

While in the CONFIGURATION mode, use the **line** command to enter the LINE mode and configure the console or virtual terminals.

To enter LINE mode:

1. Verify that you are logged in to the CONFIGURATION mode.
2. Enter the **line** command. You must include the keywords console or vty and their line number available on the E-Series.The prompt changes to include (config-line-console) or (config-line-vty).

You can exit this mode by using the **exit** command.

TRACE-LIST Mode

When in the CONFIGURATION mode, use the trace-list command to enter the TRACE-LIST mode and configure a Trace list.

1. Verify that you are logged in to the CONFIGURATION mode.
2. Enter the **ip trace-list** command. You must include the name of the Trace list. The prompt change to include (conf-trace-acl).

You can exit this mode by using the **exit** command.

MAC ACCESS LIST Mode

While in the CONFIGURATION mode, use the **mac access-list standard** or **mac access-list extended** command to enter the MAC ACCESS LIST mode and configure either standard or extended access control lists (ACL).

To enter MAC ACCESS LIST mode:

1. Verify that you are logged in to the CONFIGURATION mode.
2. Use the **mac access-list standard** or **mac access-list extended** command. You must include a name for the ACL.The prompt changes to include (conf-std-macl) or (conf-ext-macl).

You can return to the CONFIGURATION mode by entering the **exit** command.

IP ACCESS LIST Mode

While in the CONFIGURATION mode, use the **ip access-list standard** or **ip access-list extended** command to enter the IP ACCESS LIST mode and configure either standard or extended access control lists (ACL).

To enter IP ACCESS LIST mode:

1. Verify that you are logged in to the CONFIGURATION mode.
2. Use the **ip access-list standard** or **ip access-list extended** command. You must include a name for the ACL.The prompt changes to include (conf-std-nacl) or (conf-ext-nacl).

You can return to the CONFIGURATION mode by entering the **exit** command.

ROUTE-MAP Mode

While in the CONFIGURATION mode, use the **route-map** command to enter the ROUTE-MAP mode and configure a route map.

To enter ROUTE-MAP mode:

1. Verify that you are logged in to the CONFIGURATION mode.
2. Use the **route-map** *map-name* [**permit** | **deny**] [*sequence-number*] command. The prompt changes to include (route-map).

You can return to the CONFIGURATION mode by entering the **exit** command.

PREFIX-LIST Mode

While in the CONFIGURATION mode, use the **ip prefix-list** command to enter the PREFIX-LIST mode and configure a prefix list.

To enter PREFIX-LIST mode:

1. Verify that you are logged in to the CONFIGURATION mode.
2. Enter the **ip prefix-list** command. You must include a name for the prefix list.The prompt changes to include (conf-nprefixl).

You can return to the CONFIGURATION mode by entering the **exit** command.

AS-PATH ACL Mode

While in the CONFIGURATION mode, use the **ip as-path access-list** command to enter the AS-PATH ACL mode and configure an AS-PATH ACL.

To enter AS-PATH ACL mode:

1. Verify that you are logged in to the CONFIGURATION mode.
2. Enter the **ip as-path access-list** command. You must include a name for the AS-PATH ACL.The prompt changes to include (config-as-path).

You can return to the CONFIGURATION mode by entering the **exit** command.

IP COMMUNITY LIST Mode

While in the CONFIGURATION mode, use the **ip community-list** command to enter the IP COMMUNITY LIST mode and configure a Community list.

To enter IP COMMUNITY LIST mode:

1. Verify that you are logged in to the CONFIGURATION mode.
2. Enter the **ip community-list** command. You must include a name for the Community list.The prompt changes to include (config-community-list).

You can return to the CONFIGURATION mode by entering the **exit** command.

REDIRECT-LIST Mode

While in the CONFIGURATION mode, use the **ip redirect-list** command to enter the REDIRECT-LIST mode and configure a Redirect list.

To enter REDIRECT-LIST mode:

1. Verify that you are logged in to the CONFIGURATION mode.
2. Use the **ip redirect-list** command. You must include a name for the Redirect-list.The prompt changes to include (conf-redirect-list).

You can return to the CONFIGURATION mode by entering the **exit** command.

SPANNING TREE Mode

Use the protocol spanning-tree command to enter the STP mode and enable and configure Spanning Tree protocol.

To enter STP mode:

1. Verify that you are logged into the CONFIGURATION mode.
2. Enter the **protocol spanning-tree** *stp-id* command.

You can return to the CONFIGURATION mode by entering the **exit** command.

Per-VLAN SPANNING TREE Plus Mode

Use the protocol spanning-tree command to enter the PVST+ mode and enable and configure Per-VLAN Spanning Tree protocol.

Note: The protocol is PVST+, however the plus sign is dropped at the command line prompt.

To enter PVST+ mode:

1. Verify that you are logged into the CONFIGURATION mode.
2. Enter the **protocol spanning-tree pvst** command.

You can return to the CONFIGURATION mode by entering the **exit** command.

RAPID SPANNING TREE Mode

Use the protocol spanning-tree command to enter the RSTP mode and enable and configure the Rapid Spanning Tree protocol.

To enter RSTP mode:

1. Verify that you are logged into the CONFIGURATION mode.
2. Enter the **protocol spanning-tree rstp** command.

You can return to the CONFIGURATION mode by entering the **exit** command.

MULTIPLE SPANNING TREE Mode

Use the protocol spanning-tree mstp command to enter the MULTIPLE SPANNING TREE mode and enable and configure Multiple Spanning Tree protocol.

To enter MULTIPLE SPANNING TREE mode:

1. Verify that you are logged into the CONFIGURATION mode.
2. Enter the **protocol spanning-tree mstp** command.

You can return to the CONFIGURATION mode by entering the **exit** command.

PROTOCOL FVRP Mode

Use the **protocol fvrp** command to enter the PROTOCOL FVRP mode and enable Force10 VLAN Redundancy Protocol (FVRP) globally on the E-Series.

To enter the PROTOCOL FVRP mode:

1. Verify that you are logged into the CONFIGURATION mode.
2. Enter the **protocol fvrp** command.

You can return to the CONFIGURATION mode by entering the **exit** command. To configure FVRP on an interface, you change to that interface by using the **interface** *interface* command.

ROUTER OSPF Mode

Use the **router ospf** command to enter the ROUTER OSPF mode and configure OSPF on the E-Series.

To enter ROUTER OSPF:

1. Verify that you are logged into the CONFIGURATION mode.
2. Use the **router ospf** {*process-id*} command.The prompt changes to include (conf-router_ospf).

You can switch to the INTERFACE mode by using the **interface** command or you can switch to the ROUTER RIP mode by using the **router rip** command.

ROUTER RIP Mode

Use the **router rip** command to enter the ROUTER RIP mode and configure RIP on the E-Series.

To enter ROUTER RIP:

1. Verify that you are logged into the CONFIGURATION mode.

2. Enter the **router rip** command.The prompt changes to include (conf-router_rip).

You can switch to the INTERFACE mode by using the **interface** command or you can switch to the ROUTER OSPF mode by using the **router ospf** command.

ROUTER ISIS Mode

Use the **router isis** command to enter the ROUTER ISIS mode and configure ISIS on the E-Series.

To enter ROUTER ISIS:

1. Verify that you are logged into the CONFIGURATION mode.
2. Enter the **router isis** [*tag*] command.The prompt changes to include (conf-router_isis).

You can switch to the INTERFACE mode by using the **interface** command or you can switch to the ROUTER RIP mode by using the **router rip** command.

ROUTER BGP Mode

Use the **router bgp** command to enter the ROUTER BGP mode and configure BGP on the E-Series.

To enter ROUTER BGP:

1. Verify that you are logged into the CONFIGURATION mode.
2. Enter the **router bgp** *as-number* command.The prompt changes to include (conf-router_bgp).

You can return to the CONFIGURATION mode by entering the **exit** command.

Determining the Chassis Mode

The chassis mode in FTOS determines which hardware is being supported in a chassis. The chassis mode is programmed into an EEPROM on the backplane of the chassis and the change takes place only after the chassis is rebooted. Configuring the appropriate chassis mode enables the system to use all the ports on the card and recognize all software features.

For more information on the command, see the *FTOS Configuration Guide*.

Chapter 2 File Management Commands

This chapter contains commands needed to manage the configuration files and includes other file management commands found in the FTOS. The commands included are:

- boot config on page 82
- boot host on page 82
- boot network on page 83
- boot system on page 84
- boot system gateway on page 85
- cd on page 85
- change bootflash-image on page 85
- copy on page 86
- copy (Streamline Upgrade) on page 87
- copy running-config startup-config duplicate on page 88
- delete on page 88
- dir on page 89
- download alt-boot-image on page 89
- download alt-full-image on page 90
- download alt-system-image on page 90
- format on page 91
- logging kernel-coredump on page 91
- logging kernel-coredump server on page 93
- pwd on page 93
- rename on page 94
- show bootvar on page 94
- show file on page 95
- show file-systems on page 96
- show os-version on page 97
- show running-config on page 98
- show version on page 100
- show startup-config on page 102
- upgrade on page 103

boot config

Allows you to set the location of the configuration files on local device.

Syntax **boot config** {**remote-first** | **rpm0** *file-url* | **rpm1** *file-url*}

To return to the default setting, enter **no boot config** {**remote-first** | **rpm0** | **rpm1**}.

Parameters

remote-first	Enter the keywords **remote-first** to attempt to load the boot configuration files from a remote location.
rpm0	Enter the keywords **rpm0** first to specify the local boot configuration file for RPM 0.
rpm1	Enter the keywords **rpm1** first to specify the local boot configuration file for RPM 1.
file-url	Enter the location information: • For a file on the internal Flash, enter **flash://** followed by the filename. • For a file on the external Flash, enter **slot0://** followed by the filename.

Defaults Not configured.

Command Modes CONFIGURATION

Usage Information To view these changes in the show bootvar command output, you must save the running configuration to the startup configuration (using the copy command).

Related Commands

boot host	Set the location of the configuration file from remote host.
boot network	Set the location of the configuration file from the remote network.

boot host

Set the location of the configuration file from a remote host.

Syntax **boot host** {**primary** | **secondary**} *remote-url*

To return to the default settings, enter **no boot host** {**primary** | **secondary**} command.

Parameters

primary	Enter the keywords **primary** to attempt to load the primary host configuration files.
secondary	Enter the keywords **secondary** to attempt to load the secondary host configuration files.
remote-url	Enter the following location keywords and information: • For a file on an FTP server, enter **ftp://***user:password@hostip/filepath* • For a file on a TFTP server, enter **tftp://***hostip/filepath*

Defaults Not configured.

Command Modes CONFIGURATION

Usage Information To view these changes in the show bootvar command output, you must save the running configuration to the startup configuration (using the copy command).

Related Commands

boot config	Set the location of boot config files in the local device.
boot network	Set the location of the configuration file in a remote network.

boot network

Set the location of the configuration file in a remote network.

Syntax **boot network** {**primary** | **secondary**} *remote-url*

To return to the default settings, enter **no boot network** {**primary** | **secondary**} command.

Parameters

primary	Enter the keywords **primary** to attempt to load the primary network configuration files.
secondary	Enter the keywords **secondary** to attempt to load the secondary network configuration files.
remote-url	Enter the following location keywords and information: • For a file on an FTP server, enter **ftp://***user:password@hostip/filepath* • For a file on a TFTP server, enter **tftp://***hostip/filepath*

Defaults None

Command Modes CONFIGURATION

Usage Information

To view these changes in the show bootvar command output, you must save the running configuration to the startup configuration (using the copy command).

Related Commands

boot config	Set the location of boot config files in the local device.
boot host	Set the location of configuration files from a remote host.

boot system

Allows you to set the location of the FTOS image files.

Syntax

boot system {**rpm0** | **rpm1**} (**default** | **primary** | **secondary**} *file-url*

To return to the default boot sequence, use the **no boot system** {**rpm0** | **rpm1**} {**primary** | **secondary**} command.

Parameters

rpm0	Enter the keywords **rpm0** to attempt to load the boot parameters on RPM0.
rpm1	Enter the keywords **rpm1** to attempt to load the boot parameters on RPM1.
default	Enter the keyword **default** to attempt to load the default boot parameters.
primary	Enter the keywords **primary** to attempt to load the primary boot parameters.
secondary	Enter the keywords **secondary** to attempt to load the secondary boot parameters.
file-url	Enter the following location keywords and information: • From a file on the internal Flash, enter **flash://** followed by the filename. • From a file on an FTP server, enter **ftp://***user:password@hostip/filepath* • From a file on the external Flash, enter **slot0://** followed by the filename. • From a file on a TFTP server, enter **tftp://***hostip/filepath*

Defaults

Not configured.

Command Modes

CONFIGURATION

Usage Information

To view these changes in the show bootvar command output, you must save the running configuration to the startup configuration (using the copy command) and reload system.

boot system gateway

Allows you to specify a gateway IP address.

Syntax **boot system gateway** *ip-address*

To delete a gateway configuration, enter **no boot system gateway**.

Parameters

ip-address	Enter an IP address in dotted decimal format.

Command Modes CONFIGURATION

cd

Allows you to change to a different working directory.

Syntax **cd** *directory*

Parameters

directory	(OPTONAL) Enter one of the following: • **flash:** (internal Flash) or any sub-directory • **slot0:** (external Flash) or any sub-directory

Command Modes EXEC privilege

change bootflash-image

Change boot flash image to boot from.

Syntax **change bootflash-image** {**cp** | **linecard** *linecard-slot* | **rp**}

Parameters

cp	Enter the keyword **cp** to change the bootflash image on the Control Processor on the RPM.

linecard *linecard-slot*	Enter the keyword **linecard** followed by the slot number to change the bootflash image on a specific line card. C-Series Range: 0-7 on the C300 E-Series Range: 0 to 13 on the E1200; 0 on 6 for E600, and 0 to 5 on the E300.
rp	Enter the keyword **rp** to change the bootflash image on the RPM Route Processor.

Defaults Not configured.

Command Modes EXEC privilege

Usage Information A system message appears stating that the bootflash image has been changed. You must reload the system before the system can switch to the new bootflash image.

copy

Allows you to copy one file to another location.

Syntax **copy** *file-url file-url*

Parameters

file-url	Enter the following location keywords and information: • To copy a file on the internal FLASH, enter **flash://** followed by the filename. • To copy a file on an FTP server, enter **ftp://***user:password@hostip/filepath* • To copy a file on the internal FLASH on RPM0, enter **rpm0flash://***filepath* • To copy a file on the external FLASH on RPM0, enter **rpm0slot0://***filepath* • To copy a file on the internal FLASH on RPM1, enter **rpm1flash:/**/*filepath* • To copy a file on the external FLASH on RPM1, enter **rpm1slot0://***filepath* • To copy the running configuration, enter the keyword **running-config**. • To copy the startup configuration, enter the keyword **startup-config**. • To copy using secure copy client, enter the keyword **scp://** *userid:password@hostip/filepath*. • To copy a file on the external FLASH, enter **slot0://** followed by the filename. • To copy a file on a TFTP server, enter **tftp://***hostip/filepath*

Command Modes EXEC privilege

Usage Information When copying a file to a remote location (for example, using SCP client), you may enter only the keywords and the FTOS prompts you for the rest of the information.

FTOS supports a maximum of 100 files, at the root directory level, on both the internal and external Flash.

When you use the **copy running-config startup-config** command to copy the running configuration to the startup configuration, FTOS creates a backup file on the internal flash of the startup configuration.

```
Force10#copy running-config scp:/
Address or name of remote host []? 101.1.1.1
Destination file name [startup-config]? old_running
User name to login remote host? sburgess
Password to login remote host? dilling
```

Figure 4 copy running-config scp: Command Example

Related Commands

copy running-config startup-config duplicate	Change working directory.

copy (Streamline Upgrade)

Copy a system image to a local file and update the boot profile.

Syntax **copy** *source-url target-url* [**boot-image [synchronize-rpm [external]]]**

Parameters

source-url	Enter the source file in url format. The source file is a valid Force10 release image. Image validation is automatic.
target-url	Enter the local target file in url format.
boot-image	Enter the keyword **boot-image** to designate this copy command as a streamline update.
synchronize-rpm	Enter the keyword **synchronize-rpm** to copy the new image file to the peer RPM**.**
external	Enter the keyword **external** to designate the target device on the peer RPM as external flash (instead of the default internal flash). Default: Internal Flash

Defaults No default behavior

Command Modes CONFIGURATION

Command History

Version 6.1.1.0	Introduced

Usage Information In this streamline copy command, the source image is copied to the primary RPM and then, if specified, to the standby RPM. After the copy is complete, the new image file path on each RPM is automatically configured as the primary image path for the next boot. The current system image (the one from which the RPM booted) is automatically configured as the secondary image path.

Note: The keywords **boot-image**, **synchronize-rpm**, and **external** can be used on the Primary RPM only.

copy running-config startup-config duplicate

Copy the startup configuration with the running configuration, and then copy the new startup configuration to the external flash as a backup.

Syntax **copy running-config startup-config duplicate**

Command Modes EXEC privilege

Command History

Version 6.3.1.0	Introduced

Usage Information This command is useful for quickly making a changed configuration on one chassis available on external flash in order to move it to another chassis.

When you use the **copy running-config startup-config duplicate** command to copy the running configuration to the startup configuration, FTOS creates a backup file on the internal flash of the startup configuration.

delete

Allows you to delete a file from the flash. Once deleted, files cannot be restored.

Syntax **delete** *flash-url* [**no-confirm**]

Parameters

flash-url	Enter the following location and keywords: • For a file or directory on the internal Flash, enter **flash://** followed by the filename or directory name. • For a file or directory on the external Flash, enter **slot0://** followed by the filename or directory name.
no-confirm	(OPTIONAL) Enter the keyword **no-confirm** to specify that FTOS does not require user input for each file prior to deletion.

Command Modes EXEC privilege

dir

Allows you to view the files in a filesystem. The default is the current directory.

Syntax **dir** [*filename* | *directory name:*]

Parameters

filename | *directory name:*	(OPTIONAL) Enter one of the following: • For a file or directory on the internal Flash, enter **flash://** followed by the filename or directory name. • For a file or directory on the external Flash, enter **slot0://** followed by the filename or directory name:

Command Modes EXEC privilege

Example

```
Force10#dir
Directory of flash:

  1  -rwx    6478482   May 13  101 16:54:34  E1200.BIN

flash: 64077824 bytes total (57454592 bytes free)
Force10#
```

Figure 5 dir Command Example for the Internal Flash

Related Commands

cd	Change working directory.

download alt-boot-image

Download an alternate boot image to the chassis.

Syntax **download alt-boot-image** *file-url*

Parameters

file-url	Enter one of the following: flash:System image file URL ([flash://]filename) ftp: System image file URL (ftp://userid:password@hostip/filepath) slot0:System image file URL ([slot0://]filename) tftp: System image file URL (tftp://hostip/filepath)

Command Modes EXEC privilege

Usage Information Use this command before executing the upgrade command with variables **alt-bootflash-image** or **alt-bootselector-image**.

Related Commands		
	upgrade	Upgrade the bootflash or boot selector versions.

download alt-full-image

C-Series	No
E-Series	✓

Download an alternate FTOS image to the chassis.

Syntax **download alt-full-image** *file-url*

Parameters		
	file-url	Enter the location of the alternate FTOS image, for example: ftp://userid:password@hostlocation/filepath tftp://hostlocation/filepath

Defaults No default behavior or values

Command Modes EXEC privilege

Command History		
	Version 6.5.1.0	Introduced

Usage Information This command is most commonly used in the Warm Upgrade with Line Card Cache Boot procedure that is detailed in the Configuration Fundamentals chapter of the *FTOS Configuration Guide*.

Related Commands		
	upgrade	Upgrade the bootflash or boot selector versions

download alt-system-image

C-Series	No
E-Series	✓

Download an alternate system image (not the boot flash or boot selector image) to the chassis.

Syntax **download alt-system-image** *file-url*

Parameters		
	file-url	Enter the location of the alternate system image, for example: ftp://userid:password@hostlocation/filepath tftp://hostlocation/filepath

Defaults No default behavior or values

Command Modes EXEC privilege

Command History		
	Version 6.5.1.0	Introduced

format

Allows you to erase all existing files and reformat a filesystem. Once the filesystem is formatted, files cannot be restored.

Syntax **format** *filesystem*: [**dosFs1.0** | **dosFs2.0**]

Parameters		
	filesystem:	Enter one of the following: • To reformat the internal Flash, enter **flash:** • To reformat the external Flash, enter **slot0:**
	dosFs1.0	Enter the keyword **dosFs1.0** to format in DOS 1.0 (the default)
	dosFs2.0	Enter the keyword **dosFs2.0** to format in DOS 2.0

Default DOS 1.0 (dosFs1.0)

Command Modes EXEC privilege

Usage Information After reformatting is complete, three empty directories are automatically created on flash: CRASH_LOG_DIR, TRACE_LOG_DIR and NVTRACE_LOG_DIR.

Note: Version option is available on LC-ED-RPM only. LC-EE3-RPM, LC-EF-RPM, and LC-EF3-RPM supports DOS 2.0 only.

logging kernel-coredump

Disable the kernel core-dump.

C-Series	No
E-Series	✓

Syntax **logging kernel-coredump** {**enable** | **disable**}

Parameters

enable	(OPTIONAL) Enter the keyword **enable** to direct the kernel core-dump onto the flash.
disable	(OPTIONAL) Enter the keyword **disable** to stop the kernel core-dump from uploading to flash.

Defaults Enabled

Command Modes CONFIGURATION

Command History

Version 6.5.1.0	Application core-dump naming convention enhanced to include application
Version 6.1.1.0	Introduced

Usage Information By default, the kernel core-dump is enable and stored in the directory:

- Storage Directory Name: **flash:CORE_DUMP_DIR**
  - Kernel core-dump naming convention is: **f10rp***ProcessorID*.**kcore.gz**
    For example: **F10rp1.kcore.gz**
  - Application core-dump naming convention is:
    rp*ProcessorID _ApplicationName_timestamp*.**core.gz**
    For example: **rp1_ospf_060307172608.core.gz**
- Multiple core-dumps
  - Application core-dumps are timestamp embedded and are not overwritten by default. Manually delete the older core-dumps to allow more space on the flash.
  - Kernel core-dumps are overwritten whenever there is a new coredump.

Should a crash occur, the large crash kernel file may take more than ten minutes to upload and may require more space on the flash than is available. The HA module is aware of a core-dump in process and will wait until the upload is complete before rebooting the RPM.

Note: Application core-dumps are also automatically uploaded to flash. If there is not enough available space for the kernel core-dump on the flash, the kernel upload will terminate.

Related Commands

logging kernel-coredump server	Designate a sever to upload kernel core-dumps.

logging kernel-coredump server

C-Series	No
E-Series	✓

Designate a server to upload kernel core-dumps.

Syntax **logging kernel-coredump server** {*server IP address* | *hostname*} {*login name*} {*password*}

Parameters

server IP address	(OPTIONAL) Enter the target server IP address.
hostname	(OPTIONAL) Enter the target server's host name.
login name	Enter the target server's login name.
password	Enter the target server's password.

Defaults No default behavior

Command Modes CONFIGURATION

Command History

Version 6.1.1.0	Introduced

Usage Information Crash kernel files are uploaded to flash by default. Since flash space may be limited, using this command ensures your entire crash kernel files are uploaded successfully and completely.

Note: You must disable logging kernel-coredump before you designate a new server destination for your kernel core-dumps.

Related Commands

logging kernel-coredump	Disable the kernel core-dump

pwd

Allows you to view the current working directory.

Syntax **pwd**

Command Modes EXEC privilege

Example

```
Force10#pwd
flash:
Force10#
```

Figure 6 pwd Command Example

Related Commands

cd	Change directory.

rename

Allows you to rename a file in the local file system.

Syntax **rename** *url url*

Parameters

url	Enter the following keywords and a filename: • For a file on the internal Flash, enter **flash://** followed by the filename. • For a file on the external Flash, enter **slot0://** followed by the filename.

Command Modes EXEC privilege

show bootvar

Allows you to view the variable settings for the E-Series boot parameters.

Syntax **show bootvar**

Command Modes EXEC

EXEC privilege

Example

```
Force10#show bootvar
PRIMARY IMAGE FILE =  ftp://box:password@10.31.1.205//home/5.3.1/5.3.1.0/FTOS-ED-RPM1-5.3.1.0.bin
SECONDARY IMAGE FILE =  variable does not exist
DEFAULT IMAGE FILE =  flash://FTOS-ED-5.3.1.0.bin
LOCAL CONFIG FILE =  variable does not exist
PRIMARY HOST CONFIG FILE =  variable does not exist
SECONDARY HOST CONFIG FILE =  variable does not exist
PRIMARY NETWORK CONFIG FILE =  variable does not exist
SECONDARY NETWORK CONFIG FILE =  variable does not exist
CURRENT IMAGE FILE =  ftp://box:password@10.31.1.205//home/5.3.1/5.3.1.0/FTOS-ED-RPM1-5.3.1.0.bin
CURRENT CONFIG FILE 1 =  flash://startup-config
CURRENT CONFIG FILE 2 =  variable does not exist
CONFIG LOAD PREFERENCE =  local first
BOOT INTERFACE GATEWAY IP ADDRESS =  variable does not exist
Force10#
```

Figure 7 show bootvar Command Output

Related Commands

boot config	Set the location of configuration files on local devices.
boot host	Set the location of configuration files from the remote host.
boot network	Set the location of configuration files from a remote network.
boot system	Set the location of FTOS image files.

show file

View contents of a text file in the local filesystem.

Syntax **show file** *filesystem*

Parameters

filesystem	Enter one of the following: • *flash:* for the internal Flash • *slot0:* for the external Flash

Command Modes EXEC privilege

Example

```
E1200-20#show file flash://startup-config
!
boot system rpm0 primary ftp://test:server@10.16.1.144//home/images/E1200_405-3.1.2b1.86.bin
boot system rpm0 secondary flash://FTOS-ED-6.1.1.0.bin
boot system rpm0 default ftp://:@/\
!
redundancy auto-synchronize persistent-data
redundancy primary rpm0
!
hostname E1200-20
!
enable password 7 94849d8482d5c3
!
username test password 7 93e1e7e2ef
!
enable restricted 7 948a9d848cd5c3
!
protocol spanning-tree 0
 bridge-priority 8192
 rapid-root-failover enable
!
interface GigabitEthernet 0/0
 no ip address
 shutdown
```

Figure 8 show file Command Example (Partial)

show file-systems

Allows you to view information about the file systems on the E-Series.

Syntax **show file-systems**

Command Modes EXEC privilege

Example

```
Force10#show file-systems
      Size(b)     Free(b)   Feature      Type   Flags  Prefixes
     63938560    51646464  dosFs2.0       MMC      rw  flash:
     63938560    18092032  dosFs1.0       MMC      rw  slot0:
            -           -         -   network      rw  ftp:
            -           -         -   network      rw  tftp:
            -           -         -   network      rw  scp:
Force10#
```

Figure 9 show file-system Command Output

Table 5 describes the information in Figure 9.

Table 5 show file-systems Command Output Fields

Field	Description
size(b)	Lists the size in bytes of the storage location. If the location is remote, no size is listed.
Free(b)	Lists the available size in bytes of the storage location. If the location is remote, no size is listed.
Feature	Displays the formatted DOS version of the device.

Table 5 show file-systems Command Output Fields

Field	Description
Type	Displays the type of storage. If the location is remote, the word `network` is listed.
Flags	Displays the access available to the storage location. The following letters indicate the level of access: • r = read access • w = write access
Prefixes	Displays the name of the storage location.

show os-version

Allows you to view the release and software image version information of the image file specified or optionally, the image loaded on the RPM.

Syntax **show os-version** [*file-url*]

Parameters

file-url	(OPTIONAL) Enter the following location keywords and information: • For a file on the internal Flash, enter **flash://** followed by the filename. • For a file on an FTP server, enter **ftp://***user:password@hostip/filepath* • For a file on the external Flash, enter **slot0://** followed by the filename. • For a file on a TFTP server, enter **tftp://***hostip/filepath*

Defaults No default values or behavior

Command Modes EXEC privilege

Usage Information

Note: A filepath that contains a dot (**.**) is not supported.

Example

```
Force10#show os-version

RELEASE IMAGE INFORMATION :
------------------------------------------------------------------------
      Platform          Version        Size           ReleaseTime
 E-series:  EF          7.5.1.0    27676168    Aug 15 2007 10:06:21

TARGET IMAGE INFORMATION :
------------------------------------------------------------------------
          Type          Version                   Target    checksum
       runtime          7.5.1.0        control processor      passed
       runtime          7.5.1.0          route processor      passed
       runtime          7.5.1.0       terascale linecard      passed
    boot flash          2.4.1.1        control processor      passed
    boot flash          2.4.1.1          route processor      passed
    boot flash          2.3.1.3       terascale linecard      passed
 boot selector          2.4.1.1        control processor      passed
 boot selector          2.4.1.1          route processor      passed
 boot selector          2.3.1.3       terascale linecard      passed

Force10#
```

Figure 10 show os-version Command Example (E-Series)

Example

```
Force10#show os-version

RELEASE IMAGE INFORMATION :
------------------------------------------------------------------------
      Platform          Version        Size           ReleaseTime
 C-series:  CB          7.5.1.0    23734363    Aug 18 2007 11:49:51

TARGET IMAGE INFORMATION :
------------------------------------------------------------------------
          Type          Version                   Target    checksum
       runtime          7.5.1.0        control processor      passed
       runtime          7.5.1.0                  linecard      passed
    boot flash          2.7.0.1        control processor      passed
    boot flash         1.0.0.40                  linecard      passed
 boot selector          2.7.0.1        control processor      passed
 boot selector         1.0.0.40                  linecard      passed

FPGA IMAGE INFORMATION :
------------------------------------------------------------------------
          Card          Version        Release Date
   Primary RPM              4.1         May 02 2007
 Secondary RPM              4.1         May 02 2007
           LC0              3.2         May 02 2007
           LC5              3.2         May 02 2007
           LC6              2.2         May 02 2007
Force10#
```

Figure 11 show os-version Command Example (C-Series)

show running-config

Displays the current configuration, indicates changes from the default values, and .

Syntax **show running-config** [*entity*] [**configured**]

Parameters	*entity*	(OPTIONAL) Enter one of the keywords listed below to view that entities current (non-default) configuration. Note that if nothing is configured for that entity, nothing is displayed and the prompt returns: • **aaa** for the current AAA configuration • **acl** for the current ACL configuration • **arp** for the current static ARP configuration • **as-path** for the current AS-path configuration • **bgp** for the current BGP configuration • **boot** for the current boot configuration • **cam-profile** for the current CAM profile in the configuration. • **class-map** for the current class-map configuration • **community-list** for the current community-list configuration • **fefd** for the current FEFD configuration • **ftp** for the current FTP configuration • **fvrp** for the current FVRP configuration • **host** for the current host configuration • **igmp** for the current IGMP configuration • **interface** for the current interface configuration • **isis** for the current ISIS configuration • **line** for the current line configuration • **load-balance** for the current port-channel load-balance configuration • **logging** for the current logging configuration • **mac** for the current MAC ACL configuration • **mac-address-table** for the current MAC configuration • **management-route** for the current Management port forwarding configuration • **mroute** for the current Mroutes configuration • **ntp** for the current NTP configuration • **ospf** for the current OSPF configuration • **pim** for the current PIM configuration • **policy-map-input** for the current input policy map configuration • **policy-map-output** for the current output policy map configuration • **prefix-list** for the current prefix-list configuration • **privilege** for the current privilege configuration • **radius** for the current RADIUS configuration • **redirect-list** for the current redirect-list configuration • **redundancy** for the current RPM redundancy configuration • **resolve** for the current DNS configuration • **rip** for the current RIP configuration • **route-map** for the current route map configuration

	• **snmp** for the current SNMP configuration • **spanning-tree** for the current spanning tree configuration • **static** for the current static route configuration • **tacacs+** for the current TACACS+ configuration • **tftp** for the current TFTP configuration • **trace-group** for the current trace-group configuration • **trace-list** for the current trace-list configuration • **users** for the current users configuration • **wred-profile** for the current wred-profile configuration
configured	(OPTIONAL) Enter the keyword configuration to display line card interfaces with non-default configurations only.

Command Modes EXEC privilege

Command History

Version 7.4.1.0	Expanded to include last configuration change and start-up last updated (date and time) and who made the change.

Example

```
Force10#show running-config
Current Configuration ...
! Version 7.4.1.0
! Last configuration change at Tue Apr 10 17:43:38 2007 by admin
! Startup-config last updated at Thu Mar 29 02:35:08 2007 by default
!
boot system rpm0 primary flash://FTOS-EF-7.4.1.0.bin
boot system rpm0 secondary flash://FTOS-EF-6.3.1.2.bin
boot system rpm0 default flash://FTOS-EF-6.5.1.8.bin
!
...
```

Figure 12 show running-config Command Example (partial)

show version

Display the current software version.

Syntax **show version**

Command Modes EXEC privilege

Example

```
Force10#show version
Force10 Networks Real Time Operating System Software
Force10 Operating System Version: 1.0
Force10 Application Software Version: 5.3.1.0
Copyright (c) 1999-2004 by Force10 Networks, Inc.
Build Time: Sun May 9 00:57:03 PT 2004
Build Path: /local/local0/Release/5-4-1/SW/Bsp/Diag
Force10 uptime is 1 days, 3 hours, 16 minutes

System image file is "/home/5.3.1/5.3.1.0/FTOS-ED-RPM1-5.3.1.0.bin"

Chassis Type: E1200
Control Processor: IBM PowerPC 405GP (Rev D) with 268435456 bytes of memory.
Route Processor 1: IBM PowerPC 405GP (Rev D) with 536870912 bytes of memory.
Route Processor 2: IBM PowerPC 405GP (Rev D) with 536870912 bytes of memory.

128K bytes of non-volatile configuration memory.

  1 Route Processor Module
  9 Switch Fabric Module
  1 24-port GE line card with SFP optics (EE)
  1 12-port GE Flex line card with SFP optics (EE)
  1 2-port OC48c line card with SR optics (EC)
  2 24-port GE line card with SX optics (EB)
  1 2-port 10GE WAN PHY line card with 10Km (1310nm) optics (EE)
  1 12-port GE Flex line card with SFP optics (EC)
  1 2-port 10GE LAN PHY line card with 10Km (1310nm) optics (ED)
  1 12-port OC12c/3c PoS line card with IR optics (EC)
  1 24-port GE line card with SFP optics (ED)
  1 FastEthernet/IEEE 802.3 interface(s)
120 GigabitEthernet/IEEE 802.3 interface(s)
 14 SONET network interface(s)
  4 Ten GigabitEthernet/IEEE 802.3 interface(s)
Force10#
```

Figure 13 show version Command Output

Table 6 explains the information found in Figure 13

Table 6 show version Command Fields

Lines beginning with	Description
Force10 Network ...	Displays the name of the operating system.
Force10 Operating...	Displays the OS version number.
Force10 Application...	Displays the software version.
Copyright (c)...	Displays the copyright information.
Build Time...	Displays the software build's date stamp.
Build Path...	Displays the location of the software build files loaded on E-Series.
Force10 uptime is...	Displays the amount of time the E-Series is up and running.
System image...	Displays the image file name.
Chassis Type:	Displays the chassis type (E1200, E600, E600i, E300 or C300).
Control Processor: ...	Displays the E-Series control processor information and the amount of memory on that processor.
Route Processor 1:...	Displays the E-Series route processor 1 information and the amount of memory on that processor.
Route Processor 2: ...	Displays the E-Series route processor 2 information and the amount of memory on that processor.

Table 6 show version Command Fields (continued)

Lines beginning with	Description
128K bytes...	Displays the amount and type of memory on E-Series.
1 Route Processor...	Displays the hardware configuration of the E-Series, including the number and type of physical interfaces available.

show startup-config

Display the startup configuration.

Syntax **show startup-config**

Command Modes EXEC

EXEC privilege

Command History

Version 7.4.1.0	Expanded to include last configuration change and start-up last updated (date and time) and who made the change.

Example

```
Force10#show startup-config

! Version 7.4.1.0
! Last configuration change at Thu Mar 29 02:16:07 2007 by default
! Startup-config last updated at Thu Mar 29 02:35:08 2007 by default
!
boot system rpm0 primary flash://FTOS-EF-7.4.1.0.bin
boot system rpm0 secondary flash://FTOS-EF-6.3.1.2.bin
boot system rpm0 default flash://FTOS-EF-6.5.1.8.bin
!
...
```

Figure 14 show startup-config Command Output (partial)

Related Commands

show running-config	View current (running) configuration.

upgrade

Allows you to upgrade the bootflash or boot selector image on a processor. You can also upgrade to an alternate bootflash image, boot selector image, alternate system image or a system image.

Syntax **upgrade** {**alt-bootflash-image** | **alt-bootselector-image** | **alt-system-image** | **bootflash-image** | **bootselector-image** | **system-image**} {**all** | **cp** | **linecard** *linecard-slot* | **rp1** | **rp2** | **rpm**}

Parameters

alt-bootflash-image	Enter the keyword **alt-bootflash-image** to upgrade the bootflash image using the alternate bootflash image file.
alt-bootselector-image	Enter the keyword **alt-bootselector-image** to upgrade the boot selector image using the alternate boot selector image file. Use with TAC supervision only.
alt-system-image	Enter the keyword **alt-system-image** to upgrade the cache boot image with an alternate system image.
bootflash-image	Enter the keyword **bootflash-image** to upgrade the bootflash image.
bootselector-image	Enter the keyword **bootselector-image** to upgrade the boot selector image. Use with TAC supervision only.
system-image	Enter the keyword **system-image** to ugrade the cache boot image
all	Enter the keyword **all** to upgrade the bootflash/boot selector image on all processors in the E-Series.
cp	Enter the keyword **cp** to upgrade the bootflash/boot selector image on the Control Processor on the RPM.
linecard *linecard-slot*	Enter the keyword **linecard** followed by the slot number to change the bootflash image on a specific line card. C-Series Range: 0-7 on the C300 E-Series Range:0 to 13 on the E1200, 0 to 6 for the E600, 0 to 5 on the E300
rp1	Enter the keyword **rp1** to upgrade the bootflash/boot selector image on Route Processor 1 on the RPM. **Note**: Not applicable for E300.
rp2	Enter the keyword **rp2** to upgrade the bootflash/boot selector image on Route Processor 2 on the RPM. **Note**: Not applicable for E300.
rpm	Enter the keyword **rpm** to upgrade the bootflash/boot selector image on all processors on the RPM.

Defaults No configuration or default values

Command Modes EXEC privilege

Usage Information A system message appears stating the Bootflash upgrade status. Reload the system to boot from the upgraded boot images.

Prior to using **upgrade alt-bootflash-image** or **upgrade alt-bootselector-image** commands, use the download alt-boot-image command.

Related Commands

download alt-boot-image	Download an alternate boot image to the chassis
download alt-full-image	Download an alternate FTOS image to the chassis
download alt-system-image	Download an alternate system image to the chassis

Chapter 3 Control and Monitoring Commands

This chapter contains control and setup commands, including Telnet, FTP, and TFTP, to configure and monitor the system. This chapter contains two sections:

- Control and Setup Commands on page 105
- Upgrading the FPGA on page 168 (**C-Series Only**)

Control and Setup Commands

Use the following commands to configure and monitor FTOS:

- audible cut-off on page 107
- banner exec on page 107
- banner login on page 108
- banner motd on page 109
- cam-audit linecard on page 109
- chassis chassis-mode on page 110
- clear alarms on page 111
- clear line on page 111
- configure on page 111
- debug cpu-traffic-stats on page 112
- debug ftpserver on page 113
- disable on page 113
- do on page 113
- enable on page 114
- enable xfp-power-updates on page 115
- end on page 116
- epoch on page 116
- exec-banner on page 117
- exec-timeout on page 117
- exit on page 118

- ftp-server enable on page 118
- ftp-server topdir on page 119
- ftp-server username on page 120
- hostname on page 120
- ip ftp password on page 121
- ip ftp source-interface on page 121
- ip ftp username on page 122
- ip telnet server enable on page 123
- ip telnet source-interface on page 123
- ip tftp source-interface on page 124
- line on page 125
- linecard on page 126
- module power-off on page 126
- motd-banner on page 127
- ping on page 127
- power-off on page 129
- power-on on page 129
- reload on page 130
- reset on page 130
- send on page 131
- service timestamps on page 131
- show alarms on page 132
- show chassis on page 133
- show cpu-traffic-stats on page 135
- show debugging on page 136
- show environment on page 137
- show inventory on page 139
- show linecard on page 140
- show linecard boot-information on page 142
- show memory on page 144
- show processes communication (deprecated) on page 145
- show processes cpu on page 146
- show processes ipc flow-control on page 148
- show processes memory on page 150
- show processes switch-utilization on page 153
- show rpm on page 153
- show sfm on page 155
- ssh-peer-rpm on page 160
- telnet on page 160
- telnet-peer-rpm on page 161

- terminal length on page 162
- terminal xml on page 162
- traceroute on page 163
- undebug all on page 164
- upgrade sfm on page 165
- upload nvtrace linecard on page 165
- upload trace-log on page 166
- virtual-ip on page 167
- write on page 167

audible cut-off

C-Series	No
E-Series	✓

Turn off an audible alarm

Syntax **audible cut-off**

Defaults Not configured.

Command Modes EXEC privilege

banner exec

Configure a message that is displayed when another user enters the EXEC privilege mode.

Syntax **banner exec** *c line c*

To delete a banner, enter **no banner exec**.

Parameters

c	Enter the keywords **banner exec**, and then specify a character delineator, represented here by the letter *c*, and press ENTER.
line	Enter a text string for your banner message ending the message with your delineator. In the example in Figure 15, the delineator is a percent character (%); the banner message is “testing, testing”.

Defaults No banner is enabled.

Command Modes CONFIGURATION

Example

```
Force10(conf)#banner exec %
Enter TEXT message.  End with the character '%'.
testing, testing%
Force10(conf)#
```

Figure 15 banner incoming Command Example

Related Commands

banner login	Sets a banner for login connections to E-Series.
banner motd	Sets a Message of the Day banner.

banner login

Set a banner to be displayed when logging on to the E-Series.

Syntax **banner login** *c line c*

To delete a login banner, enter **no banner login**.

Parameters

c	Enter a delineator character to specify the limits of the text banner. In Figure 15, the % character is the delineator character.
line	Enter a text string for your text banner message ending the message with your delineator. In the example in Figure 15, the delineator is a percent character (%).

Defaults No banner is configured.

Command Modes CONFIGURATION

Usage Information A login banner message is displayed only in EXEC privilege mode after entering the **enable** command followed by the password. These banners are not displayed to users in EXEC (non-privilege) mode.

Related Commands

banner exec	Sets a banner to be displayed when you enter EXEC privilege mode.
banner motd	Sets a Message of the Day banner.

banner motd

Set a Message of the Day (MOTD) banner.

Syntax **banner motd** *c line c*

To delete a Message of the Day banner, enter **no banner motd**.

Parameters

c	Enter a delineator character to specify the limits of the text banner. In Figure 15, the % character is the delineator character.
line	Enter a text string for your message of the day banner message ending the message with your delineator. In the example in Figure 15, the delineator is a percent character (%).

Defaults No banner is configured.

Command Modes CONFIGURATION

Usage Information A MOTD banner message is displayed only in EXEC privilege mode after entering the **enable** command followed by the password. These banners are not displayed to users in EXEC (non-privilege) mode.

Related Commands

banner exec	Sets a banner to be displayed when you enter the EXEC privilege mode.
banner login	Sets a banner to be displayed after successful login to the E-Series.

cam-audit linecard

Enable audit of the IPv4 forwarding table on all line cards.

Syntax **cam-audit linecard all ipv4-fib interval** *time-in-minutes*

To disable audit, use the **no cam-audit linecard all ipv4-fib** command

Parameters

all	Enter the keyword **all** to enable CAM audit on all line cards.
ipv4-fib	Enter the kyeword **ipv4-fib** to designate the CAM audit on the IPv4 forwarding entries.
interval *time-in-minutes*	Enter the keyword **interval** followed by the frequency in minutes of the CAM audit. Range: 5 to 1440 minutes (24 hours) Default: 60 minutes

Defaults Disabled

Command Modes CONFIGURATION

Command History

Version 7.4.1.0	Introduced

Usage Information Enables periodic audits of software and hardware copies of the IPv4 forwarding table.

chassis chassis-mode

C-Series	**No**
E-Series	✓

Set the chassis mode to optimize hardware and software features.

Syntax **chassis chassis-mode** [**EtherScale** | **Mixed** | **TeraScale**]

Parameters

EtherScale	Enter the keyword **EtherScale** to set the chassis to use only EtherScale line cards (ED and EE) and RPMs (ED and EE).
Mixed	Enter the keyword **Mixed** to set the chassis to use both EtherScale and TeraScale line cards.
TeraScale	Enter the keyword **TeraScale** to set the chassis to use only TeraScale line cards (EF and EF3) and RPMs (EF and EF3).

Defaults EtherScale

Command Modes EXEC privilege

Command History

Version 6.1.1.0	Introduced

```
Force10# chassis chassis-mode ?
EtherScale       Set to EtherScale mode
Mixed            Set to Mixed mode
TeraScale        Set to TeraScale mode
```

Figure 16 chassis chassis-mode Command Options.

Usage Information The chassis mode is programmed into an EEPROM on the backplane of the chassis. The mode change is effective only after the chassis is rebooted. Configuring the appropriate chassis mode enables the chassis to use all the ports on the line card and recognize all software features.

To view the current mode of the chassis, use the show chassis brief command.

Related Commands		
	show chassis	View the chassis mode, hardware installed and status.

clear alarms

Clear alarms on the E-Series.

Syntax **clear alarms**

Command Modes EXEC privilege

clear line

Reset a terminal line.

Syntax **clear line** {*line-number* | **aux 0** | **console 0** | **vty** *number*}

Parameters

line-number	Enter a number for one of the 12 terminal lines on the E-Series. Range: 0 to 11.
aux 0	Enter the keywords **aux 0** to reset the Auxiliary port. **Note:** This option is supported on E-Series only.
console 0	Enter the keyword **console 0** to reset the Console port.
vty *number*	Enter the keyword vty followed by a number to clear a Terminal line. Range: 0 to 9

Command Modes EXEC privilege

configure

Enter the CONFIGURATION mode from the EXEC privilege mode.

Syntax **configure** [**terminal**]

Parameters

terminal	(OPTIONAL) Enter the keyword **terminal** to specify that you are configuring from the terminal.

Command Modes EXEC privilege

Example

```
Force10#configure
Force10(conf)#
```

Figure 17 configure Command Example

debug cpu-traffic-stats

Enable the collection of CPU traffic statistics.

Syntax **debug cpu-traffic-stats**

To disable the debugging, execute the **no debug cpu-traffic-stats** command.

Defaults Disabled

Command Modes EXEC privilege

Command History

Version 6.2.1.1	Introduced

Usage Information This command enables (and disables) the collection of CPU traffic statistics from the time this command is executed (not from system boot). However, excessive traffic received by a CPU will automatically trigger (turn on) the collection of CPU traffic statics. The message:

Excessive traffic is received by CPU and traffic will be rate controlled

is an indication that collection of CPU traffic is automatically turned on. Use the show cpu-traffic-stats to view the traffic statistics.

Note: This command must be enabled before the show cpu-traffic-stats command will display traffic statistics. Force10 recommends that you disable debugging (**no debug cpu-traffic-stats)** once troubleshooting is complete.

Related Commands

show cpu-traffic-stats	Display cpu traffic statistics

debug ftpserver

View transactions during an FTP session when a user is logged into the FTP server (the E-Series).

Syntax **debug ftpserver**

To stop debugging, enter **no debug ftpserver**.

Command Modes EXEC privilege

disable

Return to the EXEC mode.

Syntax **disable** [*level*]

Parameters

level	(OPTIONAL) Enter a number for a privilege level of the FTOS. Range: 0 to 15. Default: 1

Defaults 1

Command Modes EXEC privilege

do

Allows the execution of most EXEC level commands from all the CONFIGUATION levels without returning to the EXEC level.

Syntax **do** [*command*]

Parameters

do [*command*]	Enter the keyword **do** followed by the CONFIGURATION level command.

Defaults No default behavior

Command Modes CONFIGURATION

Command History

Version 6.1.1.0	Introduced

Usage Information

The following commands are *not* supported by the **do** command:

- enable
- disable
- exit
- config

Example

```
Force10(conf-if-te-5/0)#do clear counters
Clear counters on all interfaces [confirm]
Force10(conf-if-te-5/0)#
Force10(conf-if-te-5/0)#do clear logging
Clear logging buffer [confirm]
Force10(conf-if-te-5/0)#
Force10(conf-if-te-5/0)#do reload
System configuration has been modified. Save? [yes/no]: n
Proceed with reload [confirm yes/no]: n
Force10(conf-if-te-5/0)#
```

Figure 18 do Command Example

enable

Enter the EXEC privilege mode or any other privilege level configured. After entering this command, you must enter a password.

Syntax **enable** [*level*]

Parameters

level	(OPTIONAL) Enter a number for a privilege level of the FTOS. Range: 0 to 15. Default: 15

Defaults 15

Command Modes EXEC

Usage Information Users entering the EXEC privilege mode or any other configured privilege level can access configuration commands. To protect against unauthorized access, use the enable password command to configure a password for the enable command for a specific privilege level. If no privilege level is specified, the default is privilege level 15.

Example

```
Force10>en

Password:
Force10#
```

Figure 19 enable Command Example

Related Commands

enable password	Configure a password for the enable command and to access a privilege level.

enable xfp-power-updates

Enable XFP power updates for SNMP.

Syntax **enable xfp-power-updates interval** *seconds*

To disable XFP power updates, use the **no enable xfp-power-updates** command.

Parameters

interval *seconds*	Enter the keyword **interval** followed by the polling interval in seconds. Range: 120 to 6000 seconds Default: 300 seconds (5 minutes)

Defaults Disabled

Command Modes CONFIGURATION

Command History

Version 7.5.1.0	Introduced

Usage Information The chassis MIB contain the entry chSysXfpRecvPower in the chSysPortTable table. Periodically, IFA polls the XFP power for each of the ports, and sends the values to IFM where it is cached. The default interval for the polling is 300 seconds (5 minutes). Use this command to enable the polling and to configure the polling frequency.

end

Return to the EXEC privilege mode from other command modes (for example, the CONFIGURATION or ROUTER OSPF modes).

Syntax **end**

Command Modes CONFIGURATION, SPANNING TREE, MULTIPLE SPANNING TREE, LINE, INTERFACE, TRACE-LIST, VRRP, ACCESS-LIST, PREFIX-LIST, AS-PATH ACL, COMMUNITY-LIST, ROUTER OSPF, ROUTER RIP, ROUTER ISIS, ROUTER BGP

Example

```
Force10(conf-if)#end
Force10#
```

Figure 20 end Command Example

Related Commands

exit	Return to the lower command mode.

epoch

C-Series	**No**
E-Series	✓

Set the epoch scheduling time for the chassis.

Syntax **epoch** {**3.2** | **10.4**}

To return to the default setting, enter **no epoch**.

Parameters

3.2	Enter the keyword **3.2** to set the epoch to 3.2 micro-seconds and lower the latency. This option is available on the E600/E600i and E1200 only.
10.4	Enter the keyword **10.4** to set the epoch to 10.4 micro-seconds. This is the default setting and is available on the E300, E600/E600i, and E1200.

Defaults 10.4

Command Modes CONFIGURATION

Command History

Version 6.1.1.0	Values changed as described above
Version 6.2.1.1	Support for E300 introduced (10.4 only)

Usage Information The epoch change will take effect only after you save the configuration and reload the chassis.

Note: The E300 supports only the epoch 10.4 command. Both epoch command options are supported on the E600/E600i and the E1200 chassis.

exec-banner

Display a text string when you enter the EXEC privilege mode.

Syntax **exec-banner**

To disable the banner on terminal lines, enter **no exec-banner**.

Defaults Enabled on all lines (if configured, the banner appears).

Command Modes LINE

Related Commands

banner exec	Configure a banner to display when entering the EXEC privilege mode.

exec-timeout

Set a time interval the E-Series will wait for input on a line before disconnecting the session.

Syntax **exec-timeout** *minutes* [*seconds*]

To return to default settings, enter **no exec-timeout**.

Parameters

minutes	Enter the number of minutes on inactivity on the E-Series before disconnecting the current session. Range: 0 to 35791 Default: 10 minutes for console line; 30 minutes for VTY line.
seconds	(OPTIONAL) Enter the number of seconds Range: 0 to 2147483 Default: 0 seconds

Defaults 10 minutes for console line; 30 minutes for VTY lines; 0 seconds

Command Modes LINE

Usage Information To remove the time interval, enter **exec-timeout 0 0**.

Example

```
Force10 con0 is now available

Press RETURN to get started.
Force10>
```

Figure 21 Screenshot of Prompt After the FTOS Times Out

exit

Return to the lower command mode.

Syntax **exit**

Command Modes EXEC privilege, CONFIGURATION, LINE, INTERFACE, TRACE-LIST, PROTOCOL GVRP, SPANNING TREE, MULTIPLE SPANNING TREE, MAC ACCESS LIST, ACCESS-LIST, AS-PATH ACL, COMMUNITY-LIST, PREFIX-LIST, ROUTER OSPF, ROUTER RIP, ROUTER ISIS, ROUTER BGP

Example

```
Force10(conf-span)#exit
Force10(conf)#
```

Figure 22 exit Command Example

Related Commands

end	Return to the EXEC privilege command mode.

ftp-server enable

Enable FTP server functions on the E-Series.

Syntax **ftp-server enable**

To disable FTP server on the E-Series, enter **no ftp-server enable**.

Defaults Disabled.

Command Modes CONFIGURATION

Example

```
morpheus% ftp 10.31.1.111
Connected to 10.31.1.111.
220 Force10 (1.0) FTP server ready
Name (10.31.1.111:dch): dch
331 Password required
Password:
230 User logged in
ftp> pwd
257 Current directory is "flash:"
ftp> dir
200 Port set okay
150 Opening ASCII mode data connection
  size          date       time       name
--------       ------     ------     --------
     512    Jul-20-2004 18:15:00   tgtimg
     512    Jul-20-2004 18:15:00   diagnostic
     512    Jul-20-2004 18:15:00   other
     512    Jul-20-2004 18:15:00   tgt
226 Transfer complete
329 bytes received in 0.018 seconds (17.95 Kbytes/s)
ftp>
```

Figure 23 Example of Logging on to an FTP Server

Related Commands

ftp-server topdir	Set the directory to be used for incoming FTP connections to the E-Series.
ftp-server username	Set a username and password for incoming FTP connections to the E-Series.

ftp-server topdir

Specify the top-level directory to be accessed when an incoming FTP connection request is made.

Syntax **ftp-server topdir** *directory*

To return to the default settings, enter **no ftp-server topdir**.

Parameters

directory	Enter the directory path.

Defaults The internal flash is the default directory.

Command Modes CONFIGURATION

Usage Information

After you enable FTP server functions with the ftp-server enable command, Force10 Networks recommends that you specify a top-level directory path. Without a top-level directory path specified, the FTOS directs users to the flash directory when they log in to the FTP server (the E-Series).

Related Commands

ftp-server enable	Enables FTP server functions on the E-Series.
ftp-server username	Set a username and password for incoming FTP connections to the E-Series.

ftp-server username

Create a user name and associated password for incoming FTP server sessions.

Syntax

ftp-server username *username* **password** [*encryption-type*] *password*

To delete a user name and its password, use the **no ftp-server username** *username* command.

Parameters

username	Enter a text string up to 40 characters long as the user name.
password *password*	Enter the keyword **password** followed by a string up to 40 characters long as the password. Without specifying an encryption type, the password is unencrypted.
encryption-type	(OPTIONAL) After the keyword **password** enter one of the following numbers: • 0 (zero) for an unecrypted (clear text) password • 7 (seven) for hidden text password.

Defaults

Not enabled.

Command Modes

CONFIGURATION

hostname

Set the host name of the E-Series.

Syntax

hostname *name*

To delete a hostname assigned, enter **no hostname**.

Parameters

name	Enter a text string, up to 32 characters long.

Defaults Force10.

Command Modes CONFIGURATION

Usage Information The hostname is used in the prompt.

ip ftp password

Specify a password for outgoing FTP connections.

Syntax **ip ftp password** [*encryption-type*] *password*

To remove a password and return to the default setting, use the **no ip ftp password** [*password*] command.

Parameters

encryption-type	(OPTIONAL) Enter one of the following numbers: • 0 (zero) for an unecrypted (clear text) password • 7 (seven) for hidden text password
password	Enter a string up to 40 characters as the password.

Defaults Not configured.

Command Modes CONFIGURATION

Usage Information The password is listed in the configuration file; you can view the password by entering the **show running-config ftp** command.

The password configured by the ip ftp password command is used when you use the ftp: parameter in the copy command.

Related Commands

copy	Copy files.
ip ftp username	Set the user name for FTP sessions.

ip ftp source-interface

Specify an interface's IP address as the source IP address for FTP connections.

Syntax **ip ftp source-interface** *interface*

To delete an interface, use the **no ip ftp source-interface** *interface* command.

Parameters

interface	Enter the following keywords and slot/port or number information: • For an 100/1000 Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For Loopback interfaces, enter the keyword **loopback** followed by a number from zero (0) to 16383. • For a Port Channel interface, enter the keyword **port-channel** followed by a number: C-Series Range: 1-128 E-Series Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale • For SONET interface types, enter the keyword **sonet** followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information. • For a VLAN interface, enter the keyword **vlan** followed by a number from 1 to 4094.

Defaults The IP address on the E-Series that is closest to the Telnet address is used in the outgoing packets.

Command Modes CONFIGURATION

ip ftp username

Assign a user name for outgoing FTP connection requests.

Syntax **ip ftp username** *username*

To return to anonymous FTP connections, use the **no ip ftp username** [*username*] command.

Parameters

username	Enter a text string as the user name up to 40 characters long.

Defaults No user name is configured.

Command Modes CONFIGURATION

Usage Information You must also configure a password with the ip ftp password command.

Related Commands		
	ip ftp password	Set the password for FTP connections.

ip telnet server enable

Enable the telnet server on the system.

Syntax **ip telnet server enable**

To disable the telnet server, execute the **no ip telnet server enable** command.

Defaults Enabled

Command Modes CONFIGURATION

Command History		
	Version 6.1.1.0	Introduced

Related Commands		
	ip ssh server	Enable SSH server on the E-Series.

ip telnet source-interface

Set an interface's IP address as the source address in outgoing packets for Telnet sessions.

Syntax **ip telnet source-interface** *interface*

To return to the default setting, use the **no ip telnet source-interface** [*interface*] command.

Parameters

interface	Enter the following keywords and slot/port or number information: • For an 100/1000 Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For Loopback interfaces, enter the keyword **loopback** followed by a number from zero (0) to 16383. • For the SONET interfaces, enter the keyword **sonet** followed by slot/port information. • For a Port Channel, enter the keyword **port-channel** followed by a number: C-Series Range: 1-128 E-Series Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information. • For VLAN interface, enter the keyword **vlan** followed by a number from 1 to 4094.

Defaults The IP address on the E-Series that is closest to the Telnet address is used in the outgoing packets.

Command Modes CONFIGURATION

Related Commands

telnet	Telnet to another device.

ip tftp source-interface

Assign an interface's IP address in outgoing packets for TFTP traffic.

Syntax **ip tftp source-interface** *interface*

To return to the default setting, use the **no ip tftp source-interface** *interface* command.

Parameters

interface	Enter the following keywords and slot/port or number information: • For an 100/1000 Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For Loopback interfaces, enter the keyword **loopback** followed by a number from zero (0) to 16383. • For a Port Channel, enter the keyword **port-channel** followed by a number: C-Series: 1-128 E-Series: 1 to 32 for EtherScale, 1 to 255 for TeraScale • For the SONET interfaces, enter the keyword **sonet** followed by slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information. • For a VLAN interface, enter the keyword **vlan** followed by a number from 1 to 4094.

Defaults The IP address on the E-Series that is closest to the Telnet address is used in the outgoing packets.

Command Modes CONFIGURATION

line

Enable and configure console and virtual terminal lines to the E-Series.

Syntax **line** {**aux 0** | **console 0** | **vty** *number* [*end-number*]}

Parameters

aux 0	Enter the keyword **aux 0** to configure the auxiliary terminal connection. **Note:** This option is supported on E-Series only.
console 0	Enter the keyword **console 0** to configure the console port.
vty *number*	Enter the keyword **vty** followed by a number from 0 to 9 to configure a virtual terminal line for Telnet sessions. The E-Series supports 10 Telnet sessions.
end-number	(OPTIONAL) Enter a number from 1 to 9 as the last virtual terminal line to configure. You can configure multiple lines at one time.

Defaults Not configured

Command Modes CONFIGURATION

Usage Information You cannot delete a terminal connection.

linecard

Configure a non-existent line card in a currently empty slot of the E-Series or a different line card type for the slot.

Syntax **linecard** *number card-type*

To delete a card setting, use the **no linecard** *number* command.

Parameters

number	Enter the number of the slot. C-Series Range: 0-7 on the C300 E-Series Range: 0 to 13 on a E1200, 0 to 6 on a E600, and 0 to 5 on a E300.
card-type	Enter the six digit character identification for your line card (refer to your line card documentation for the your line card identification).

Defaults Not configured

Command Modes CONFIGURATION

Usage Information Use this command only for empty slots or a slot where you have hot-swapped a different line card type.

Note: It is advisable to shutdown interfaces on a line card that you are hot-swapping.

module power-off

Turn-off power to a line card at next reboot.

Syntax **module power-off linecard** *number*

To remove the command from the running configuration, use the **no module power-off linecard** *number* command.

Parameters

linecard *number*	Enter the keyword **line card followed** by the line card slot number C-Series Range: 0-7 on the C300 E-Series Range: 0 to 13 on a E1200, 0 to 6 on a E600, and 0 to 5 on a E300.

Defaults Not configured.

Command Modes CONFIGURATION

motd-banner

Enable a Message of the Day (MOTD) banner to appear when you log in to the E-Series.

Syntax **motd-banner**

To disable the MOTD banner, enter **no motd-banner**.

Defaults Enabled on all lines.

Command Modes LINE

Related Commands

banner motd	Configure a Message of the Day banner.

ping

Test connectivity between the E-Series and another device by sending echo requests and waiting for replies.

Syntax **ping** [*host* | *ip-address* | *ipv6-address*]

Parameter

ip-address	(OPTIONAL) Enter the IP address of the device to which you are testing connectivity. The address must be in the dotted decimal format.
ipv6-address	Enter the IPv6 address, in the **x:x:x:x::x** format, to which you are testing connectivity. **Note:** The **::** notation specifies successive hexadecimal fields of zeros
host	(OPTIONAL) Enter the host name of the devices to which you are testing connectivity.

Defaults The default is 5 repeat count, 100 datagram size, and 2 second timeout

Command Modes EXEC

EXEC privilege

Command History

Version 7.4.1.0	Added support for IPv6 address

Usage Information

When you enter the **ping** command without specifying an IP/IPv6 address (Extended Ping), you are prompted for a target IP/IPv6 address, a repeat count, a datagram size (up to 1500 bytes), a timeout in seconds, and for Extended Commands. If you enter "y" at the Extended Commands prompt, you can also configure the following:

- source address or interface (none configured by default. Enter an IP/IPv6 address or the complete interface type slot/port as the source of pings. You cannot abbreviate the interface type.)
- type of service (0, by default),
- Set DF bit in IP header (n or not set, by default. Enter y to set the Don't Fragment bit.),
- Validate reply data (n or no, by default. Enter y to validate reply data),
- Data pattern (0xABCD, by default),
- Sweep range of sizes (n or no, by default.)

See Appendix A, ICMP Message Types for information on the ICMP message codes that return from a ping command.

```
Force10#ping 172.31.1.255

Type Ctrl-C to abort.

Sending 5, 100-byte ICMP Echos to 172.31.1.255, timeout is 2 seconds:
Reply to request 1 from 172.31.1.208     0 ms
Reply to request 1 from 172.31.1.216     0 ms
Reply to request 1 from 172.31.1.205     16 ms
:
:
Reply to request 5 from 172.31.1.209     0 ms
Reply to request 5 from 172.31.1.66      0 ms
Reply to request 5 from 172.31.1.87      0 ms

Force10#
```

Figure 24 ping (IPv4) Command Example

Figure 25 displays the **ping** command using a compressed IPv6 address.

```
Force10#ping 100::1

Type Ctrl-C to abort.

Sending 5, 100-byte ICMP Echos to 100::1, timeout is 2 seconds:
!!!!!
Success rate is 100.0 percent (5/5), round-trip min/avg/max = 0/0/0 (ms)
Force10#
```

Figure 25 ping (IPv6) Command Example

power-off

Turn off power to a selected line card or the standby (extra) Switch Fabric Module (SFM).

Syntax **power-off** {**linecard** *number* | **sfm standby**}

Parameters

linecard *number*	Enter the keyword **linecard** and a number for the line card slot number. C-Series Range: 0-7 on the C300 E-Series Range: 0 to 13 on a E1200, 0 to 6 on a E600, and 0 to 5 on a E300.
sfm standby	Enter the keyword **sfm standby** to turn off power to the standby SFM. **Note:** This option is supported on E-Series only.

Defaults Disabled

Command Modes EXEC privilege

Related Commands

power-on	Power on a line card or standby SFM.

power-on

Turn on power to a line card or the standby (extra) Switch Fabric Module (SFM).

Syntax **power-on** {**linecard** *number* | **sfm standby**}

Parameters

linecard *number*	Enter the keyword **linecard** and a number for the line card slot number. C-Series Range: 0-7 on the C300 E-Series Range: 0 to 13 on a E1200, 0 to 6 on a E600/E600i, and 0 to 5 on a E300.
sfm standby	Enter the keyword **sfm** standby to power on the standby SFM. **Note:** This option is supported on E-Series only.

Defaults Disabled

Command Modes EXEC privilege

Related Commands

power-off	Power off a line card or standby SFM.

reload

Reboot the FTOS.

Syntax **reload**

Command Modes EXEC privilege

Usage Information If there is a change in the configuration, FTOS will prompt you to save the new configuration. Or you can save your running configuration with the copy running-config command.

reset

Reset a line card, RPM, a standby SFM (EtherScale only), or a failed SFM (TeraScale only).

Syntax **reset** {**linecard** *number* [**hard**] | **rpm** *number* [**hard**] | **sfm** *slot number* | **standby**}

Parameters

linecard *number*	Enter the keyword **linecard** and a number for the line card slot number. Add the keyword **hard** to power cycle the line card. C-Series Range: 0-7 on the C300 Range: 0 to 13 on a E1200, 0 to 6 on a E600, and 0 to 5 on a E300.
rpm *number*	Enter the keyword **rpm** followed by a number for the RPM slot number. Add the keyword **hard** to power cycle the RPM. Range: 0 to 1.
sfm standby	Enter the keyword **sfm standby** to reset the standby SFM. **Note:** This option is supported on E-Series EtherScale only.
sfm *slot number*	Enter the keyword **sfm** followed by the failed or powered -off SFM slot number. **Note:** Supported on E-Series TeraScale only.

Defaults Disabled.

Command Modes EXEC privilege

Usage Information When a soft reset is issued on a line card (**reset linecard** *number*), FTOS boots the line card from its runtime image. Only when you enter **reset linecard** *number* **hard** is the software image reloaded on the line card.

Related Commands

reload	Reboots the E-Series.

send

Send messages to one or all terminal line users.

Syntax **send** [*] | [*line*] | [**aux**] | [**console**] | [**vty**]

Parameters

*	Enter the asterik character * to send a message to all tty lines.
line	Send a message to a specific line. Range: 0 to 11
aux	Enter the keyword **aux** to send a message to an Auxiliary line. **Note:** This option is supported on E-Series only.
console	Enter the keyword **console** to send a message to the Primary terminal line.
vty	Enter the keyword **vty** to send a message to the Virtual terminal

Defaults No default behavior or values

Command Modes EXEC

Command History

Version 6.5.1.0	Introduced

Usage Information Messages can contain an unlimited number of lines, however each line is limited to 255 characters. To move to the next line, use the <CR>. To send the message use CTR-Z, to abort a message use CTR-C.

service timestamps

Add time stamps to debug and log messages. This command adds either the uptime or the current time and date.

Syntax **service timestamps** [**debug** | **log**] [**datetime** [**localtime**] [**msec**] [**show-timezone**] | **uptime**]

To disable timestamping, use the **no service timestamps** [**debug** | **log**] command.

Parameters

debug	(OPTIONAL) Enter the keyword **debug** to add timestamps to debug messages.
log	(OPTIONAL) Enter the keyword **log** to add timestamps to log messages with severity 0 to 6.
datetime	(OPTIONAL) Enter the keyword **datetime** to have the current time and date added to the message.

localtime	(OPTIONAL) Enter the keyword **localtime** to include the localtime in the timestamp.
msec	(OPTIONAL) Enter the keyword **msec** to include milliseconds in the timestamp.
show-timezone	(OPTIONAL) Enter the keyword **show-timezone** to include the time zone information in the timestamp.
uptime	(OPTIONAL) Enter the keyword **uptime** to have the timestamp based on time elapsed since system reboot.

Defaults Not configured.

Command Modes CONFIGURATION

Usage Information If you do not specify parameters and enter **service timestamps**, it appears as **service timestamps debug uptime** in the running-configuration.

Use the show running-config command to view the current options set for the service timestamps command.

show alarms

View alarms for the RPM, SFMs, line cards and fan trays.

Syntax **show alarms** [**threshold**]

Parameters

threshold	(OPTIONAL) Enter the keyword **threshold** to display the temperature thresholds set for the line cards, RPM, and SFMs.

Command Modes EXEC

EXEC privilege

Example

```
Force10# show alarms

--  Minor Alarms  --
Alarm Type                                  Duration
-------------------------------------------------
RPM 0 PEM A failed or rmvd                  7 hr, 37 min
SFM 0 PEM A failed or rmvd                  7 hr, 37 min
SFM 1 PEM A failed or rmvd                  7 hr, 37 min
SFM 2 PEM A failed or rmvd                  7 hr, 37 min
SFM 3 PEM A failed or rmvd                  7 hr, 37 min
SFM 4 PEM A failed or rmvd                  7 hr, 37 min
SFM 5 PEM A failed or rmvd                  7 hr, 37 min
SFM 6 PEM A failed or rmvd                  7 hr, 37 min
SFM 7 PEM A failed or rmvd                  7 hr, 36 min
line card 1 PEM A failed or rmvd            7 hr, 36 min
line card 4 PEM A failed or rmvd            7 hr, 36 min
only 8 SFMs in chassis                      7 hr, 35 min

--  Major Alarms  --
Alarm Type                                  Duration
-------------------------------------------------
No major alarms

Force10#
```

Figure 26 show alarms Command Example

show chassis

View the configuration and status of modules in the E-Series chassis. Use this command to determine the chassis mode.

Syntax **show chassis** [**brief**]

Parameters

brief	(OPTIONAL) Enter the keyword **brief** to view a summary of the show chassis output.

Command Modes EXEC

EXEC privilege

Example

```
Force10#Force10#show chassis brief
Chassis Type  : E1200
Chassis Mode  : TeraScale
Chassis Epoch : 3.2 micro-seconds

--  Line cards  --
Slot  Status        NxtBoot    ReqTyp   CurTyp   Version     Ports
--------------------------------------------------------------------------------
  0   not present
  1   not present
  2   not present
  3   not present
  4   not present
  5   not present
  6   not present
  7   not present
  8   not present
  9   not present
 10   not present
 11   online        online     E48PF    E48PF    6.1.1.0      48
 12   not present              E48PF
 13   not present              E48PF
--  Route Processor Modules --
Slot  Status        NxtBoot    Version
--------------------------------------------------------------------------------
  0   active        online     6.1.1.0
  1   not present

Switch Fabric State:  up

--  Switch Fabric Modules  --
Slot  Status
--------------------------------------------------------------------------------
  0   active
  1   active
  2   active
  3   active
  4   active
  5   active
  6   active
  7   active
  8   active

--  Power Entry Modules  --
Bay   Status
--------------------------------------------------------------------------------
  0   up
  1   up

--  Fan Status  --
Tray  Status  Temp    Volt    Speed               PEM0  PEM1   Fan1  Fan2  Fan3
------------------------------------------------------------------------------
 0    up      < 50C   12-16V  low/2100-2700 RPM   up    up     up    up    up
 1    up      < 50C   12-16V  low/2100-2700 RPM   up    up     up    up    up
 2    up      < 50C   12-16V  low/2100-2700 RPM   up    up     up    up    up
 3    up      < 50C   12-16V  low/2100-2700 RPM   up    up     up    up    up
```

Figure 27 show chassis brief Command Example

Related Commands

show linecard	View line card status
show rpm	View Route Processor Module status.
show sfm	View Switch Fabric Module status.

show console lp

C-Series	✓
E-Series	No

View the buffered boot-up log of a line card.

Syntax **show console lp** *number*

Parameters

number	Enter the line card slot number. Range: 0-7 for the C300

Defaults None.

Command Mode EXEC

EXEC privilege

Usage Information

Note: Use this command only when you are working directly with a technical support representative to troubleshoot a problem. Do not use this command unless a technical support representative instructs you to do so.

show cpu-traffic-stats

View the CPU traffic statistics.

Syntax **show cpu-traffic-stats** [*port number* | **all** | **cp** | **rp1** | **rp2**]

Parameters

port number	(OPTIONAL) Enter the port number to display traffic statistics on that port only. Range: 1 to 1568
all	(OPTIONAL) Enter the keyword **all** to display traffic statistics on all the interfaces receiving traffic, sorted based on traffic.
cp	(OPTIONAL) Enter the keyword **cp** to display traffic statistics on the specified CPU.
rp1	(OPTIONAL) Enter the keyword **rp1** to display traffic statistics on the RP1. **Note:** This option is supported on E-Series only.
rp2	(OPTIONAL) Enter the keyword **rp2** to display traffic statistics on the RP2. **Note:** This option is supported on E-Series only.

Defaults **all**

Command Modes EXEC

Command History

Version 6.2.1.1	Introduced

Example

```
Force10#show cpu-traffic-stats
Processor : CP
--------------
   Received 100% traffic on GigabitEthernet 8/2   Total packets:100
       LLC:0, SNAP:0, IP:100, ARP:0, other:0
       Unicast:100, Multicast:0, Broadcast:0

Processor : RP1
---------------
   Received 62% traffic on GigabitEthernet 8/2   Total packets:500
       LLC:0, SNAP:0, IP:500, ARP:0, other:0
       Unicast:500, Multicast:0, Broadcast:0

   Received 37% traffic on GigabitEthernet 8/1   Total packets:300
       LLC:0, SNAP:0, IP:300, ARP:0, other:0
       Unicast:300, Multicast:0, Broadcast:0

Processor : RP2
---------------
   No CPU traffic statistics.
Force10#
```

Figure 28 show cpu-traffic-stats Command Example

Usage Information

The traffic statistics is sorted on a per Interface bases; the Interface receiving the most traffic is displayed first. All CPU and Port information is displayed unless specific Port or CPU is specified. Traffic information is displayed for router ports only; not for management interfaces. The traffic statistics are collected only after the debug cpu-traffic-stats command is executed; not from the system boot up.

Note: After debugging is complete, use the no debug cpu-traffic-stats to shut off traffic statistics collection.

Related Commands

debug cpu-traffic-stats	Enable CPU traffic statistics for debugging

show debugging

View a list of all enabled debugging processes.

Syntax **show debugging**

Command Mode EXEC privilege

Example

```
Force10#show debug
Generic IP:
  IP packet debugging is on for
    ManagementEthernet 0/0
    Port-channel 1-2
    Port-channel 5
    GigabitEthernet 4/0-3,5-6,10-11,20
    GigabitEthernet 5/0-1,5-6,10-11,15,17,19,21
  ICMP packet debugging is on for
    GigabitEthernet 5/0,2,4,6,8,10,12,14,16
Force10#
```

Figure 29 show debugging Command Example

show environment

View E-Series system component status (for example, temperature, voltage).

Syntax **show environment** [**all** | **fan** | **linecard** | **linecard-voltage | PEM** | **RPM** | **SFM**]

Parameters

all	Enter the keyword **all** to view all components.
fan	Enter the keyword **fan** to view information on the fans. The output of this command is chassis dependent. See Figure 30, Figure 31, and Figure 32 for a comparison of output.
linecard	Enter the keyword **linecard** to view only information on line cards
linecard-voltage	Enter the keyword **linecard-voltage** to view line card voltage information.
PEM	Enter the keyword **pem** to view only information on power entry modules.
RPM	Enter the keyword **rpm** to view only information on RPMs.
SFM	Enter the keyword **sfm** to view only information on SFMs. **Note:** This option is supported on E-Series only.

Command Modes EXEC

EXEC privilege

Example 1

```
Force10#show environment

--  Fan Status  --
Tray  Status  Temp    Volt    Speed               PEM0  PEM1   Fan1  Fan2  Fan3
-------------------------------------------------------------------------------
 0    up      < 50C   12-16V  low/2100-2700 RPM   up    up     up    up    up
 1    up      < 50C   12-16V  low/2100-2700 RPM   up    up     up    up    up
 2    up      < 50C   12-16V  low/2100-2700 RPM   up    up     up    up    up
 3    up      < 50C   12-16V  low/2100-2700 RPM   up    up     up    up    up
 4    up      < 50C   16-20V  med/2700-3200 RPM   up    up     up    up    up
 5    up      < 50C   12-16V  low/2100-2700 RPM   up    up     up    up    up
--  Power Entry Modules  --
Bay   Status
-------------------------------------------------------------------------------
  0   absent or down
  1   up

--  Line Card Environment Status  --
Slot  Status        Temp   PEM0  PEM1   Voltage
-------------------------------------------------------------------------------
  0   not present
  1   not present
  2   not present
  3   not present
  4   not present
  5   not present
  6   not present
  7   not present
  8   not present
  9   not present
 10   not present
 11   booting       53C    down  up     ok
 12   not present
 13   not present

--  RPM Environment Status  --
Slot  Status        Temp   PEM0  PEM1   Voltage
-------------------------------------------------------------------------------
  0   active        48C    down  up     ok
  1   not present

--  SFM Environment Status  --
Slot  Status        Temp   PEM0  PEM1
-------------------------------------------------------------------------------
  0   active        49C    up    up
  1   active        47C    up    up
  2   active        46C    up    up
  3   active        48C    up    up
  4   active        52C    up    up
  5   active        50C    up    up
  6   active        47C    up    up
  7   active        48C    up    up
  8   active        47C    up    up
Force10#
```

Figure 30 show environment Command Example for the E1200

Example 2

```
Force10#show environment fan

--  Fan Status  --
Status  Temp   Fan1      Fan2      Fan3     Serial Num    Version
-------------------------------------------------------------------
  up    29C   6000 RPM  7500 RPM  7500 RPM                 0.0

Force10#
```

Figure 31 show environment fan Command Example on the E600

Example 3

```
Force10#show environment fan

--  Fan Status  --
Status
------------------------------------------------------------------
  up

Force10#
```

Figure 32 show environment fan Command Example on the E300

show inventory

Display the chassis type, components (including media), FTOS version including hardware identification numbers and configured protocols.

Syntax **show inventory** [**media** *slot*]

Parameters

media *slot*	(OPTIONAL) Enter the keyword **media** followed by the slot number. C-Series Range: 0-7 on the C300 E-Series Range: 0 to 13 on a E1200, 0 to 6 on a E600/E600i, and 0 to 5 on a E300

Defaults No default behavior or values

Command Modes CONFIGURATION

Command History

Version 7.5.1.0	Expanded to include transceiver media
Version 6.2.1.0	Expanded to include Software Protocol Configured field
Version 5.3.1.0	Introduced

Usage Information The display output may include a double asterisk (**) next to the SFMs, for example:

```
...
0     CC-E-SFM **   0004875       7490007411   A
1     CC-E-SFM **   0004889       7490007411   A
...
```

The double asterisk generally indicates the SFM's frequency capabilities. These SFMs are either operating at 125 MHz or the frequency capability, which is stored in an EPROM, cannot be determined.

Example

```
Force10#show inventory media 3
Slot Port Type Media        Vendor           Serial Number    F10Qualified
------------------------------------------------------------------------------
...
   3   11 SFP  1000BASE-SX  FINISAR CORP.    U9600L0          Yes
...
```

Figure 33 show inventory media (partial) Command Example

Example

```
Force10# show inventory
Chassis Type     : E300
Chassis Mode     : TeraScale
Software Version : FTOS-EF-7.5.1.0

Slot Item               Serial Number  Part Number  Revision
--------------------------------------------------------------
     E300               0015259        7520009601   02
  1  LC-EF3-10GE-2P     0017259        7520012501   01
  2  LC-EF3-GE-48T      0017269        7520009702   01
  3  LC-EF3-1GE-24P     0031151        7520014206   04
  4  LC-EF3-1GE-24P     0017291        7520014202   02
  0  LC-EF3-RPM         0031177        7520013808   05
  0  CC-E-SFM           0019071        7520003706   A
  1  CC-E-SFM           0019120        7520003706   A
  1  CC-E300-PWR-DC     TDX0524-00031  7520015400   A
  0  CC-E300-FAN        N/A            N/A          N/A

 * - standby


Software Protocol Configured
--------------------------------------------------------------
  BFD
  BGP
  ISIS
  OSPF
  RIP
  OSPFV3

Force10#
```

Figure 34 show inventory Command Example

show linecard

View the line card(s) status.

Syntax **show linecard** [*number* [**brief**] | **all**]

Parameters

number	(OPTIONAL) Enter a slot number to view information on the line card in that slot. C-Series Range: 0-7 on the C300 E-Series Range: 0 to 13 on a E1200, 0 to 6 on a E600, and 0 to 5 on a E300.
all	(OPTIONAL) Enter the keyword **all** to view a table with information on all present line cards.
brief	(OPTIONAL) Enter the keyword **brief** to view an abbreviated list of line card information.

Command Modes EXEC

EXEC privilege

Example

```
Force10#Force10#  show linecard 11

--  Line card 11 --
Status         : online
Next Boot      : online
Required Type  : E48PF - 48-port GE line card with SFP optics (EF)
Current Type   : E48PF - 48-port GE line card with SFP optics (EF)
Hardware Rev   : Base  - 1.0  PP0 - n/a  PP1 - n/a
Num Ports      : 48
Up Time        : 12 hr, 37 min
FTOS Version   : 6.2.1.x
Jumbo Capable  : yes
Boot Flash     : A: 2.0.3.4 B: 2.0.3.4 [booted]
Memory Size    : 268435456 bytes
Temperature    : 49C
Power Status   : PEM0: absent or down    PEM1: up
Voltage        : ok
Serial Number  :
Part Number    :            Rev
Vendor Id      :
Date Code      :
Country Code   :
Force10#
```

Figure 35 show linecard Command Example

Table 7 list the definitions of the fields shown in Figure 35

Table 7 show linecard Command Example Information

Field	Description
Line card	Displays the line card slot number (only listed in **show linecard all** command output).
Status	Displays the line card's status.
Next Boot	Displays whether the line card is to be brought online at the next system reload.
Required Type	Displays the line card type configured for the slot. The Required Type and Current Type must match. Use the **linecard** command to reconfigure the line card type if they do not match.
Current Type	Displays the line card type installed in the slot. The Required Type and Current Type must match. Use the **linecard** command to reconfigure the line card type if they do not match.
Hardware Rev	Displays the chip set revision.
Num Ports	Displays the number of ports in the line card.
Up Time	Displays the number of hours and minutes the card is online.
FTOS Version	Displays the operating software version.
Jumbo Capable	Displays Yes or No indicating if the line card can support Jumbo frames. This field does not state whether the chassis is operating in EtherScale or TeraScale mode.
Boot Flash Ver	Displays the two possible Bootflash versions. The [Booted] keyword next to the version states which version was used at system boot.
Memory Size	List the memory of the line card processor.

Table 7 show linecard Command Example Information (continued)

Field	Description
Temperature	Displays the temperature of the line card. Minor alarm status if temperature is over 65° C.
Power Status	Lists the type of power modules used in the chassis: • AC = AC power supply • DC = DC Power Entry Module (PEM)
Voltage	Displays OK if the line voltage is within range.
Serial Number	Displays the line card serial number.
Part Num	Displays the line card part number.
Vendor ID	Displays an internal code, which specifies the manufacturing vendor.
Date Code	Displays the line card's manufacturing date.

```
Force10#show linecard 11 brief

--  Line card 11 --
Status        : online
Next Boot     : online
Required Type : E48PF - 48-port GE line card with SFP optics (EF)
Current Type  : E48PF - 48-port GE line card with SFP optics (EF)
Hardware Rev  : Base  - 1.0  PP0 - n/a  PP1 - n/a
Num Ports     : 48
Up Time       : 11 hr, 24 min
FTOS Version  : 6.1.1.0
Jumbo Capable : yes
Force10#
```

Figure 36 show linecard brief Command Example

Related Commands

show chassis	View information on all elements of the E-Series chassis.
show rpm	View information on the RPM.
show sfm	View information on the SFM.

show linecard boot-information

View the line card status and boot information.

Syntax **show linecard boot-information**

Command Modes EXEC

EXEC Privilege

Command History

Version 6.5.1.4	Introduced

Example

```
Force10#show linecard boot-information

-- Line cards --
                    Serial    Booted       Next       Cache                    Boot
# Status  CurType   number    from         boot       boot                     flash
-------------------------------------------------------------------------------------------------
0 online  EXW4PF    012345    B: 6.5.1.4   6.5.1.4    A: invalid  B: 6.5.1.4   A: 2.3.0.8 [b] B: invalid

1    -

2 online  E48TF     0031318   6.5.1.4      6.5.1.4    A: invalid  B: 6.5.1.4   A: 2.3.0.6  B: 2.3.0.8 [b]

3    -

4    -

5    -

6    -
Force10#
```

Figure 37 show linecard boot-information Command

Table 8 defines the fields in Figure 37.

Table 8 show linecard boot-information output definitions

Field	Description
#	Displays the line card slot numbers, beginning with slot 0. The number of slots listed is dependent on your chassis: C-Series: 0-7 on the C300 E-Series: 0 to 13 on a E1200, 0 to 6 on a E600/E600i, and 0 to 5 on a E300.
Status	Indicates if a line card is online, offline, or booting. If a line card is not detected in the slot, a hyphen (**-**) is displayed.
CurType	Displays the line card identification number, for example EXW4PF.
Serial number	Displays the line card serial number.
Booted from	Indicates whether the line card cache booted or system booted. In addition, the image with which the line card booted is also displayed. If the line card cache booted, then the output is A: or B: followed by the image in the flash partition (A: 6.5.1.4 or B: 6.5.1.4). If the line card system booted, then display is the current FTOS version number (6.5.1.4).
Next boot	Indicates if the next line card boot is a cache boot or system boot and which image will be used in the boot.

Table 8 show linecard boot-information output definitions

Field	Description
Cache boot	Displays the system image in cache boot flash partition A: and B: for the line card. If the cache boot does not contain a valid image, “invalid” is displayed.
Boot flash	Displays the two possible Boot flash versions. The [b] next to the version number is the current boot flash, that is the image used in the last boot.

Usage Information

The display area of this command uses the maximum 80 character length. If your display area is not set to 80 characters, the display will wrap.

Related Commands

show linecard	View the line card status
upgrade	Upgrade the boot flash, boot selector, or system image
download alt-boot-image	Download an alternate boot image to the chassis
download alt-full-image	Download an alternate FTOS image to the chassis
download alt-system-image	Download an alternate system image to the chassis

show memory

View current memory usage on the E-Series.

Syntax

show memory [**cp** | **lp** *slot-number* | **rp1** | **rp2**]

Parameters

cp	(OPTIONAL) Enter the keyword **cp** to view information on the Control Processor on the RPM.
lp *slot-number*	(OPTIONAL) Enter the keyword **lp** and the slot number to view information on the line-card processor in that slot. C-Series Range: 0-7 on the C300 E-Series Range: 0 to 13 on a E1200, 0 to 6 on a E600, and 0 to 5 on a E300.
rp1	(OPTIONAL) Enter the keyword **rp1** to view information on Route Processor 1 on the RPM. **Note:** This option is supported on the E-Series only.
rp2	(OPTIONAL) Enter the keyword rp2 to view information on Route Processor 2 on the RPM. **Note:** This option is supported on the E-Series only.

Command Modes

EXEC

EXEC privilege

Usage Information

In FTOS Release 7.4.1.0 and higher, the total counter size (for all 3 CPUs) in show memory and show processes memory will differ based on which FTOS processes are counted.

- In the show memory display output, the memory size is equal to the size of the application processes.
- In the show processes memory display output, the memory size is equal to the size of the application processes *plus* the size of the system processes.

Example

```
Force10#show memory
     Statistics On  CP Processor
     ============================
   Total(b)      Used(b)       Free(b)      Lowest(b)      Largest(b)
   452689184      64837834     387851350    387805590    371426976
     Statistics On RP1 Processor
     ============================
   Total(b)      Used(b)       Free(b)      Lowest(b)      Largest(b)
   629145600       4079544     625066056    625066056             0
     Statistics On RP2 Processor
     ============================
   Total(b)      Used(b)       Free(b)      Lowest(b)      Largest(b)
   510209568      47294716     462914852    462617968    446275376
Force10#
```

Figure 38 show memory Command Example

Table 9 defines the fields displayed in Figure 38.

Table 9 show memory Command Example Information

Field	Description
Lowest	Displays the memory usage the system went to in the lifetime of the system. Indirectly, it indicates the maximum usage in the lifetime of the system: Total minus Lowest.
Largest	The current largest available. This relates to block size and is not related to the amount of memory on the system.

show processes communication (deprecated)

Command History

Version 7.5.1.0	Deprecated (see show processes ipc flow-control)
Version 6.5.4.0	Introduced

show processes cpu

View CPU usage information based on processes running in the E-Series.

Syntax **show processes cpu** [**cp** | **rp1** | **rp2**] [**lp** *linecard-number* | *linecard-number number of task with highest CPU usage last 5 seconds* | **all** | **summary**]

Parameters

cp	(OPTIONAL) Enter the keyword **cp** to view CPU usage of the Control Processor.
rp1	(OPTIONAL) Enter the keyword **rp1** to view CPU usage of the Route Processor 1. **Note:** This option is supported on the E-Series only.
rp2	(OPTIONAL) Enter the keyword **rp2** to view CPU usage of the Route Processor 2. **Note:** This option is supported on the E-Series only.
lp *linecard-number*	(OPTIONAL) Enter the keyword **lp** followed by the line card number to view the CPU usage of that line card.
lp *linecard-number number of task with highest CPU usage last 5 seconds*	(OPTIONAL) Enter the keyword **lp** followed by the line card number and the task number with the highest CPU usage within the past 5 seconds, to view the line card highest CPU usage over the past 5 seconds.
lp all	(OPTIONAL) Enter the keyword **lp all** to view CPU utilization on all active line cards.
lp summary	(OPTIONAL) Enter the keyword **lp summary** to view a summary of the line card CPU utilization.

Command Modes EXEC

EXEC privilege

Command History

Version 7.4.1.0	Added the **lp all** option
Version 6.5.1.0	The granularity of the output for rp1 and rp2 is changed. The granularity of the output is now at the process level, and hence process specific statistics are now displayed.

Example

```
Force10#show processes cpu
     CPU Statistics On  CP Processor
     ================================

CPU utilization for five seconds: 4%/2%; one minute: 2%; five minutes: 2%
PID        Runtime(ms)    Invoked       uSecs     5Sec     1Min     5Min  TTY     Process
0xd02e4e8     1498633      89918       16666    3.00%    2.67%    2.67%    0          KP
0xd9d4c70           0          0           0    0.00%    0.00%    0.00%    0     tLogTask
0xd9cd200           0          0           0    0.00%    0.00%    0.00%    0     soc_dpc
0xd9bf588           0          0           0    0.00%    0.00%    0.00%    0        tARL
0xd9bd2f8           0          0           0    0.00%    0.00%    0.00%    0    tBCMlink
0xd9bb0e0         700         42       16666    0.00%    0.00%    0.00%    0    tBcmTask
0xd9798d0      106683       6401       16666    0.00%    0.00%    0.00%    0    tNetTask
0xd3368a0           0          0           0    0.00%    0.00%    0.00%    0    tWdbTask
0xd3329b0         166         10       16600    0.00%    0.00%    0.00%    0    tWdtTask
0xd32a8c8      102500       6150       16666    0.00%    0.00%    0.00%    0         tme
0xd16b1d8       12050        723       16666    0.00%    0.00%    0.00%    0         ipc
0xd1680c8          33          2       16500    0.00%    0.00%    0.00%    0         irc
0xd156008         116          7       16571    0.00%    0.00%    0.00%    0  RpmAvailMgr
0xd153ab0         216         13       16615    0.00%    0.00%    0.00%    0          ev
-more-
```

Figure 39 show processes cpu Command Example (Partial)

Example

```
Force10#Force10>show processes cpu rp1

CPU utilization for five seconds: 0%/0%; one minute: 0%; five minutes: 0%
PID        Runtime(ms)    Invoked       uSecs     5Sec     1Min     5Min TTY          Process

0x0000007c          60          6       10000    0.00%    0.00%    0.00%   0            ospf
0x00000077         460         46       10000    0.00%    0.00%    0.00%   0             dsm
0x00000074         100         10       10000    0.00%    0.00%    0.00%   0            ipm1
0x0000006e         180         18       10000    0.00%    0.00%    0.00%   0             rtm
0x0000006b         100         10       10000    0.00%    0.00%    0.00%   0             rip
0x00000068         120         12       10000    0.00%    0.00%    0.00%   0             acl
0x00000064         690         69       10000    0.00%    0.00%    0.00%   0            sysd1
0x00000062          20          2       10000    0.00%    0.00%    0.00%   0           sysmon
0x00000024         880         88       10000    0.00%    0.00%    0.00%   0            sshd
0x00000022           0          0           0    0.00%    0.00%    0.00%   0           inetd
0x00000020        2580        258       10000    0.00%    0.00%    0.00%   0       mount_mfs
0x00000013           0          0           0    0.00%    0.00%    0.00%   0       mount_mfs
0x00000006          80          8       10000    0.00%    0.00%    0.00%   0              sh
0x00000005          30          3       10000    0.00%    0.00%    0.00%   0        aiodoned
0x00000004         840         84       10000    0.00%    0.00%    0.00%   0         ioflush
0x00000003         250         25       10000    0.00%    0.00%    0.00%   0          reaper
0x00000002           0          0           0    0.00%    0.00%    0.00%   0       pagedaemon
0x00000001         160         16       10000    0.00%    0.00%    0.00%   0            init
0x00000000         700         70       10000    0.00%    0.00%    0.00%   0          swapper
0x00000088         260         26       10000    0.00%    0.00%    0.00%   0             bgp
```

Figure 40 show processes cpu rp1 Command Example

Example

```
Force10#show processes cpu rp2

CPU utilization for five seconds: 0%/0%; one minute: 0%; five minutes: 0%

PID        Runtime(ms)    Invoked       uSecs     5Sec     1Min     5Min TTY          Process

0x00000090         140         14       10000    0.00%    0.00%    0.00%   0            vrrp
0x0000008d         120         12       10000    0.00%    0.00%    0.00%   0            fvrp
0x00000088         360         36       10000    0.00%    0.00%    0.00%   0            xstp
0x00000084          60          6       10000    0.00%    0.00%    0.00%   0            span
0x00000083         180         18       10000    0.00%    0.00%    0.00%   0             pim
0x00000080          80          8       10000    0.00%    0.00%    0.00%   0            igmp
0x0000007b         130         13       10000    0.00%    0.00%    0.00%   0            ipm2
0x00000078         700         70       10000    0.00%    0.00%    0.00%   0            mrtm
0x00000074         100         10       10000    0.00%    0.00%    0.00%   0           l2mgr
0x00000070          80          8       10000    0.00%    0.00%    0.00%   0            l2pm
0x0000006c          80          8       10000    0.00%    0.00%    0.00%   0            arpm
0x00000068          60          6       10000    0.00%    0.00%    0.00%   0            acl2
0x00000064         750         75       10000    0.00%    0.00%    0.00%   0           sysd2
0x00000062           0          0           0    0.00%    0.00%    0.00%   0          sysmon
0x00000024         880         88       10000    0.00%    0.00%    0.00%   0            sshd
0x00000022           0          0           0    0.00%    0.00%    0.00%   0          inetd
0x00000020        2250        225       10000    0.00%    0.00%    0.00%   0       mount_mfs
0x00000013           0          0           0    0.00%    0.00%    0.00%   0       mount_mfs
0x00000006         100         10       10000    0.00%    0.00%    0.00%   0             sh
0x00000005           0          0           0    0.00%    0.00%    0.00%   0        aiodoned
0x00000004         960         96       10000    0.00%    0.00%    0.00%   0         ioflush
0x00000003         140         14       10000    0.00%    0.00%    0.00%   0          reaper
0x00000002           0          0           0    0.00%    0.00%    0.00%   0      pagedaemon
0x00000001         160         16       10000    0.00%    0.00%    0.00%   0            init
0x00000000         700         70       10000    0.00%    0.00%    0.00%   0         swapper
0x00000098         140         14       10000    0.00%    0.00%    0.00%   0            msdp
```

Figure 41 show processes cpu rp2 Command Example

Usage Information

The CPU utilization for the last five seconds as shown in Figure 39 is 4%/2%. The first number (4%) is the CPU utilization for the last five seconds. The second number (2%) indicates the percent of CPU time spent at the interrupt level.

show processes ipc flow-control

Display the Single Window Protocol Queue (swpq) statistics.

Syntax

show processes ipc flow-control [**cp** | **rp1** | **rp2** | **lp** *linecard-number*]

Parameters

cp	(OPTIONAL) Enter the keyword **cp** to view the Control Processor's swpq statistics.
rp1	(OPTIONAL) Enter the keyword **rp1** to view the Control Processor's swpq statistics on Route Processor 1.
rp2	(OPTIONAL) Enter the keyword **rp2** to view the Control Processor's swpq statistics on Route Processor 2.
lp *linecard-number*	(OPTIONAL) Enter the keyword **lp** followed by the line card number to view the Control Processor's swpq statistics on the specified line card.

Defaults No default values or behavior

Command Modes EXEC

EXEC privilege

Command History

Version 7.5.1.0	Introduced

Example

```
Force10# show processes ipc flow-control rp2

[qid] Source->Dest          Cur High #of #of  #msg   #msg Retr total
                            Len Mark to  Retr Sent   Ackd
-------------------------------------------------------------------
[1] unknown2->unknown2      0    0   0   0    0      0    3    3
[2] l2pm0->spanMgr0         0    2   0   0    2298   2298 25   25
[3] fvrp0->macMgr0          0    0   0   0    0      0    25   25
[4] l2pm0->fvrp0            0    2   0   0    1905   1905 25   25
[5] fvrp0->l2pm0            0    0   0   0    0      0    25   25
[6] stp0->l2pm0             0    0   0   0    0      0    25   25
[7] spanMgr0->macMgr0       0    0   0   0    0      0    25   25
[8] spanMgr0->ipMgr0        0    0   0   0    0      0    25   25
Force10#
```

Figure 42 show processes ipc flow-control rp Command Example

Example

```
Force10#show processes ipc flow-control lp 10
Q Statistics on LP 10
       TxProcess  RxProcess          Cur     High   Time   Retries   Msg     Ack    Aval    Max
                                     Len     Mark   Out              Sent    Rcvd   Retra   Retra
-------------------------------------------------------------------------------------------------
  ACL_AGENT10          PIM0          0        0      0      0         0       0      20      20
  ACL_AGENT10          PIM0          0        0      0      0         0       0      20      20
    FRRPAGT10         FRRP0          0        0      0      0         0       0      30      30
      IFAGT10        IFMGR0          0        1      0      0         1       1       8       8
LPDMACAGENT10       MACMGR0          0        0      0      0         0       0      25      25
Force10#
```

Figure 43 show processes ipc flow-control lp Command Example

Usage Information The Single Window Protocol (SWP) provides flow-control-based reliable communication between the sending and receiving software tasks.

Important Points to Remember

- A sending task enqueues messages into the SWP queue3 for a receiving task and waits for an acknowledgement.
- If no response is received within a period of time, the SWP time-out mechanism re-submits the message at the head of the FIFO queue.
- After retrying several times, the following time-out message is generated:

  `SWP-2-NOMORETIMEOUT`

- In the display output in Figure 43, a retry (Retries) value of zero indicates that the SWP mechanism reached the maximum number of retransmissions without an acknowledgement.

show processes memory

View memory usage information based on processes running in the E-Series.

Syntax

show processes memory [**cp** | **lp** *slot-number* {**lp all | lp summary**} | **rp1** | **rp2**]

Parameters

cp	(OPTIONAL) Enter the keyword **cp** to view memory usage of the Control Processor.
lp *slot-number*	(OPTIONAL) Enter the keyword **lp** and the slot number to view information on the line-card processor in that slot. C-Series Range: 0-7 on the C300 E-Series Range: 0 to 13 on a E1200, 0 to 6 on a E600, and 0 to 5 on a E300.
lp all	(OPTIONAL) Enter the keyword **lp all** to view CP memory usage on all active line cards.
lp summary	(OPTIONAL) Enter the keyword **lp summary** to view a summary of the line card CP memory usage.
rp1	(OPTIONAL) Enter the keyword **rp1** to view memory usage of the Route Processor 1. **Note:** This option is supported on the E-Series only.
rp2	(OPTIONAL) Enter the keyword **rp2** to view memory usage of the Route Processor 2. **Note:** This option is supported on the E-Series only.

Command Modes

EXEC

EXEC privilege

Command History

Version 7.4.1.0	Added **lp all** and **lp summary** options
Version 6.5.1.0	For rp1 and rp2 only, the output displays memory consumption of all the processes including a summary (see Figure 45 on page 151 and Figure 46 on page 152.

Usage Information

In FTOS Release 7.4.1.0 and higher, the total counter size (for all 3 CPUs) in show memory and show processes memory will differ based on which FTOS processes are counted.

- In the show memory display output, the memory size is equal to the size of the application processes.
- In the show processes memory display output, the memory size is equal to the size of the application processes *plus* the size of the system processes.

Example

```
Force10#show processes memory
     Memory Statistics On  CP Processor (bytes)
     ===========================================
Total:   452689184, MaxUsed:    64886986, CurrentUsed:    64873866, Current
    TaskName  TotalAllocated     TotalFreed       MaxHeld  CurrentHolding
   tRootTask        39083408        1395840      38143920        37687568
        tARL              64              0            64              64
    tBcmTask             256              0           256             256
   tPortmapd           18560              0         18560           18560
      tShell            3440              0          3440            3440
   tPingTmo0               0           1088             0               0
    tExcTask               0         592864             0               0
         tme         4002494            192       4002302         4002302
         ipc           34060            192         34060           33868
         irc          943436              0        943436          943436
 RpmAvailMgr            9376             32          9344            9344
          ev          133188              0        133188          133188
      evterm           26752              0         26752           26752
      evhdlr            2528           8064          2528               0
         dlm         7556256        7366960       1239104          189296
         dla             416              0           416             416
         tsm           15136              0         15136           15136
         fmg          766560              0        766560          766560
    fileProc             416              0           416             416
   sysAdmTsk           42028              0         42028           42028
```

Figure 44 show processes memory (partial) Command Example

Example

```
Force10#show processes memory rp1

Total      :   954650624, MaxUsed    :   114135040 [3/8/2006 15:1:42]
CurrentUsed:   114135040, CurrentFree:   840515584
SharedUsed :     7849096, SharedFree :    13122448

 PID   Process        ResSize       Size       Allocs       Frees        Max       Current

 124 ospf             3215360     425984            0           0          0             0
 119 dsm              7749632    1859584       797026           0     797026        797026
 114 ipm1             3821568     229376       297324           0     297324        297324
 112 rtm              4722688     421888       925008           0     925008        925008
 107 rip              3731456     253952       198216           0     198216        198216
 104 acl              4734976     430080      1127524           0    1127524       1127524
 100 sysd1           11636736    2019328       965798           0     965798        965798
  98 sysmon            528384      94208            0           0          0             0
  36 sshd             1286144     430080            0           0          0             0
  34 inetd             663552      98304            0           0          0             0
  32 mount_mfs       42397696    2514944            0           0          0             0
  19 mount_mfs         364544    2449408            0           0          0             0
   6 sh                446464     737280            0           0          0             0
   5 aiodoned        76529664          0            0           0          0             0
   4 ioflush         76529664          0            0           0          0             0
   3 reaper          76529664          0            0           0          0             0
   2 pagedaemon      76529664          0            0           0          0             0
   1 init              139264    2375680            0           0          0             0
   0 swapper         76529664          0            0           0          0             0
```

Figure 45 show processes memory rp1 Command Example

Example

```
Force10#show processes memory rp2

Total      :   953700352, MaxUsed    :   149417984 [3/8/2006 12:33:6]
CurrentUsed:   149417984, CurrentFree:   804282368
SharedUsed :     7847200, SharedFree :    13124344

 PID   Process        ResSize       Size       Allocs       Frees        Max       Current

 145 vrrp             3870720     266240      297324           0      297324      297324
 141 fvrp             4472832     204800      797010           0      797010      797010
 138 xstp            10764288    7155712      367534           0      367534      367534
 133 span             4136960     167936      565810           0      565810      565810
 132 pim              6664192     516096     2812528           0     2812528     2812528
 128 igmp             4112384     344064      627684           0      627684      627684
 124 ipm2             3923968     237568      363396           0      363396      363396
 120 mrtm            25567232     593920      697790           0      697790      697790
 116 l2mgr            4579328     520192      830098           0      830098      830098
 112 l2pm             3874816     225280      367446       32948      367446      334498
 108 arpm             3702784     208896      268420           0      268420      268420
 104 acl2             3485696      94208      132144           0      132144      132144
 100 sysd2           11657216    1679360      998834           0      998834      998834
  98 sysmon            528384      94208           0           0           0           0
  36 sshd             1286144     430080           0           0           0           0
  34 inetd             663552      98304           0           0           0           0
  32 mount_mfs       41791488    2514944           0           0           0           0
  19 mount_mfs         364544    2449408           0           0           0           0
   6 sh                446464     737280           0           0           0           0
   5 aiodoned        76967936          0           0           0           0           0
   4 ioflush         76967936          0           0           0           0           0
   3 reaper          76967936          0           0           0           0           0
   2 pagedaemon      76967936          0           0           0           0           0
   1 init              139264    2375680           0           0           0           0
   0 swapper         76967936          0           0           0           0           0
Force10#
```

Figure 46 show processes memory rp2 Command Example

Table 10 defines the fields that appear in Figure 45 and Figure 46

Table 10 show processes memory rp1/rp2

Field	Description
Total:	Total system memory available
MaxUsed:	Total maximum memory used ever (history indicated with time stamp)
CurrentUsed:	Total memory currently in use
CurrentFree:	Total system memory available
SharedUsed:	Total used shared memory
SharedFree:	Total free shared memory
PID	Process ID
Process	Process Name
ResSize	Actual resident size of the process in memory
Size	Process test, stack, and data size
Allocs	Total dynamic memory allocated
Frees	Total dynamic memory freed
Max	Maximum dynamic memory allocated
Current	Current dynamic memory in use

show processes switch-utilization

C-Series	No
E-Series	✓

Show switch fabric utilization.

Syntax **show processes switch-utilization**

Command Mode EXEC

EXEC privilege

Example

```
Force10#show processes switch-utilization

 Switch fabric utilization        5Sec    1Min    5Min
 ------------------------------------------
                                  3%      3%      3%
```

Figure 47 show processes switch-utilization Command Example

Usage Information An asterisk (*) in the output indicates a legacy card that is not support by the **show processes switch-utilization** command.

show rpm

View the current RPM status.

Syntax **show rpm** [*number* [**brief**] | **all**]

Parameters

number	(OPTIONAL) Enter either zero (0) or 1 for the RPM.
all	(OPTIONAL) Enter the keyword **all** to view a table with information on all present RPMs.
brief	(OPTIONAL) Enter the keyword **brief** to view an abbreviated list of RPM information.

Command Modes EXEC

EXEC privilege

Example

```
Force10#show RPM 0

-- RPM card 0 --
Status         : active
Next Boot      : online
Card Type      : RPM - Route Processor Module (LC-EF-RPM)
Hardware Rev   : 2.0
Num Ports      : 1
Up Time        : 36 min, 51 sec
Last Restart   : reset
FTOS Version   : 6.2.1.0
Jumbo Capable : yes
CP Boot Flash : A: 2.4.0.6              B: 2.4.0.7 [booted]
RP1 Boot Flash: A: 2.4.0.7 [booted]   B: 2.4.0.5
RP2 Boot Flash: A: 2.4.0.7 [booted]   B: 2.4.0.5
CP Mem Size    : 536870912 bytes
RP1 Mem Size   : 0 bytes
RP2 Mem Size   : 0 bytes
Temperature    : 49C
Power Status   : PEM0: absent or down    PEM1: up
Voltage        : ok
Serial Number : 0016788
Part Number    : 7520013800 Rev 01
Vendor Id      : 01
Date Code      : 06182004
Country Code   : 01
Force10#
```

Figure 48 show rpm Command Example

Table 11 defines the fields displayed in Figure 48.

Table 11 show rpm Command Example Information

Field	Description
Status	Displays the RPM's status.
Next Boot	Displays whether the RPM is to be brought online at the next system reload.
Card Type	Displays the RPM catalog number.
Hardware Rev	Displays if the chip set is 1.0 (non-Jumbo) or 1.5 (Jumbo-enabled).
Num Ports	Displays the number of active ports.
Up Time	Displays the number of hours and minutes since the RPM's last reboot.
Last Restart	States the reason for the RPM's last reboot.
FTOS Version	Displays the operating software version.
Jumbo Capable	Displays a Yes or No indicating if the RPM is capable of sending and receiving Jumbo frames. This field does not indicate if the chassis is in Jumbo mode; for that determination, use the **show chassis brief** command.
CP Boot Flash	Displays the two possible Boot Flash versions for the Control Processor. The [Booted] keyword next to the version states which version was used at system boot.
RP1 Boot Flash	Displays the two possible Boot Flash versions for the Routing Processor 1. The [Booted] keyword next to the version states which version was used at system boot.
RP2 Boot Flash	Displays the two possible Boot Flash versions for the Routing Processor 2. The [Booted] keyword next to the version states which version was used at system boot.
CP Mem Size	Displays the memory of the Control Processor.

Table 11 show rpm Command Example Information (continued)

Field	Description
RP1 Mem Size	Displays the memory of the Routing Processor 1.
PR2 Mem Size	Displays the memory of the Routing Processor 2.
Temperature	Displays the temperature of the RPM. Minor alarm status if temperature is over 65° C.
Power Status	Lists the status of the power modules in the chassis.
Voltage	Displays the power rails for the line card.
Serial Num	Displays the line card serial number.
Part Num	Displays the line card part number.
Vendor ID	Displays an internal code, which specifies the manufacturing vendor.
Date Code	Displays the line card's manufacturing date.
Country Code	Displays the country of origin. 01 = USA

Related Commands

show chassis	View information on all elements of the E-Series chassis.
show linecard	View information on a line card.
show sfm	View information on the SFM.

show sfm

View the current SFM status.

Syntax **show sfm** [*number* [**brief**] | **all**]

Parameters

number	Enter a number to view information on that SFM. Range: 0 to 8.
all	(OPTIONAL) Enter the keyword **all** to view a table with information on all present SFMs.
brief	(OPTIONAL) Enter the keyword **brief** to view a list with SFM status.

Command Modes EXEC

EXEC privilege

Example

```
Force10#show sfm

Switch Fabric State:  up

-- SFM card 0 --
Status         : active
Card Type      : SFM - Switch Fabric Module
Up Time        : 37 min, 24 sec
Temperature    : 49C
Power Status   : PEM0: absent or down    PEM1: up
Serial Number  : 0018102
Part Number    : 7520012900 Rev 02
Vendor Id      : 02
Date Code      : 06182004
Country Code   : 01
```

Figure 49 show sfm Command Example (Partial)

Table 12 defines the fields in Figure 48.

Table 12 show sfm Command Output Fields

Field	Description
Switch Fabric State:	States that the Switch Fabric is up (8 SFMs are online and operating).
Status	Displays the SFM's active status.
Card Type	States the type of SFM.
Up Time	Displays the number of hours and minutes since the RPM's last reboot.
Temperature	Displays the temperature of the RPM. Minor alarm status if temperature is over 65° C.
Power Status	Displays power status: absent, down, or up
Serial Num	Displays the line card serial number.
Part Num	Displays the line card part number.
Vendor ID	Displays an internal code, which specifies the manufacturing vendor.
Date Code	Displays the line card's manufacturing date.
Country Code	Displays the country of origin. 01 = USA

```
Force10#show sfm all

Switch Fabric State:  up

--  Switch Fabric Modules  --
Slot  Status
------------------------------------------------------------------------------
  0   active
  1   active
  2   active
  3   active
  4   active
  5   active
  6   active
  7   active
  8   active
Force10#
```

Figure 50 show sfm all Command Example

Related Commands

show chassis	View information on all elements of the E-Series chassis.
show rpm	View information on a RPM.
show sfm	View information on a SFM.

show switch links

C-Series	✓
E-Series	**No**

View the switch fabric backplane or internal status.

Syntax **show switch links** {**backplane** | **internal**}

Parameters

backplane	Enter the keyword **backplane** to view a table with information on the link status of the switch fabric backplane for both SFMs.
internal	Enter the keyword **internal** to view a table with information on the internal status of the switch fabric modules.

Defaults None.

Command Modes EXEC

Command History

Version 4.2.1.0	Introduced

Example

```
Force10# show switch links backplane

Switch fabric backplane link status:

                    SFM0 Links Status                SFM1 Links Status
LC SlotID   Port0 | Port1 | Port2 | Port3 | Port4 | Port5 | Port6 |
Port7

   0         up      up      up      up     down    down    down    down
   1         not present
   2         not present
   3         not present
   4         not present
   5         not present
   6         up      up      up      up     down    down    down    down
   7         not present

up - Both ends of the link are up
down - Both ends of the link are down
up / down - SFM side up and LC side down
down / up - SFM side down and LC side up
Force10#
```

show tech-support

C-Series	✓
E-Series	No

View the information necessary for Force10 Networks technical support to perform troubleshooting. The output includes show version and show version commands.

Syntax **show tech-support [page]**

Parameters

page	(OPTIONAL) Enter the keyword **page** to view 24 lines of text at a time. Press the SPACE BAR to view the next 24 lines. Press the ENTER key to view the next line of text.

Command Modes EXEC privilege

Command History

Version 4.2.1.0	Introduced

Example

```
Force10#show tech-support page

---------------------------------- show version -------------------------------
Force10 Networks Real Time Operating System Software
Force10 Operating System Version: 1.0
Force10 Application Software Version: CS-1-1-317
Copyright (c) 1999-2007 by Force10 Networks, Inc.
Build Time: Tue Sep 12 15:39:17 IST 2006
Build Path: /sites/maa/work/sw/purushothaman/cser-latest/depot/main/Dev/Cyclone/
DevBranches/C-SERIES/SW/SRC
Force10 uptime is 18 minutes

System image file is "/work/sw/IMAGES/Chassis/C300-ODC-2/FTOS-CS.bin"

Chassis Type: C300
Control Processor: IBM PowerPC 750FX (Rev D2.2) with 1073741824 bytes of memory.
128K bytes of non-volatile configuration memory.

  1 Route Processor/Switch Fabric Module
  2 48-port GE 10/100/1000Base-T line card with RJ45 interface (CB)
  1 FastEthernet/IEEE 802.3 interface(s)
 96 GigabitEthernet/IEEE 802.3 interface(s)

 ---------------------------------- show HA information -------------------

--  RPM Status  --
-------------------------------------------------
 RPM Slot ID:               0
 RPM Redundancy Role:       Primary
 RPM State:                 Active
 RPM SW Version:            CS-1-1-317
 Link to Peer:              Down
 Peer RPM:                  not present

--  RPM Redundancy Configuration  --
-------------------------------------------------
 Primary RPM:               rpm0
 Auto Data Sync:            Full
 Failover Type:             Hot Failover
 Auto reboot RPM:           Disabled
 Auto failover limit:       3 times in 60 minutes

--  RPM Failover Record  --
-------------------------------------------------
 Failover Count:            0
 Last failover timestamp:   None
 Last failover Reason:      None

--  Last Data Block Sync Record:  --
-------------------------------------------------
  Line Card Config:         no block sync done
   Start-up Config:         no block sync done
 Runtime Event Log:         no block sync done
    Running Config:         no block sync done

 ---------------------------------- show running-config ------------------------
Current Configuration ...
! Version CS-1-1-317
!
boot system rpm0 primary ftp://ftp:ftp@10.16.2.1//work/sw/IMAGES/Chassis/
C300-ODC-2/FTOS-CS.bin
boot system rpm0 secondary flash://dummy
boot system rpm0 default flash://dummy
boot system gateway 10.16.2.1
!
service timestamps log datetime
!
hostname Force10
!
enable password 7 b125455cf679b208e79b910e85789edf
!
username admin password 7 1d28e9f33f99cf5c
!
--More--
```

Figure 51 partial output of the show tech-support Command Example

Usage Information Without the **page** option, the command output is continuous, use CNTL-z to interrupt the command output.

Related Commands

show running-config	View current configuration.

ssh-peer-rpm

Open a SSH connection to the peer RPM.

Syntax **ssh-peer-rpm** [**-l** *username*]

Parameters

-l *username*	(OPTIONAL) Enter the keyword **-l** followed by your user name. Default: The user name associated with the terminal

Defaults Not configured.

Command Modes EXEC

EXEC privilege

Command History

Version 6.3.1.0	Introduced

Usage Information This command is not available when the peer RPMs are running different FTOS releases.

telnet

Connect through Telnet to a server.

Syntax **telnet** {*host* | *ip-address* | *ipv6-address prefix-length*} [**/source-interface**]

Parameters

host	Enter the name of a server.
ip-address	Enter the IPv4 address in dotted decimal format of the server.

ipv6-address prefix-length	Enter the IPv6 address in the **x:x:x:x::x** format followed by the prefix length in the **/x** format. Range: /0 to /128 **Note:** The **::** notation specifies successive hexadecimal fields of zeros
source-interface	(OPTIONAL) Enter the keywords **/source-interface** followed by the interface information to include the interface's IP address. Enter the following keywords and slot/port or number information: • For an 100/1000 Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For Loopback interfaces, enter the keyword **loopback** followed by a number from zero (0) to 16383. • For the Null interface, enter the keyword **null** followed by 0. • For a Port Channel interface, enter the keyword **port-channel** followed by a number: C-Series Range: 1-128 E-Series Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale. • For SONET interface types, enter the keyword **sonet** followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information. • For VLAN interface, enter the keyword **vlan** followed by a number from 1 to 4094.

Defaults Not configured.

Command Modes EXEC

EXEC privilege

Command History

Version 7.5.1.0	Added support for IPv6 address

telnet-peer-rpm

Open a telnet connection to the peer RPM.

Syntax **telnet-peer-rpm**

Defaults Not configured.

Command Modes EXEC

EXEC privilege

Command History

Version 6.2.1.1	Introduced

Usage Information

Opening a telnet connection from the Standby RPM to an Active RPM follows the authentication procedure configured in the chassis. However, opening a telnet connection from the Active RPM into the Standby RPM requires local authentication.

Configuring an ACL on a VTY line will block a Telnet session using the **telnet-peer-rpm** command in the standby to active RPM direction only. Such an ACL will not block an internal Telnet session in the active RPM to standby RPM direction.

terminal length

Configure the number of lines displayed on the terminal screen.

Syntax **terminal length** *screen-length*

To return to the default values, enter **terminal no length**.

Parameters

screen-length	Enter a number of lines. Entering zero will cause the terminal to display without pausing. Range: 0 to 512. Default: 24 lines.

Defaults 24 lines

Command Modes EXEC

EXEC privilege

terminal xml

C-Series	No
E-Series	✓

Enable XML mode in Telnet and SSH client sessions.

Syntax **terminal xml**

To exit the XML mode, enter **terminal no xml**.

Defaults Disabled

Command Modes EXEC

EXEC privilege

Command History

Version 6.5.1.0	Introduced

Usage Information This command enables the XML input mode where you can either cut and paste XML requests or enter the XML requests line-by-line. For more information on using the XML feature, refer to the XML chapter in the *FTOS Configuration Guide*.

traceroute

View a packet's path to a specific device.

Syntax **traceroute** {*host* | *ip-address* | *ipv6-address*}

Parameters

host	Enter the name of device.
ip-address	Enter the IP address of the device in dotted decimal format.
ipv6-address	Enter the IPv6 address, in the **x:x:x:x::x** format, to which you are testing connectivity. **Note:** The **::** notation specifies successive hexadecimal fields of zeros

Defaults Timeout = 5 seconds; Probe count = 3; 30 hops max; 40 byte packet size; UDP port = 33434

Command Modes EXEC

EXEC privilege

Command History

Version 7.4.1.0	Added support for IPv6 address

Usage Information When you enter the **traceroute** command without specifying an IP address (Extended Traceroute), you are prompted for a target and source IP address, timeout in seconds (default is 5), a probe count (default is 3), minimum TTL (default is 1), maximum TTL (default is 30), and port number (default is 33434). To keep the default setting for those parameters, press the ENTER key.

For IPv6, you are prompted for a minimum hop count (default is 1) and a maximum hop count (default is 64).

Example

```
Force10#traceroute www.force10networks.com

Translating "www.force10networks.com"...domain server (10.11.0.1) [OK]
Type Ctrl-C to abort.

------------------------------------------------------------------------------------------
Tracing the route to www.force10networks.com (10.11.84.18), 30 hops max, 40 byte packets
------------------------------------------------------------------------------------------

 TTL Hostname            Probe1      Probe2      Probe3
  1  10.11.199.190        001.000 ms  001.000 ms  002.000 ms
  2  gwegress-sjc-02.force10networks.com (10.11.30.126) 005.000 ms  001.000 ms  001.000 ms
  3  fw-sjc-01.force10networks.com (10.11.127.254) 000.000 ms  000.000 ms  000.000 ms
  4  www.force10networks.com (10.11.84.18) 000.000 ms  000.000 ms  000.000 ms
Force10#
```

Figure 52 traceroute (IPv4) Command Example

Figure 53 contains examples of the IPv6 **traceroute** command with both a compressed IPv6 addresses and uncompressed address.

Example

```
Force10#traceroute 100::1

Type Ctrl-C to abort.

------------------------------------------------------------
Tracing the route to 100::1, 64 hops max, 60 byte packets
------------------------------------------------------------
Hops Hostname            Probe1      Probe2      Probe3
  1  100::1              000.000 ms  000.000 ms  000.000 ms

Force10#traceroute 3ffe:501:ffff:100:201:e8ff:fe00:4c8b

Type Ctrl-C to abort.

------------------------------------------------------------------------------------------
Tracing the route to 3ffe:501:ffff:100:201:e8ff:fe00:4c8b, 64 hops max, 60 byte packets
------------------------------------------------------------------------------------------
Hops Hostname            Probe1      Probe2      Probe3
  1  3ffe:501:ffff:100:201:e8ff:fe00:4c8b
                         000.000 ms  000.000 ms  000.000 ms
Force10#
```

Figure 53 Traceroute (IPv6) Command Example

Related Commands

ping	Test connectivity to a device.

undebug all

Disable all debug operations on the E-Series.

Syntax **undebug all**

Defaults No default behavior or values

Command Modes EXEC privilege

upgrade sfm

C-Series	No
E-Series	✓

Upgrade the FPGA version in the specified SFM and automatically initiate an auto reset to complete the version upgrade.

Syntax **upgrade sfm** [*slot-number* | **all**] [**autoreset**]

Parameters

slot-number	Enter the SFM slot number of the SFM with the FPGA to upgrade. Range: 0 to 7
all	(OPTIONAL) Enter the keyword **all** to upgrade the FPGA on all the SFMs.
autoreset	Enter the keyword **autoreset** to initiate the auto upgrade to the FPGA.

Defaults No default values or behavior

Command Modes EXEC

EXEC privilege

Command History

Version 7.5.1.0	Introduced

Example

```
Force10#upgrade sfm 1 autoreset
SFM1: upgrade in progress
!!! !!! !!!
SFM1: upgrade complete
SFM1 is active. Resetting it might temporarily impact traffic.
Proceed with reset [confirm yes/no]: yes
Force10#
```

Figure 54 upgrade sfm autoreset Command Example

Related Commands

show sfm all	Display the SFM status

upload nvtrace linecard

Upload the nvtrace-log file from the line card to flash.

Syntax **upload nvtrace linecard** *slot*

upload nvtrace-log linecard slot number

Parameters

slot	Enter the slot number of the line card. C-Series Range: 0-7 on the C300 E-Series Range: 0 to 13 on the E1200; 0 on 6 for E600, and 0 to 5 on the E300..

Defaults No default behavior or values

Command Modes EXEC

EXEC privilege

Usage Information The log information is uploaded to LP*linecard number*-Upload-nvtrace-log file at flash://NVTRACE_LOG_DIR/.

upload trace-log

Upload trace log files from the three CPUs (cp, rp1, and rp2)

Syntax **upload trace-log** {**cp** {**cmd-history** | **hw-trace** | **sw-trace**}| **rp1** {**cmd-history** | **hw-trace** | **sw-trace**}| **rp2** {**cmd-history** | **hw-trace** | **sw-trace**}}

Parameters

cp | **rp1** | **rp2**	Enter the keyword **cp** | **rp1** | **rp2** to upload the trace log from that CPU.
cmd-history	(OPTIONAL) Enter the keyword **cmd-history** to upload the CPU's command history.
hw-trace	(OPTIONAL) Enter the keyword **hw-trace** to upload the CPU's hardware trace.
sw-trace	(OPTIONAL) Enter the keyword **sw-trace** to upload the CPU's software trace.

Defaults No default behavior or values

Command Modes EXEC

EXEC privilege

Usage Information The log information is uploaded to flash:/TRACE_LOG_DIR

Command History

Version 7.5.1.0	Expanded to

virtual-ip

Configure a virtual IP for the active management interface.

Syntax **virtual-ip** *ip address*

To return to the default, use the **no virtual-ip** *ip address* command.

Parameters

ip address	Enter the IP address of the active management interface in a dotted decimal format (A.B.C.D.)

Defaults No default behavior or values

Command Modes CONFIGURATION

write

Copy the current configuration to either the startup-configuration file or the terminal.

Syntax **write** {**memory** | **terminal**}

Parameters

memory	Enter the keyword **memory** to copy the current running configuration to the startup configuration file. The write memory command is similar to the **copy running-config startup-config** command.
terminal	Enter the keyword **terminal** to copy the current running configuration to the terminal. The write terminal command is similar to the **show running-config** command.

Command Modes EXEC privilege

Upgrading the FPGA

C-Series	✓
E-Series	NO

Platform Specific Feature: This feature supported on the C-Series only.

These commands are for upgrading the FPGA for C-Series RPMs and line cards.

- reset on page 168
- restore fpga-flash on page 169
- upgrade primary-fpga-flash on page 170

reset

C-Series	✓
E-Series	No

Reset a line card.

Syntax **reset** {**linecard** *number* [**hard** | **power-cycle**]}

Parameters

linecard *number*	Enter the keyword **linecard** and a number for the line card slot number. Range: 0 to 7 on the C300.
hard	Enter the keyword **hard** to power cycle the line card.
power-cycle	Enter the keyword **power-cycle** after upgrading the FPGA to cause the FPGA to be reprogrammed based on the contents of the FPGA PROM.

Defaults Disabled.

Command Modes EXEC privilege

Usage Information When a soft reset is issued on a line card (**reset linecard** *number*), FTOS boots the line card from its runtime image. Only when you enter **reset linecard** *number* **hard** is the software image reloaded on the line card.

The **reset linecard** *number* **power-cycle** command is required after upgrading FPGA PROM. The FPGA is responsible for central board control. It will cause the FPGA to be reprogrammed based on the contents of the FPGA PROM.

See Upgrading the FPGA on page 168 for more information.

Related Commands		
	upgrade primary-fpga-flash	Upgrade the PRIMARY-FPGA-FLASH with the FPGA image in the currently loaded FTOS image.

restore fpga-flash

C-Series	✔
E-Series	**No**

This command copies the BACKUP-FPGA-FLASH to PRIMARY-FPGA-FLASH.

Syntax **restore fpga-flash** {**rpm** | **linecard** *number*}

Parameters

rpm	Enter **rpm** to upgrade an RPM FPGA flash.
linecard	Enter **linecard** to upgrade a line card FPGA flash.
number	Enter the line card number. C-Series Range: 0-7 on the C300

Defaults None.

Command Mode CONFIGURATION

Example

```
Force10# restore fpga-flash rpm
Proceed to restore primary fpga flash for rpm 0 [confirm yes/no]: yes
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Force10#
```

Figure 55 restore fpga-flash Command Example

Usage Information The user can restore a single rpm, or a single linecard at a time. Each card must be rebooted, after restoration. Verify that the restoration procedure occurred correctly. This command can be executed whether the FPGA was loaded from 'PRIMARY' or 'BACKUP' FPGA-FLASH.

Related Commands		
	reset	Reset a line card.
	show rpm	View the current RPM status.
	show linecard	View the line card(s) status.

upgrade primary-fpga-flash

C-Series	✓
E-Series	No

Upgrade the PRIMARY-FPGA-FLASH with the FPGA image in the currently loaded FTOS image.

Syntax

upgrade primary-fpga-flash {**rpm** | **linecard** *number*}

Parameters

rpm	Enter **rpm** to upgrade an RPM FPGA flash.
linecard	Enter **linecard** to upgrade a line card FPGA flash.
number	Enter the line card number. C-Series Range: 0-7 on the C300

Defaults

None.

Command Mode

CONFIGURATION

Example

```
Force10#conf
Force10(conf)# upgrade primary-fpga-flash rpm
Proceed to upgrade primary fpga flash for rpm 0 [confirm yes/no]: yes
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Force10#
```

Figure 56 upgrade primary-fpga-flash Command Example

Usage Information

The user can upgrade a single rpm, or a single linecard at a time. This command can be executed whether the FPGA was loaded from 'PRIMARY' or 'BACKUP' FPGA-FLASH.

Note: After an upgrade, power-cycle the RPM or line card using the **reset rpm** *number* **power-cycle** or **reset linecard** *number* **power-cycle** commands, respectively. Verify that the upgrade procedure occurred correctly, using the **show linecard** command.

Related Commands

reset	power-cycle an RPM or line card.
restore fpga-flash	This command copies the BACKUP-FPGA-FLASH to PRIMARY-FPGA-FLASH.
show linecard	View the line card(s) status.
show rpm	View the current RPM status.

Chapter 4 IPv6 Basic Commands

Platform Specific Feature: IPv6 is supported on E-Series only.

The Force10 Networks implementation of IPv6 is based on the following IETF (Internet Engineering Task Force) RFCs:

RFC 2460	IPv6 Specification
RFC 2461	IPv6 Neighbor Discovery for IP Version 6 (IPv6)
RFC 2463	ICMPv6
RFC 3513	IPv6 Addressing Architecture
RFC 3587	IPv6 Global Unicast Address Format
RFC 2464	Transmission of IPv6 Packets over Ethernet Networks

The IPv6 commands are:

- clear ipv6 route on page 172
- ipv6 address on page 172
- ipv6 route on page 173
- ipv6 unicast-routing on page 175
- show ipv6 cam linecard on page 175
- show ipv6 fib linecard on page 178
- show ipv6 interface on page 178
- show ipv6 route on page 179
- trust ipv6-diffserv on page 182

clear ipv6 route

C-Series	No
E-Series	✓

Clear (refresh) all or a specific route from the IPv6 routing table.

Syntax **clear ipv6 route** {* | *ipv6-address prefix-length* }

Parameters

*	Enter the * to clear (refresh) all routes from the IPv6 routing table.
ipv6-address prefix-length	Enter the IPv6 address in the **x:x:x:x::x** format followed by the prefix length in the **/x** format. Range: /0 to /128 **Note:** The **::** notation specifies successive hexadecimal fields of zeros

Command Mode EXEC

EXEC privilege

Command History

Version 7.4.1.0	Introduced

ipv6 address

C-Series	No
E-Series	✓

Configure an IPv6 address to an interface.

Syntax **ipv6 address** {*ipv6-address prefix-length*}

To remove the IPv6 address, use the **no ipv6 address** {*ipv6-address prefix-length*} command.

Parameters

ipv6-address prefix-length	Enter the IPv6 address in the **x:x:x:x::x** format followed by the prefix length in the **/x** format. Range: /0 to /128 **Note:** The **::** notation specifies successive hexadecimal fields of zeros

Defaults No default values or behavior

Command Modes INTERFACE

Command History

Version 7.4.1.0	Introduced

Example

```
Force10(conf)#interface gigabitethernet 10/0
Force10(conf-if-gi-10/0)#ipv6 address ?
X:X:X:X::X              IPv6 address
Force10(conf-if-gi-10/0)#ipv6 address 2002:1:2::3 ?
<0-128>                 Prefix length in bits
Force10(conf-if-gi-10/0)#ipv6 address 2002:1:2::3 /96 ?
<cr>
Force10(conf-if-gi-10/0)#ipv6 address 2002:1:2::3 /96
Force10(conf-if-gi-10/0)#show config
!
interface GigabitEthernet 10/0
 no ip address
 ipv6 address 2002:1:2::3 /96
 no shutdown
Force10(conf-if-gi-10/0)#
```

Usage Information

FTOS allows multiple IPv6 addresses to be configured on an interface. When the **no ipv6 address** command is issued without specifying a particular IPv6 address, all IPv6 addresses on that interface are deleted.

ipv6 route

C-Series	**No**
E-Series	✓

Establish a static IPv6 route.

Syntax

ipv6 route *ipv6-address prefix-length* {*ipv6-address* | *interface* | *interface ipv6-address*} [*distance*] [**tag** *value*] [**permanent**]

To remove the IPv6 route, use the **no ipv6 route** *ipv6-address prefix-length* {*ipv6-address* | *interface* | *interface ipv6-address*} [*distance*] [**tag** *value*] [**permanent**] command.

Parameters

ipv6-address prefix-length	Enter the IPv6 address in the **x:x:x:x::x** format followed by the prefix length in the **/x** format. Range: /0 to /128 **Note:** The **::** notation specifies successive hexadecimal fields of zeros
interface	(OPTIONAL) Enter the following keywords and slot/port or number information: • For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For a loopback interface, enter the keyword **loopback** followed by a number from zero (0) to 16383. • For the null interface, enter the keyword **null** followed by zero (0). • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information.

ipv6-address	(OPTIONAL) Enter the forwarding router IPv6 address in the **x:x:x:x::x** format. **Note:** The **::** notation specifies successive hexadecimal fields of zeros
distance	(OPTIONAL) Enter a number as the distance metric assigned to the route. Range: 1 to 255
tag *value*	(OPTIONAL) Enter the keyword **tag** followed by a tag value number. Range: 1 to 4294967295
permanent	(OPTIONAL) Enter the keyword **permanent** to specify that the route is not to be removed, even if the interface assigned to that route goes down. **Note:** If you disable the interface with an IPv6 address associated with the keyword **permanent**, the route disappears from the routing table.

Defaults

No default values or behavior

Command Modes

CONFIGURATION

Command History

Version 7.4.1.0	Introduced

Example

```
Force10(conf)#ipv6 route 44::0 /64 33::1 ?
<1-255>                         Distance metric for this route
permanent                       Permanent route
tag                             Set tag for this route

Force10(conf)#ipv6 route 55::0 /64 ?
X:X:X:X::X                      Forwarding router's address
gigabitethernet                 Gigabit Ethernet interface
loopback                        Loopback interface
null                            Null interface
port-channel                    Port channel interface
sonet                           Sonet interface
tenGigabitethernet              TenGigabit Ethernet interface
vlan                            VLAN interface

Force10(conf)#ipv6 route 55::0 /64 gigabitethernet 9/0 ?
<1-255>                         Distance metric for this route
X:X:X:X::X                      Forwarding router's address
permanent                       Permanent route
tag                             Set tag for this route

Force10(conf)#ipv6 route 55::0 /64 gigabitethernet 9/0 66::1 ?
<1-255>                         Distance metric for this route
permanent                       Permanent route
tag                             Set tag for this route
Force10#
```

Figure 57 ipv6 route command

Usage Information

When the interface goes down, FTOS withdraws the route. The route is re-installed, by FTOS, when the interface comes back up. When a recursive resolution is “broken,” FTOS withdraws the route. The route is re-installed, by FTOS, when the recursive resolution is satisfied.

Related Commands

show ipv6 route	View the IPv6 configured routes.

ipv6 unicast-routing

C-Series	No
E-Series	✓

Enable IPv6 Unicast routing.

Syntax **ipv6 unicast-routing**

To disable unicast routing, use the **no ipv6 unicast-routing** command.

Defaults Enabled

Command Modes EXEC

Command History

Version 7.4.1.0	Introduced

Usage Information Since this command is enabled by default, it does not appear in the running configuration. When unicast routing is disabled, the **no ipv6 unicast-routing** command is included in the running configuration. Whenever unicast routing is disabled or re-enabled, FTOS generates a syslog message indicating the action.

Disabling unicast routing on an E-Series chassis causes the following behavior:

- static and protocol learnt routes are removed from RTM and from the CAM; packet forwarding to these routes is terminated.
- connected routes and resolved neighbors remain in the CAM and new IPv6 neighbors are still discoverable
- additional protocol adjacencies (OSPFv3 and BGP4) are brought down and no new adjacencies are formed
- the IPv6 address family configuration (under **router bgp**) is deleted
- IPv6 Multicast traffic continues to flow unhindered

Related Commands

router bgp	Enable BGP

show ipv6 cam linecard

C-Series	No
E-Series	✓

Displays the IPv6 CAM entries for the specified line card.

Syntax **show ipv6 cam linecard** *slot-number* [**fib**] [**summary**] [*ipv6-address prefix-length*]

Parameters

slot-number	Enter the line card slot ID number. Range: 0 to 13 on the E1200; 0 on 6 for E600, and 0 to 5 on the E300.
fib	(OPTIONAL) Enter the keyword **fib** to display Forwarding Information Base entries in the line card.
summary	(OPTIONAL) Enter the keyword **summary** to display a table listing network prefixes and the total number prefixes which can be entered into the IPv6 CAM.
ipv6-address prefix-length	Enter the IPv6 address in the **x:x:x:x::x/n** format to display networks that have more specific prefixes. Range: /0 to /128 **Note:** The **::** notation specifies successive hexadecimal fields of zeros.

Defaults No default values or behavior

Command Modes EXEC

EXEC privilege

Command History

Version 7.4.1.0	Introduced

Usage Information The forwarding table displays host route first, then displays route originated by routing protocol including static route.

The egress port section displays the egress port of the forwarding entry which is designated as:

C for the Control Processor

1 for the Route Processor 1

2 for the Route Processor 2

Example

```
Force10#show ipv6 cam linecard 13 fib

Neighbor                                    Mac-Addr          Port      VId
------------------------------------------- ----------------- --------- ----

[   31] 2002:44:1:1::11                     00:00:01:1a:1e:d5 Gi 13/2      0

Prefix                          Next-Hop                        Mac-Addr          Port      VId  EC
------------------------------- ------------------------------- ----------------- --------- ---- --

[ 3147] 100::/64                [    0] 2002:44:1:1::11               -          Gi 0/0       0 1
                                [    0] 2002:44:1:24::11              -          Gi 0/0       0 1
                                [    0] 2002:44:1:23::11              -          Gi 0/0       0 1
                                [    0] 2002:44:1:21::11              -          Gi 0/0       0 1
                                [    0] 2002:44:1:20::11              -          Gi 0/0       0 1
                                [    0] 2002:44:1:19::11              -          Gi 0/0       0 1
Force10#
```

Figure 58 show ipv6 cam linecard fib Command

Example

```
Force10#show ipv6 cam linecard 1 p 0
Neighbor                                          Mac-Addr          Port      VId
--------------------------------------------------- ----------------- --------- ----
[    0] fe80::201:e8ff:fe17:5cae                  00:01:e8:17:5c:ae BLK        100
[    1] fe80::201:e8ff:fe17:5bbe                  00:01:e8:17:5b:be BLK          0
[    2] fe80::201:e8ff:fe17:5bbd                  00:01:e8:17:5b:bd BLK          0
[    3] fe80::201:e8ff:fe17:5cb0                  00:01:e8:17:5c:b0 BLK          0
[    4] fe80::201:e8ff:fe17:5cae                  00:01:e8:17:5c:ae BLK       1000
[    5] fe80::201:e8ff:fe17:5caf                  00:01:e8:17:5c:af BLK          0

Prefix                              First-Hop                Mac-Addr          Port      VId  EC
------------------------------------ ------------------------  ----------------- --------- ----
--

[   80] 2222::2/128                 [    2] :                00:00:00:00:00:00 RP2          0  0

[   81] 3333::2/128                 [    2] ::1              00:00:00:00:00:00 RP2          0  0
Force10#
```

Figure 59 show ipv6 cam linecard Command

show ipv6 fib linecard

View all Forwarding Information Base entries.

Syntax **show ipv6 fib linecard** *slot-number* [**summary**] *ipv6-address mask*

Parameters

slot-number	Enter the number of the line card slot. E-Series Range: 0 to 13 on a E1200, 0 to 6 on a E600/E600i, and 0 to 5 on a E300
summary	(OPTIONAL) Enter the keyword **summary** to view a summary of entries in IPv6 cam.
ipv6-address mask	Enter the IPv6 address in the **x:x:x:x::x/n** format to display networks that have more specific prefixes. Range: /0 to /128 **Note:** The **::** notation specifies successive hexadecimal fields of zeros.

Command Mode EXEC

EXEC privilege

Command History

Version 7.4.1.0	Introduced

show ipv6 interface

C-Series	**No**
E-Series	✓

Display the status of interfaces configured for IPv6.

Syntax **show ipv6 interface** *interface* [**brief**] [**linecard** *slot-number*] [**configuration**]

Parameters

interface	(OPTIONAL) Enter the following keywords and slot/port or number information: • For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For a Loopback interface, enter the keyword **Loopback** followed by a number from 0 to 16383. • For the Null interface, enter the keyword **null** followed by zero (0). • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information.
brief	(OPTIONAL) Enter the keyword **brief** to view a summary of the interfaces.

linecard *slot-number*	(OPTIONAL) Enter the keyword **linecard** followed by the number of the line card slot. Range: 0 to 13 on a E1200, 0 to 6 on a E600, and 0 to 5 on a E300.
configuration	(OPTIONAL) Enter the keyword **configuration** to display the interfaces with non-default configurations only.

Defaults No default values or behavior

Command Modes EXEC
EXEC privilege

Command History

Version 7.4.1.0	Introduced

Example

```
Force10#show ipv6 interface gigabitethernet 1/1
GigabitEthernet 1/1 is up, line protocol is up
  IPV6 is enabled
  Link Local address: fe80::201:e8ff:fe04:62c4
  Global Unicast address(es):
    2001::1, subnet is 2001::/64
    2002::1, subnet is 2002::/120
    2003::1, subnet is 2003::/120
    2004::1, subnet is 2004::/32
  Global Anycast address(es):
  Joined Group address(es):
    ff02::1
    ff02::2
    ff02::1:ff00:1
    ff02::1:ff04:62c4
    MTU is 1500
  ICMP redirects are not sent
  DAD is enabled: number of DAD attempts: 1
  ND reachable time is 30 seconds
  ND advertised reachable time is 30 seconds
  ND advertised retransmit interval is 30 seconds
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
```

Figure 60 show ipv6 interface Command

show ipv6 route

C-Series	No
E-Series	✓

Displays the IPv6 routes.

Syntax **show ipv6 route** [*ipv6-address prefix-length*] [**longer-prefixes**] [**connected**] [**static**] [**summary**]

Parameter

ipv6-address prefix-length	(OPTIONAL) Enter the IPv6 address in the **x:x:x:x::x** format followed by the prefix length in the **/x** format. Range: /0 to /128 The **::** notation specifies successive hexadecimal fields of zeros.
longer-prefixes	(OPTIONAL) Enter the keyword **longer-prefixes** to view all routes with a common prefix.
connected	(OPTIONAL) Enter the keyword **connected** to view only the directly connected routes.
static	(OPTIONAL) Enter the keyword **static** to view only routes configured by the ipv6 route command.
summary	(OPTIONAL) Enter the keyword **summary** to view a brief list of the configured IPv6 routes.

Defaults

No default values or behavior

Command Modes

EXEC

EXEC privilege

Command History

Version 7.4.1.0	Introduced

Example 1

```
Force10#show ipv6 route

Codes: C - connected, L - local, S - static, R - RIP,
       B - BGP, IN - internal BGP, EX - external BGP,LO - Locally Originated,
       O - OSPF, IA - OSPF inter area, N1 - OSPF NSSA external type 1,
       N2 - OSPF NSSA external type 2, E1 - OSPF external type 1,
       E2 - OSPF external type 2, i - IS-IS, L1 - IS-IS level-1,
       L2 - IS-IS level-2, IA - IS-IS inter area, * - candidate default,
Gateway of last resort is not set

       Destination  Dist/Metric,      Gateway,   Last Change
       ------------------------------------------------------
  C    2001::/64 [0/0]
        Direct, Gi 1/1, 00:28:49
  C    2002::/120 [0/0]
        Direct, Gi 1/1, 00:28:49
  C    2003::/120 [0/0]
        Direct, Gi 1/1, 00:28:49
  C    2004::/32 [0/0]
        Direct, Gi 1/1, 00:28:49
  L    fe80::/10 [0/0]
        Direct, Nu 0, 00:29:09
```

Figure 61 show ipv6 route Command Example

Example 2

```
Force10#show ipv6 route summary

Route Source              Active Routes   Non-active Routes
connected                 5               0
static                    0               0
Total                     5               0
Total 5 active route(s) using 952 bytes
```

Figure 62 show ipv6 route summary Command Example

Table 13 details the information displayed in Figure 61 and Figure 62.

Table 13 show ipv6 route Command Example Fields

Field	Description
(undefined)	Identifies the type of route: • L = Local • C = connected • S = static • R = RIP • B = BGP • IN = internal BGP • EX = external BGP • LO = Locally Originated • O = OSPF • IA = OSPF inter area • N1 = OSPF NSSA external type 1 • N2 = OSPF NSSA external type 2 • E1 = OSPF external type 1 • E2 = OSPF external type 2 • i = IS-IS • L1 = IS-IS level-1 • L2 = IS-IS level-2 • IA = IS-IS inter-area • * = candidate default • > = non-active route • + = summary routes
Destination	Identifies the route's destination IPv6 address.
Gateway	Identifies whether the route is directly connected and on which interface the route is configured.
Dist/Metric	Identifies if the route has a specified distance or metric.
Last Change	Identifies when the route was last changed or configured.

Defaults

This command has no default behavior or value.

Command Modes

EXEC

EXEC privilege

Command History

Version 7.4.1.0	Introduced

trust ipv6-diffserv

C-Series	No
E-Series	✓

Allows the dynamic classification of IPv6 DSCP.

Syntax

trust ipv6-diffserv

To remove the definition, use the **no trust ipv6-diffserv** command.

Defaults

This command has no default behavior or values.

Command Modes

CONFIGURATION (conf-policy-map-in)

Command History

Version 7.4.1.0	Introduced

Usage Information

When trust IPv6 diffserv is configured, matched bytes/packets counters are *not* incremented in the show qos statistics command.

Trust differv (IPv4) can co-exist with **trust ipv6-diffserv** in an Input Policy Map. Dynamic classification happens based on the mapping detailed in Table 14.

Table 14 IPv6 -Diffserv Mapping

IPv6 Service Class Field	Queue ID
111XXXXX	7
110XXXXX	6
101XXXXX	5
100XXXXX	4
011XXXXX	3
010XXXXX	2
001XXXXX	1
000XXXXX	0

Chapter 5 C-Series Diagnostics and Debugging

C-Series	✓
E-Series	NO

Platform Specific Feature: This chapter is specific to the C-Series only.

This chapter contains the following sections:

- Inter-process Communication Commands on page 183
- RPM Management Port Commands on page 189
- Data Path Debugging on page 191
- Interface Troubleshooting on page 195
- Advanced ASIC Debugging Information on page 198
- ACL & System-Flow Debug Commands on page 200
- Interface Management Debug Commands on page 203
- Layer 2 Debug Commands on page 205
- Trace Logging Commands on page 206
- Offline Diagnostics on page 213

Inter-process Communication Commands

The following are Inter-Process Communication (IPC) commands. IPC commands display receive and transmit frame counters for the party-bus switch and CPU interfaces. These interfaces are the interfaces over which FTOS task-to-task control messages are exchanged.

- clear hardware cpu party-bus on page 184
- clear hardware rpm mac counters on page 184
- clear hardware mac port-statistics on page 185
- show hardware cpu party-bus on page 185
- show hardware rpm mac on page 187

clear hardware cpu party-bus

Clear the receive, transmit, and error counters for the party-bus port on the CPU of the specified linecard or RPM.

Syntax **clear hardware** {**linecard** | **rpm**} *number* **cpu party-bus statistics**

Parameters

linecard	Enter the keyword **linecard** to clear counters on a line card.
rpm	Enter the keyword **rpm** to clear counters on an RPM.
number	Enter a number after the following keywords: • After the keyword **rpm**: Range: 0-1 • After the keyword **linecard**: Range: 0-7 for the C300

Defaults None.

Command Mode EXEC

EXEC privilege

Command History

Version 7.5.1.0	Introduction

Usage Information

Note: Use this command only when you are working directly with a technical support representative to troubleshoot a problem. Do not use this command unless a technical support representative instructs you to do so.

clear hardware rpm mac counters

Clear receive & transmit Ethernet statistics for all ports on the party-bus switch of the specified RPM.

Syntax **clear hardware rpm** *number* **mac counters**

Parameters

number	Enter the RPM slot number. Range: 0-1

Defaults None.

Command Mode EXEC

EXEC privilege

Command History

Version 7.5.1.0	Introduction

Usage Information

Note: Use this command only when you are working directly with a technical support representative to troubleshoot a problem. Do not use this command unless a technical support representative instructs you to do so.

clear hardware mac port-statistics

Clear Ethernet statistics of party-bus switch port connected specified line card or RPM.

Syntax **clear hardware** {**linecard** | **rpm**} *number* **mac port-statistics** {**linecard** | **rpm**} *number*

Parameters

linecard	Enter the keyword **linecard** to clear Ethernet statistics for all ports on the party-bus switch a line card.
rpm	Enter the keyword **rpm** to clear Ethernet statistics for all ports on the party-bus switch of an RPM.
number	Enter a number after the following keywords: • After the keyword **rpm**: Range: 0-1 • After the keyword **linecard**: Range: 0-7 for the C300

Defaults None.

Command Mode EXEC

EXEC privilege

Command History

Version 7.5.1.0	Introduction

show hardware cpu party-bus

View advanced debugging counters for the party-bus port on the CPU of the specified line card or RPM.

Syntax **show hardware** {**linecard** | **rpm**} *number* **cpu party-bus statistics**

Parameters

linecard	Enter the keyword **linecard** to view debugging counters for a line card.
rpm	Enter the keyword **rpm** to view cpu debugging counters for an RPM.
number	Enter a number after the following keywords: • After the keyword **rpm**: Range: 0-1 • After the keyword **linecard**: Range: 0-7 for the C300

Defaults

None.

Command Mode

EXEC

EXEC privilege

Command History

Version 7.5.1.0	Introduction

Example

Figure 63 shows the output of this command.

```
Force10#show hardware linecard 1 cpu party-bus statistic
ACTIVE EMAC DEVICE:2 STATISTICS
 Num of Pkts. Tx Requested = 2788452, Number of Pkts Transmitted  = 2788452
 Num of Pkts. Received     = 139662, Number of Pkts Given to MUX = 139662
 Transmit Errors due to no Data              = 0
 Transmit Errors due to exceed num of Desc   = 0
 Transmit Block Count (Stall Count)          = 0
 Recv Pkts Dropped due to Bad Pkts Rx        = 0
 Recv Pkts Dropped due to more than one Buf = 0
 Recv Pkts Dropped due to out of Mem         = 0
 Recv Pkts Dropped due to out of CBlk        = 0
 Recv Pkts Dropped due to out of MBlk        = 0
ALTERNATIVE EMAC DEVICE:3 STATISTICS
 Num of Pkts. Tx Requested = 0, Number of Pkts Transmitted  = 0
 Num of Pkts. Received     = 0, Number of Pkts Given to MUX = 0
 Transmit Errors due to no Data              = 0
 Transmit Errors due to exceed num of Desc   = 0
 Transmit Block Count (Stall Count)          = 0
 Recv Pkts Dropped due to Bad Pkts Rx        = 0
 Recv Pkts Dropped due to more than one Buf = 0
 Recv Pkts Dropped due to out of Mem         = 0
 Recv Pkts Dropped due to out of CBlk        = 0
 Recv Pkts Dropped due to out of MBlk        = 0
 value = 0 = 0x0
```

Figure 63 show hardware linecard Command Example

Usage Information

Note: Use this command only when you are working directly with a technical support representative to troubleshoot a problem. Do not use this command unless a technical support representative instructs you to do so.

Related Commands

clear hardware cpu party-bus	Clear the receive, transmit, and error counters and for the party-bus port on the CPU of the specified RPM.

show hardware rpm mac

View receive and transmit counters for the party-bus switch in the IPC subsystem.

Syntax **show hardware rpm** *number* **mac** {**counters** | **port-statistics** [**linecard** *number* | **rpm** *number*]}

Parameters

counters	Enter the keyword **counters** to view high-level receive and transmit counters.
port-statistics	Enter the keyword **port-statistics** to view detailed Ethernet statistics for the specified port on the party-bus switch.
linecard	(OPTIONAL) Enter the keyword **linecard** to view information about a particular line card.
rpm	(OPTIONAL) Enter the keyword **rpm** to view information about a particular RPM.
number	Enter a number after the following keywords: • After the keyword **rpm**: Range: 0-1 • After the keyword **linecard**: Range: 0-7 for the C300

Defaults None.

Command Mode EXEC

EXEC privilege

Command History

Version 7.5.1.0	Introduction

Example Figure 64 shows the output of this command using the **counters** option. Table 15 describes the fields shown in the figure.

```
Force10#show hardware rpm 0 mac counters
Received and Transmitted Packets without Errors
SLOT ID#        Rx Counter      TxCounter
RSM SLOTS:
0                1                      17
1                0                      0
LCM SLOTS:
0                0                      0
1                17                     1
2                0                      0
3                0                      0
4                0                      0
5                0                      0
6                0                      0
```

Figure 64 show hardware rpm mac counters Command Example

Table 15 show hardware rpm mac counters Output Description

Slot ID #	Port number on the party-bus control switch.
RX Frames	Number of packets received by the party-bus switch from the processor in the specified slot. **Note:** Verify the counters are incrementing.
TX Frames	Number of packets sent by the party-bus switch to the processor in the specified slot. **Note:** Verify the counters are incrementing.

Figure 65 shows the ouput of this command using the **port-statistics** option.

```
Force10#show hardware rpm 0 mac port-statistics linecard 1
IPC Switch Port Number :7
snmpIfInOctets                                  : 2471340
snmpIfInUcastPkts                               : 2410
snmpIfOutOctets                                 : 16046
snmpIfOutUcastPkts                              : 99
snmpDot1dTpPortInFrames                         : 2410
snmpDot1dTpPortOutFrames                        : 99
snmpEtherStatsPkts128to255Octets                : 491
snmpEtherStatsPkts512to1023Octets               : 640
snmpEtherStatsPkts1024to1518Octets              : 1378
snmpEtherStatsOctets                            : 2487386
snmpEtherStatsPkts                              : 2509
snmpEtherStatsTXNoErrors                        : 99
snmpEtherStatsRXNoErrors                        : 2410
snmpIfHCInOctets                                : 2471340
snmpIfHCInUcastPkts                             : 2410
snmpIfHCOutOctets                               : 16046
snmpIfHCOutUcastPkts                            : 99
```

Figure 65 show hardware rpm mac port-statistics Command Example

Usage Information

Note: Use this command only when you are working directly with a technical support representative to troubleshoot a problem. Do not use this command unless a technical support representative instructs you to do so.

Related Commands

clear hardware rpm mac counters	Clear the receive, transmit, and error counters and for the party-bus port on the CPU of the specified RPM.

RPM Management Port Commands

- show hardware rpm cpu management on page 189

show hardware rpm cpu management

View standard Ethernet receive and transmit counters as well as auto-negotiation debugging information for the external management interface.

Syntax **show hardware rpm** *number* **cpu management statistics**

Parameters

number	Enter the RPM slot number. Range: 0-1

Defaults None.

Command Mode EXEC

EXEC privilege

Command History

Version 7.5.1.0	Introduction

Example Figure 66 shows the output of this command.

```
Force10#show hardware rpm 0 cpu management statistics

         Port #0 MIB Counters

GoodFramesReceived          = 4214683
BadFramesReceived           = 2
BroadcastFramesReceived     = 275828
MulticastFramesReceived     = 3787188
GoodOctetsReceived          = 0x0000303000000000

GoodFramesSent              = 9539
BroadcastFramesSent         = 0
MulticastFramesSent         = 0
GoodOctetsSent              = 128

         FC Control Counters
UnrecogMacControlReceived   = 0
GoodFCFramesReceived        = 0
BadFCFramesReceived         = 0
FCFramesSent                = 0

         RX Errors
BadOctetsReceived           = 260
UndersizeFramesReceived     = 0
FragmentsReceived           = 0
OversizeFramesReceived      = 0
JabbersReceived             = 0
MacReceiveErrors            = 0
BadCrcReceived              = 0
Rx Discarded packets counter= 0
Rx Overrun packets counter  = 0

         TX Errors
TxMacErrors                 = 0
TxExcessiveCollisions       = 0
TxCollisions                = 2
TxLateCollisions            = 0


10 BASE-T half-duplex

Auto-negotiation is complete

The PHY Port power is normal
         ethGiga #0 port Status: 0x2444 = 0x00000402

Link=UP, Speed=10, Duplex=HALF, RxFlowControl=DISABLE, padLen=136
RxCoal = 0 usec, TxCoal = 0 usec
MacAddr (0x3bc75e54) = 00:01:e8:2e:2f:20

RX Queue #0: base=0x42000000, free=1024

TX Queue #0: base=0x42008020, free=2048
MANAGEMENT PHY REGISTER VALUES
         0x00: 0x1000    0x01: 0x796D    0x02: 0x0143    0x03: 0xBCB1
         0x04: 0x0021    0x05: 0x41E1    0x06: 0x0065    0x07: 0x2001
         0x08: 0x0000    0x09: 0x0000    0x0A: 0x0000    0x0B: 0x0000
         0x0C: 0x0000    0x0D: 0x0000    0x0E: 0x0000    0x0F: 0x3000
         0x10: 0x0000    0x11: 0x0100    0x12: 0x0000    0x13: 0x0000
         0x14: 0x0000    0x15: 0x0101    0x16: 0x0000    0x17: 0x0F04
         0x18: 0x0400    0x19: 0x8114    0x1A: 0x0000    0x1B: 0xFFFF
         0x1C: 0x38A3    0x1D: 0x06CD    0x1E: 0x0000    0x1F: 0x0000

MII Control Register
SpeedSelection: 10Mbps
--More--
```

Figure 66 show hardware rpm Command Example

Usage Information

Note: Use this command only when you are working directly with a technical support representative to troubleshoot a problem. Do not use this command unless a technical support representative instructs you to do so.

Data Path Debugging

Data path refers to external data and control packets that are sent to an RPM or line card, or processed by FP and forwarded through the system.

- show hardware drops
- show hardware cpu data-plane on page 193

show hardware drops

View internal packet-drop counters on a line card or RPM.

Syntax **show hardware** {**linecard** *number* | **rpm** *number*} **drops** [**unit** *number*] [**port** *number*]

Parameters

linecard	Enter the keyword linecard to view information about a line card.
rpm	Enter the keyword rpm to view information about an RPM.
unit	(OPTIONAL) Enter the keyword unit to view information about a unit.
port	(OPTIONAL) Enter the keyword port to view information about a port.
number	Enter a number after the following keywords: • After the keyword **linecard**: Range: 0-7 for the C300 • After the keyword **rpm**: Range: 0-1 • After the keyword **unit**, enter the number of CSF or FP ASIC. • After the keyword **port**, enter the port number.

Defaults None.

Command Mode EXEC

EXEC privilege

Command History

Version 7.5.1.0	Introduction

Example Figure 67 shows the command to display the dropped packets per chassis slot.

```
Force10#show hardware rpm 0 drops

UNIT No: 0

Total Ingress Drops           :0
Total IngMac Drops            :0
Total Mmu Drops               :0
Total EgMac Drops             :0
Total Egress Drops            :0

UNIT No: 1

Total Ingress Drops           :0
Total IngMac Drops            :0
Total Mmu Drops               :0
Total EgMac Drops             :0
Total Egress Drops            :0

UNIT No: 2

Total Ingress Drops           :0
Total IngMac Drops            :0
Total Mmu Drops               :0
Total EgMac Drops             :0
Total Egress Drops            :0

UNIT No: 3

Total Ingress Drops           :0
Total IngMac Drops            :0
Total Mmu Drops               :0
Total EgMac Drops             :0
Total Egress Drops            :0
```

Figure 67 show hardware drops Command Example

Figure 68 shows the command to display dropped packers per unit, in other words, dropped packets for a particular FP or CSF ASIC.

```
Force10#show hardware rpm 0 drops unit 0

Port#       :Ingress Drops  :IngMac Drops   :Total Mmu Drops :EgMac Drops   :Egress
Drops
 1              0              0              0              0              0
 2              0              0              0              0              0
 3              0              0              0              0              0
 4              0              0              0              0              0
 5              0              0              0              0              0
 6              0              0              0              0              0
 7              0              0              0              0              0
 8              0              0              0              0              0
```

Figure 68 show hardware drops unit Command Example

Figure 69 shows the command to display dropped packets for a particular port on a unit.

```
Force10#show hardware rpm 0 drops unit 0 port 1
 --- Ingress Drops       ---
Unknown HiGig HDR             :0
Unknown HiGig OPCODE          :0
Unknown HiGig HDR Format      :0
RX EgressBlockMask            :0
Rx LinkBlockCntr              :0
Rx SrcModBlockCntr            :0
IBP CBP FullDrops             :0
Rx AgedCounter                :0
 --- Ingress MAC Drops   ---
IngressMacDrops               :0
 --- MMU Drops           ---
HOL DROPS on COS0             :0
HOL DROPS on COS1             :0
HOL DROPS on COS2             :0
HOL DROPS on COS3             :0
HOL DROPS on COS4             :0
HOL DROPS on COS5             :0
HOL DROPS on COS6             :0
HOL DROPS on COS7             :0
 --- Egress MAC counters ---
egressMACDrops                :0
 --- Egress Drops        ---
Tx AgedCounter                :0
Tx ErrCounter                 :0
Tx MacUnderFlow               :0
```

Figure 69 show hardware drops unit port Command Example

Usage Information

Note: Use this command only when you are working directly with a technical support representative to troubleshoot a problem. Do not use this command unless a technical support representative instructs you to do so.

show hardware cpu data-plane

View the driver statistics on the CPU of the specified line card or RPM.

Syntax **show hardware** {**linecard** | **rpm**} *number* **cpu data-plane statistics**

Parameters

linecard	Enter the keyword **linecard** to view cpu data plane statistics for a line card.
rpm	Enter the keyword **rpm** to view cpu data plane statistics for an RPM.
number	Enter a number after the following keywords: • After the keyword **rpm**: Range: 0-1 • After the keyword **linecard**: Range: 0-7 for the C300

Defaults None.

Command Mode

EXEC

EXEC privilege

Command History

Version 7.5.1.0	Introduction

Example 1

Figure 70 shows the output of this command.

```
Force10#show hardware linecard 1 cpu data-plane statistics

-----SOCEND driver statistics for device 4-----
 rxHandle        :0
 noBuff          :0
 noMblk          :0
 noClblk         :0
 recvd           :0
 dropped         :0
 recvToMux       :0
 txInt           :0
 transmitted     :0
 txRequested     :0
 noTxDesc        :0
 txError         :0
 txWrongIntf     :0
 txNotInit       :0
 txReqTooLarge   :0
 txInternalError :0
 rxError         :0
Socend Driver Pool Statistics for device 4
-----------------------------------------
poolMBlkGetCnt      = 0
poolMClGetCnt       = 0
poolClBlkGetCnt     = 0
poolClusterGetCnt   = 0
poolMBlkFreeCnt     = 0
poolMBlkClFreeCnt   = 0
poolClBlkFreeCnt    = 0
poolClFreeCnt       = 0
poolClPoolIdGetCnt  = 1
-----------------------------------------
```

Figure 70 show hardware linecard Command Example

Example 2

Figure 71 shows the output of this command.

```
Force10#show hardware rpm 0 cpu data-plane statistics

-----SOCEND driver statistics for device 2-----
 rxHandle        :0
 noBuff          :0
 noMblk          :0
 noClblk         :0
 recvd           :0
 dropped         :0
 recvToMux       :0
 txInt           :0
 transmitted     :0
 txRequested     :0
 noTxDesc        :0
```

Figure 71 show hardware rpm Command Example

Usage Information

Note: Use this command only when you are working directly with a technical support representative to troubleshoot a problem. Do not use this command unless a technical support representative instructs you to do so.

Interface Troubleshooting

These commands provide additional information related to standard **show interface** commands.

- show hardware interface phy on page 195

show hardware interface phy

View MAC- and PHY-related registers and link status information, including the transmitted and received auto-negotiation control words.

Syntax **show hardware interface** *interface* **phy** [**registers**]

Parameters

phy	Enter the keyowd **phy** to display sent and received auto-negotiation and Layer 1 link status information.
registers	(OPTIONAL) Use the **registers** keyword to display a dump of the PHY registers in hexadecimal.
interface	Enter the following keywords and slot/port or number information: • For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information.

Defaults None.

Command Mode EXEC

EXEC privilege

Command History

Version 7.5.1.0	Introduction

Example Figure 72 shows the output of this command.

```
Force10#show hardware interface gig 1/0 phy
MII Control Register
SpeedSelection: 1000Mbps
AutoNeg: ON
Loopback: False
PowerDown: Flase
Isolate: Flase
DuplexMode: Full
MII Status Register :
AutoNegComplete: False
RemoteFault: False
LinkStatus: False
JabberDetect: False
PHY Identifier Register :
PHY Identifier Register :
Auto-Negotiation Advertisement Register
100MegFullDplx: True
100MegHalfDplx: True
10MegFullDplx: True
10MegHalfDplx: True
Asym Pause: False
Sym Pause: True
Auto-Negotiation Link Partenr Register :
100MegFullDplx: False
100MegHalfDplx: False
10MegFullDplx: False
10MegHalfDplx: False
Asym Pause: False
Sym Pause: False
1000Base-T Control Register:
Master/Slave Mode: Auto
1000MegFullDplx: True
1000MegHalfDplx: True
1000Base-T Status Register
Master/Slave Fault: No
Master/Slave: Slave
Local RX OK: False
Remote RX OK: False
Link Partner 1000MegFullDplx: False
Link Partner 1000MegHalfDplx: False
Idle Error Count: 0
1000Base-T/100Base-TX/10Base-T IEEE Extnd Status Register
1000Base-T/100Base-TX/10Base-T PHY Extnd Control Register
Automatic MDI Crossover Mode: Enable
1000Base-T/100Base-TX/10Base-T PHY Extnd Status Register
Automatic MDI Crossover State: Crossover
```

Figure 72 show hardware interface Command Example

Table 16 describes the fields shown in the figure.

Table 16 show hardware rpm number mac Output Description

Mode Control	Indicates whether auto-negotiation is enabled and the selected speed and duplex.
Mode Status	Displays auto-negotiation fault information. The AutoNegComplete shows True and the LinkStatus field says OK when the interface completes auto-negotiation successfully.
AutoNegotation Advertise	Displays the control words advertised by the local interface during negotiation. The duplex can be full-duplex or half-duplex. The "AsymPause" and "SymPause" describes the types of flow control supported by the local interface.
AutoNegotiation Remote Partner's Ability	Displays the control words advertised by the remote interface during negotiation. The duplex can be full-duplex or half-duplex. The "AsymPause" and "SymPause" fields describe the types of flow control supported by the remote interface.

Table 16 show hardware rpm number mac Output Description

AutoNegotiation Expansion	Parallel detection refers to a handshaking scheme in which the link partners continuously transmit an "idle" data packet using the Fast Ethernet MLT-3 waveform. Equipment that does not support auto-negotiation must be configured to exactly match the mode of operation as the link partner, or else no link can be established.
1000Base-T Control	1000Base-T requires auto-negotiation. The IEEE Ethernet standard does not support setting the speed to 1000 Mbps with the **speed** command without auto-negotiation. C-Series line cards support both full-duplex and half-duplex 1000BaseT.
Automatic MDI Crossover Control	Indicates whether Automatic MDI crossover mode is enabled or disabled
Automatic MDI Crossover State	Indicates whether Automatic MDI crossover state is crossover or normal.

Usage Information

Use the **show hardware interface** *interface* **phy** command when you are troubleshooting a link issue, such as when the **show interfaces** *interface* command is reporting an auto-negotiation mismatch (there is an "Auto-neg Error" string in the output, as shown in Figure 73).

```
Force10#show interfaces gigabit 0/3
GigabitEthernet 0/3 is up, line protocol is down
Hardware is Force10Eth, address is 00:01:e8:07:16:b3
Internet address is not set
MTU 1554 bytes, IP MTU 1500 bytes
LineSpeed auto, Mode full duplex, Auto-neg Error
ARP type: ARPA, ARP Timeout 04:00:00
Last clearing of "show interface" counters 04:39:17
[output omitted]
```

Figure 73 Auto-negotiation Mismatch Example

The **no auto-negotiation** command disables auto-negotiation on an interface. Force10 recommends keeping auto-negotiation enabled.

If the remote interface is not configured for auto-negotiation, the Force10 interface can detect the speed at which the remote device is operating by the type of electrical signal that is arriving.

If the local and remote interfaces are configured differently for auto-negotiation—for example, one side is configured for auto-negotiation and the other side is configured for a particular speed—the link does no not come up. Both sides of the link must be configured for auto-negotiation (recommended) or esle the same speed.

1000Base-T requires auto-negotiation. The IEEE Ethernet standard does not support setting the speed manually to 1000 Mbps.

Advanced ASIC Debugging Information

- clear hardware unit on page 198
- show hardware unit on page 199
- show revision on page 199

clear hardware unit

Clear debugging information on the internal Gigabit Ethernet interfaces on the CSF and FP ASICs.

Syntax

clear hardware {**linecard** *number* | **rpm** *number*} **unit** *number* **counters**

Parameters

linecard	Enter the keyword **linecard** to clear information about a line card.
rpm	Enter the keyword **rpm** to clear information about an RPM.
number	Enter a number: • After the keyword **linecard**: • Range: 0-7 for the C3000 • After the keyword **rpm**: Range: 0-1 • After the **unit** keyword: For a line card: Range: 0 - 3 For an RPM: Range 0 - 4

Defaults

None.

Command Mode

EXEC

EXEC privilege

Command History

Version 7.5.1.0	Introduction

Usage Information

Note: Use this command only when you are working directly with a technical support representative to troubleshoot a problem. Do not use this command unless a technical support representative instructs you to do so.

show hardware unit

View advanced debugging information on the internal Gigabit Ethernet interfaces on the CSF and FP ASICs.

Syntax **show hardware** {**linecard** *number* | **rpm** *number*} **unit** *number* {**counters** | **details** | **port-statistics** | **register**}

Parameters

linecard	Enter the keyword **linecard** to view information about a line card.
rpm	Enter the keyword **rpm** to view information about an RPM.
number	Enter a number after the following keywords: • After the keyword **linecard**: Range: 0-7 for the C300 • After the keyword **rpm**: Range: 0-1 • After the keyword **unit**, enter the number of CSF or FP ASIC.

Defaults None.

Command Mode EXEC

EXEC privilege

Command History

Version 7.5.1.0	Introduction

Usage Information

Note: Use this command only when you are working directly with a technical support representative to troubleshoot a problem. Do not use this command unless a technical support representative instructs you to do so.

show revision

Displays the currently loaded fpga images.

Syntax **show revision**

Defaults No default behavior or value

Command Modes EXEC privilege

Command History

Version 7.5.1.0	Introduced

```
Force10#show revision

-- RPM 0 --
C300 RPM FPGA : 3.8
Required FPGA version : 3.8

-- Secondary RPM --
C300 RPM FPGA : 3.8
Required FPGA version : 3.8

-- Line card 3 --
48 Port 1G LCM FPGA : 2.6
Required FPGA version : 2.6

-- Line card 7 --
48 Port 1G LCM FPGA : 2.6
Required FPGA version : 2.6

Forcve10#
```

Figure 74 show revision command Example

ACL & System-Flow Debug Commands

- clear hardware system-flow on page 200
- show hardware acl on page 201
- show hardware layer3 qos linecard port-set on page 202
- show hardware system-flow layer2 linecard port-set on page 202

clear hardware system-flow

Clear system-flow entry counters.

Syntax **clear hardware system-flow layer2 linecard** *number* **port-set** *number* **counters**

Parameters

number	Enter a number after the following keywords: • After the keyword **linecard**: Range: 0-7 for the C300 • After the keyword **port-set**, enter the port-pipe/FB ID.

Defaults None.

Command Mode EXEC

EXEC privilege

Command History

Version 7.5.1.0	Introduction

Usage Information

Note: Use this command only when you are working directly with a technical support representative to troubleshoot a problem. Do not use this command unless a technical support representative instructs you to do so.

Related Commands

show hardware system-flow layer2 linecard port-set	View system-flow entries.

show hardware acl

View Layer 2 or Layer 3 access control list entries.

Syntax **show hardware {layer2 | layer 3} acl linecard** *number* **port-set** *number*

Parameters

layer2	Enter the keyword **layer2** to view Layer 2 access control list entries for the specified line card.
layer3	Enter the keyword **layer3** to view Layer 3 access control list entries for the Forwarding Processor of the specified line card.
number	Enter a number after the following keywords: • After the keyword **linecard**: Range: 0-7 for the C300 • After the keyword **port-set**, enter the port-pipe/FB ID.

Defaults None.

Command Mode EXEC

EXEC privilege

Command History

Version 7.5.1.0	Introduction

Usage Information

Note: Use this command only when you are working directly with a technical support representative to troubleshoot a problem. Do not use this command unless a technical support representative instructs you to do so.

show hardware layer3 qos linecard port-set

View Layer 3 QoS messages.

Syntax **show hardware layer3 qos linecard port-set**

Parameters

number	Enter a number after the following keywords: • After the keyword **linecard**: Range: 0-7 for the C300 • After the keyword **port-set**, enter the port-pipe/FB ID.

Defaults None.

Command Mode EXEC

EXEC privilege

Command History

Version 7.5.1.0	Introduction

Usage Information

Note: Use this command only when you are working directly with a technical support representative to troubleshoot a problem. Do not use this command unless a technical support representative instructs you to do so.

show hardware system-flow layer2 linecard port-set

View system-flow entries.

Syntax **show hardware system-flow layer2 linecard** *number* **port-set** *number* [**counters**]

Parameters

number	Enter a number after the following keywords: • After the keyword **linecard**: Range: 0-7 for the C300 • After the keyword **port-set**, enter the port-pipe/FB ID.
counters	Enter the keyword **counters** to view counters of system-flow entries.

Defaults None.

Command Mode EXEC

EXEC privilege

Command History

Version 7.5.1.0	Introduction

Usage Information

Note: Use this command only when you are working directly with a technical support representative to troubleshoot a problem. Do not use this command unless a technical support representative instructs you to do so.

Related Commands

clear hardware system-flow	Clear system-flow entry counters.

Interface Management Debug Commands

These commands display advanced debugging information related to the Interface Manager (IFM) process.

- debug ifm trace-flags on page 203
- show software ifm on page 204

debug ifm trace-flags

Turn on IFM internal trace-flags.

Syntax **debug ifm trace-flags** *trace-flag*

Disable this command using the **no debug ifm trace-flags** command.

Parameters

trace-flag	Enter a hexadecimal number representing the trace-flag.

Defaults None.

Command Mode EXEC

EXEC privilege

Command History

Version 7.5.1.0	Introduction

Usage Information Turning on a trace-flag does not result in an output to the console/terminal. It prints trace information to the trace buffer, which is viewed using the **show trace history** command.

Note: Use this command only when you are working directly with a technical support representative to troubleshoot a problem. Do not use this command unless a technical support representative instructs you to do so.

show software ifm

View interface management information.

Syntax

show software ifm {**clients** [**summary**] | **ifagt** *number* | **ifcb** *interface* | **linecard** *number* | **trace-flags**}

Parameters

summary	(OPTIONAL) Enter the keyword **summary** to view show brief information of IFM clients.
ifagt	Enter the keyword **ifagt** to view software pipe and IPC statistics for IFAGT.
ifcb	Enter the keyword **ifcb** to view information about the Interface Control Block.
linecard	Enter the keyword **linecard** view interface managment information for line cards.
trace-flags	Enter the keyword **trace-flags** to view interface managment information for internal trace flags.
interface	Enter one of the following keywords and slot/port or number information: • For a Fast Ethernet interface, enter the keyword **FastEthernet** followed by the slot/port information. • For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For Loopback interfaces, enter the keyword **loopback** followed by a number from 0 to 16383. • For the management interface on the RPM, enter the keyword **ManagementEthernet** followed by the slot/port information. The slot range is 0-1 and the port range is 0. • For the Null interface, enter the keywords **null 0**. • For Port Channel interfaces, enter the keyword **port-channel** followed by a number from 1 to 128. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information.
number	Enter the linecard slot number. Range: 0-7 for the C300

Defaults

None.

Command Mode

EXEC

EXEC privilege

Command History

Version 7.5.1.0	Introduction

Usage Information

Note: Use this command only when you are working directly with a technical support representative to troubleshoot a problem. Do not use this command unless a technical support representative instructs you to do so.

Layer 2 Debug Commands

These commands display tables and advanced debugging information related to the MAC Agent process.

- show software macagent on page 205

show software macagent

Syntax **show software macagent** {**configs** | **mac-addr-table** {**dump** | **count**} | **port interface** *interface* | **port-channel** *number* | **stg** *number* | **vlan** *number*} **line-card** *number*

Parameters

configs	The keyword **configs** shows the initial configurations of the MAC Agent.
mac-addr-table	The keyword **mac-addr-table** shows the number of MAC addresses in the MAC Agent software.
dump	The keyword **dump** shows the mac addresses present in the software.
count	The keyword **count** shows the number of mac addresses present in the software.
port interface	The keywords **port interface** show Layer 2 information for a port on a particular line card.
stg	The keyword **stg** shows the state of each port in a particular Spanning Tree Group on a line card.
vlan	The keyword **vlan** shows Layer 2 information in the MAC Agent for a VLAN on a particular line card.
interface	Enter one of the following keywords and slot/port or number information: • For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information.
number	Enter a number after the following keywords: • After the keyword **linecard**: Range: 0-7 for the C300 • After the **port-channel** keyword, enter the port-channel number. • After the keyword **stg**, enter the Spanning Tree Group number. • After the keyword **vlan**: Range: 1 - 4095 for the C300

Defaults None.

Command Mode EXEC

EXEC privilege

Command History

Version 7.5.1.0	Introduction

Usage Information

Note: Use this command only when you are working directly with a technical support representative to troubleshoot a problem. Do not use this command unless a technical support representative instructs you to do so.

Trace Logging Commands

Trace logging is a critical debugging tool most often used by the Force10 Networks Technical Assistance Center (TAC) to isolate and resolve both software and hardware issues.

- clear trace hardware on page 206
- debug cpu-traffic-stats on page 207
- show command-history on page 208
- show console lp on page 208
- show cpu-traffic-stats on page 209
- show hardware linecard fpga on page 209
- show hardware rpm fpga on page 210
- show trace on page 212

clear trace hardware

Clear the buffered messages in the hardware log.

Syntax **clear trace hardware**

Parameters None.

Defaults None.

Command Mode EXEC

EXEC privilege

Command History

Version 7.5.1.0	Introduction

debug cpu-traffic-stats

Enable the collection of CPU traffic statistics.

Syntax **debug cpu-traffic-stats** [**linecard** {**all** | *number*}]

To disable the debugging, execute the **no debug cpu-traffic-stats** command.

Parameters

linecard	(OPTIONAL) Enter the keyword **linecard** to view CPU traffic statistics for a particular line card.
all	Enter the keyword **all** to specify all line cards.
number	Enter a line card number Range: 0-7 for the C300

Defaults Disabled

Command Modes EXEC privilege

Command History

Version 7.5.1.0	Introduced

Usage Information This command can be used to turn on CPU traffic statistics collection either on a specific linecard or on all linecards. The statistics currently collected are:

- Numbers of packets trapped due to Egress MTU violation
- Numbers of packets trapped due to TTL 1 or IP Options, and
- Numbers of packets trapped due to TTL 0

Note: Use **show cpu-traffic-stats** to view the traffic statistics

This command enables (and disables) the collection of CPU traffic statistics from the time this command is executed, not from system boot). However, excessive traffic received by a CPU will automatically turn on the collection of CPU traffic statics. The message is an indication that collection of CPU traffic is automatically turned on:

```
Excessive traffic is received by CPU and traffic will be rate controlled
```

Note: This command must be enabled before the **show cpu-traffic-stats** command will display traffic statistics. Force10 recommends that you disable debugging (**no debug cpu-traffic-stats)** once troubleshooting is complete.

Related Commands

show cpu-traffic-stats	Display cpu traffic statistics

show command-history

View a buffered log of all commands entered by all users with a time stamp.

Syntax **show command-history**

Parameters None.

Defaults None.

Command Mode EXEC

EXEC privilege

Command History

Version 7.5.1.0	Introduction

Usage Information One trace log message is generated for each command. No password information is saved to this file.

A command-history trace log is saved to a file upon an RPM failover. This file can be analyzed by the Force10 Networks TAC to help identify the root cause of an RPM failover.

show console lp

View the buffered console log for a line card.

Syntax **show console lp** *number*

Parameters

lp	Enter the keyword **lp** to view buffered console messages for a line card processor.
number	Enter a line card number. Range: 0-7 for the C300

Defaults None.

Command Mode EXEC

EXEC privilege

Command History

Version 7.5.1.0	Introduction

Usage Information This log displays initialization messages while the line card is going through the steps to reach check-in status.

show cpu-traffic-stats

View traffic statistics for a line card CPU.

Syntax **show cpu-traffic-stats** [**linecard** {**all** | *number*}]

Parameters

linecard	(OPTIONAL) Enter the keyword **linecard** to view CPU traffic statistics for a particular line card.
all	Enter the keyword **all** to specify all line cards.
number	Enter a line card number Range: 0-7 for the C300

Defaults None.

Command Mode EXEC

EXEC privilege

Command History

Version 7.5.1.0	Introduction

Example

```
Force10#show cpu-traffic-stats linecard all
Stats for Line card 2, Port pipe 0, Port 0
-------------------------------------------
Numbers of packets trapped due to Egress MTU violation   : 1
Numbers of packets trapped due to TTL 1 or IP Options    : 0
Numbers of packets trapped due to TTL 0                  : 0
```

Usage Information The statistics are displayed only if at least one of the counters is non-zero for any linecard, port pipe, or port combination.

show hardware linecard fpga

Display internal information about the line card FPGA.

Syntax **show hardware linecard** *slot* **fpga** {**errorlog | registers | stats**}

Parameters

slot	Enter the line card slot number. Range: 0 to 7
errorlog	(OPTIONAL) Enter the keyword **errorlog** to dump the FPGA Error Log.

registers	(OPTIONAL) Enter the keyword **registers** to dump the FPGA Registers.
stats	(OPTIONAL) Enter the keyword **stats** to dump the FPGA Interrupt Statistics.

Defaults No default behavior or values

Command Modes EXEC

EXEC privilege

Command History

Version 7.5.1.0	Introduced

Usage Information

Note: Use this command only when you are working directly with a technical support representative to troubleshoot a problem. Do not use this command unless a technical support representative instructs you to do so.

show hardware rpm fpga

Display internal RPM FPGA information.

Syntax **show hardware rpm** *slot* **fpga** {**errorlog | linecard** {*slot* **registers** } | **registers | stats**}

Parameters

rpm *slot*	Enter the keyword **rpm** followed by the RPM slot number. Range: 0 or 1
errorlog	(OPTIONAL) Enter the keyword **errorlog** to dump the FPGA Error Log.
linecard *slot* **registers**	Enter the keyword **linecard** followed by the line card slot number and the keyword **registers** to dump the line card's FPGA registers. Range: 0 to 7
registers	(OPTIONAL) Enter the keyword **registers** to dump the FPGA Registers.
stats	(OPTIONAL) Enter the keyword **stats** to dump the FPGA Interrupt Statistics.

Defaults No default behavior or values

Command Modes EXEC

Command History

Version 7.5.1.0	Introduced

Usage Information

Note: Use this command only when you are working directly with a technical support representative to troubleshoot a problem. Do not use this command unless a technical support representative instructs you to do so.

Example

```
Force10>show hardware rpm 0 fpga registers
************************************************
Local Memory Dump

0x0000: 00010401 5a5a1234 01200b11 00000111 00000011 0000000f 000003ff 00000000
0x0020: 00000000 00000000 00010000 00000001 00ffffe 00000104 00000104 00000104
0x0040: 00000104 00000104 00000104 00000104 00000104 00000104 00000104 00000104
0x0060: 00000104 00000104 00000104 00000104 00000104 00000104 00000104 00000104
0x0080: 00000002 0000003f 0000ff01 0000008a 00000000 0000008b 00000089 0000008b
0x00a0: 0000008b 00000000 00000000 00000000 00000000 00000000 00000000 00000000
0x00c0: 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
0x00e0: 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
0x0100: 00000000 000000ff 00000003 00000003 00000008 00000008 00000008 00000008
0x0120: 00000008 00000008 00000008 00000008 00000008 00000008 00000008 00000008
0x0140: 00000008 00000008 00000008 00000008 00000008 00000008 00000008 00000008
0x0160: 00000008 00000008 00000008 00000008 00000008 00000008 00000008 00000008
0x0180: 00000000 00010000 00000000 00000000 00000000 00010000 00000000 00000000
0x01a0: 00000000 00010000 00000000 00000000 00000000 00010000 00000000 00000000
0x01c0: 00000000 00010000 00000000 00000000 00000000 00010000 00000000 00000000
0x01e0: 00000000 00010000 00000000 00000000 00000000 00010000 00000000 00000000
0x0200: 00000000 00000000 000001cc 00000000 00000000 00000000 00000000 00000000
0x0220: 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
0x0240: 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
0x0260: 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
Force10>
```

Figure 75 show hardware rpm fpga registers Command Example

Example

```
orce10#show hardware rpm 1 fpga stats

DUMPING FPGA INTERRUPT STATISTICS

FAN Interrupts received - 0
PSU Interrupts received - 0
Card Presence Interrupts received - 0
I2C[0] Interrupts received - 0
I2C[0] Interrupts handled - 0
I2C[1] Interrupts received - 337
I2C[1] Interrupts handled - 337
I2C[2] Interrupts received - 0
I2C[2] Interrupts handled - 0
I2C[3] Interrupts received - 1209
...
I2C[7] Interrupts handled - 0
HDLC[0] Interrupts received - 0
HDLC[0] Interrupts handled - 0
HDLC[1] Interrupts received - 0
HDLC[1] Interrupts handled - 0
HDLC[2] Interrupts received - 0
HDLC[2] Interrupts handled - 0
...
HDLC[6] Interrupts handled - 0
SPI Interrupts received - 0
SMI Write Interrupts received - 0
LM 80 Interrupts received - 0
LCLK Interrupts received - 0
Mastership change Interrupts received - 1
Over temperature Interrupts received - 0
Low temperature Interrupts received - 0
XFP[0] Interrupts received - 0
XFP[1] Interrupts received - 0
XFP[2] Interrupts received - 0
XFP[3] Interrupts received - 0
XFP[4] Interrupts received - 0
XFP[5] Interrupts received - 0
XFP[6] Interrupts received - 0
XFP[7] Interrupts received - 0
POE[0] Interrupts received - 0
POE[1] Interrupts received - 0
POE[2] Interrupts received - 0
POE[3] Interrupts received - 0
PCI Reset Interrupts received - 0
Spurious interrupts received - 0
Force10>
```

Figure 76 show hardware rpm fpga stats Command Example

show trace

View the software or hardware trace log on an RPM or line card.

Syntax **show trace** [**hardware**] [**all | error | warning** | **linecard** *number*]

Parameters

all	(OPTIONAL) Enter the keyword **all** to view the entire trace log.
error	(OPTIONAL) Enter the keyword **error** to view only the error messages.
warning	(OPTIONAL)Enter the keyword **warning** to view only the warning messages.

linecard	(OPTIONAL) Enter the keyword **linecard** to view trace log messages for a particular line card.
hardware	(OPTIONAL) Enter the keyword **hardware** to view the hardware trace log.
number	Enter the line card slot number. Range: 0-7 for the C300

Defaults None.

Command Mode EXEC

EXEC privilege

Command History

Version 7.5.1.0	Introduction

```
st-c300-2#show trace hardware line 2
[3/7 13:45:59] HW: SWAGT-(swAgt):swAgtProgramCpuPort: masterRpmSlotId=1
swAgtGv0

st-c300-2#show trace hardware
[3/7 13:44:37] HW: CHMGR-(chmgr):lc 2 detected - I2C read rc/0 retry/1
[3/7 13:44:37] HW: POLLER-(PM):doLcsDet: eventId=0, slotId=2, state=1,
value[0]=0x0, value[1]=0x0
[3/7 13:44:37] HW: POLLER-(PM):doLcsDet: eventId=0, slotId=5, state=1,
value[0]=0x0, value[1]=0x0
[3/7 13:44:37] HW: POLLER-(PM):doRsmPwrBusErr: eventId=10, slotId=0, state=1,
value[0]=0x0, value[1]=0x0
[3/7 13:44:38] HW: CHMGR-(chmgr):lc 5 detected - I2C read rc/0 retry/1
[3/7 13:44:39] HW: CHMGR-(swMgr):0x1902 reg w/chmgr
[3/7 13:44:39] HW: CHMGR-(xntpd):0x3982 reg w/chmgr
[3/7 13:44:39] HW: CHMGR-(statMgr):0x1702 reg w/chmgr
[3/7 13:44:39] HW: CHMGR-(diagmgr):0xe02 reg w/chmgr
[3/7 13:44:40] HW: CHMGR-(POEMgr):0x1b02 reg w/chmgr
[3/7 13:44:41] HW: CHMGR-(macmgr_1):0x2f82 reg w/chmgr
[3/7 13:46:1] HW: SWMGR-(swMgr):swMgrProcSwAgtLinkStateChange(): link state
change for slotId=5 linkType=BDP

--more--
```

Figure 77 show trace Command Example

Offline Diagnostics

The offline diagnostics test suite is useful for isolating faults and debugging hardware. The tests results are written to a file in flash memory and can be displayed on screen. Detailed statistics for all tests are collected. These statistics include:

- last execution time
- first and last test pass time
- first and last test failure time
- total run count
- total failure count
- consecutive failure count

- error code

- diag linecard on page 214
- offline on page 215
- online on page 215
- show diag on page 216

diag linecard

Run offline diagnostics on a line card.

Syntax

diag linecard *number* {**alllevels** | **level0** | **level1** | **level2**}

Parameters

alllevels	Enter the keyword **alllevels** to run th complet diagnostics test suite.
level0	Enter the keyword **level0** to check the device inventory and verify the existence of the devices (e.g., device ID test).
leve1	Enter the keyword **Level1** to verify that the devices are accessible via the designated paths (e.g., line integrity tests) and test the internal parts (e.g., registers) of the devices.
level2	Enter the keyword **level2** to perform on-board loopback tests on various data paths (e.g., data port pipe and Ethernet).
number	Enter a number: Range: 0-7 for the C300

Defaults

None.

Command Mode

EXEC

EXEC privilege

Command History

Version 7.5.1.0	Introduction

Usage Information

Warning: Do not use this command when a line card is in a booting state.

offline

Place a line card or RPM in an offline state.

Syntax **offline** {**linecard** | **rpm**} *number*

Parameters

linecard	Enter the keyword **linecard** to place the linecard in an offline state.
rpm	Enter the keyword **rpm** to place the RPM in an offline state.
number	Enter a number after the following keywords: • After the keyword **rpm**: Range: 0-1 • After the keyword **linecard**: Range: 0-7 for the C300

Defaults None.

Command Mode EXEC

EXEC privilege

Command History

Version 7.5.1.0	Introduction

Usage Information

Warning: Do not use this command when a line card is in a booting state.

online

Place a linecard or RPM in an online state.

Syntax **online** {**linecard** | **rpm**} *number*

Parameters

linecard	Enter the keyword **linecard** to place the linecard in an online state.

rpm	Enter the keyword **rpm** to place the RPM in an online state.
number	Enter a number after the following keywords: • After the keyword **rpm**: Range: 0-1 • After the keyword **linecard**: Range: 0-7 for the C300

Defaults None.

Command Mode EXEC

EXEC privilege

Command History

Version 7.5.1.0	Introduction

Usage Information

Warning: Do not use this command when a line card is in a booting state.

show diag

View diagnostics information.

Syntax **show diag** {**information** | **linecard** *number* | **summary** | **detail**}

Parameters

information	Enter the keyword **information** to view diagnostics processes by line card.
linecard	Enter the keyword **linecard** for diagnostics information for a particular line card.
number	Enter a line card number. Range: 0-7 for the C300
summary	Enter the keyword **summary** brief diagnostics information.
detail	Enter the keyword **detail** for detailed diagnostics information.

Defaults None.

Command Mode EXEC

EXEC privilege

Command History

Version 7.5.1.0	Introduction

Usage Information

Warning: Do not use this command when a line card is in a booting state.

Chapter 6 E-Series Debugging and Diagnostics

C-Series	NO
E-Series	✓

Platform Specific Feature: This chapter is specific to the E-Series only.

FTOS supports an extensive suite of protocol-specific debug commands for packet- and event-level debugging. These commands are described throughout this document. In addition, FTOS supports commands for diagnosing suspected hardware issues.

This chapter contains the following sections:

- Diagnostics and Monitoring on page 219
- Offline Diagnostics on page 239
- Hardware Information on page 242

Diagnostics and Monitoring

In addition to these debug commands, FTOS supports diagnostics, monitoring, and fault isolation commands to assist in gathering information.

Important Points to Remember

- Unless otherwise noted, these commands are available on TeraScale systems only.
- The trace-log file captures failure information on *most* failure events.
- The RPM-SFM runtime loopback testfailure initiates an SFM *walk*. The system automatically places each SFM (in sequential order) in an offline state, runs the loopback test, and then places the SFM back in an active state. This continues until the system determines a working SFM combination. If no working combination is found, the system restores to the pre-walking SFM state
- If the line card runtime loopback test fails, the system does not launch an SFM walk.

Note: SFM walking assumes a chassis with the maximum number of SFMs in an active state.

The diagnostics and monitoring commands are:

- dataplane-diag disable loopback on page 220
- dataplane-diag disable sfm-bringdown on page 221
- dataplane-diag disable sfm-walk on page 222
- dataplane-diag disable dfo-reporting on page 223
- diag sfm on page 223
- logging coredump kernel disable on page 224
- logging coredump kernel server on page 225
- logging coredump linecard on page 226
- power-off/on sfm on page 226
- reset sfm on page 230
- show command-history on page 228
- show console on page 230
- show diag sfm on page 231
- show processes communication (deprecated) on page 232
- show processes ipc on page 232
- show processes ipc flow-control on page 234
- show revision on page 236
- show tech-support on page 237

dataplane-diag disable loopback

Disable the runtime loopback test on the primary RPM and line cards.

Syntax **dataplane-diag disable loopback**

To re-enable, use the **no dataplane-diag disable loopback** command.

Defaults Enabled

Command Modes CONFIGURATION

Command History

Version 6.5.4.0	Introduced

Related Commands

show diag sfm	Display the loopback test results
dataplane-diag disable sfm-bringdown	Disable the automatic SFM bringdown
dataplane-diag disable sfm-walk	Diable the automatic SFM walk

Usage Information

The runtime dataplane loopback test, by default, runs in the background. Every 10 seconds, the primary RPM and each line card sends packets through the SFMs and back again (loopback) to monitor the overall health status of the dataplane at a system level. This command disables that automatic runtime loopback test. Execute the **show diag sfm** command to view the diagnostics results (see Figure 78).

Note: Only the Primary RPM can perform runtime dataplane loopback test.

Example

```
Force10#show diag sfm

Switch Fabric Module Loopback Test:   enabled
SFM Walk-Through in Loopback Test:  enabled
SFM Bring-Down in Loopback Test:     enabled
Switch Fabric Module Loopback State:  on

--  Route Processor Modules  --
Slot  Test Status   Last Result   Time Stamp
-------------------------------------------------------
  0     off         none
  1     on          pass         Feb 16 2007 15:50:26

--  Line cards  --
Slot  Test Status   Last Result   Time Stamp
-------------------------------------------------------
  0     off         none
  1     off         none
  2     on          pass         Feb 16 2007 15:50:26
  3     off         none
  4     on          pass         Feb 16 2007 15:50:26
  5     off         none
  6     off         none
Force10#
```

Figure 78 show diag sfm command Example

dataplane-diag disable sfm-bringdown

Disable the automatic bring down of the single faulty SFM identifed by the SFM walk during the RPM-SFM runtime loopback test.

Syntax **dataplane-diag disable sfm-bringdown**

To re-enable the automatic SFM bring down, use the **no dataplane-diag disable sfm-bringdown** command.

Defaults Enabled

Command Modes CONFIGURATION

Command History

Version 6.5.4.0	Introduced

Usage Information If a full set of SFMs are online during the runtime loopback test and a failure occurs, an automatic SFM walk is launched in an attempt to determine if the failure is due to a single faulty SFM. If confimed, the single faulty SFM is identified and disabled by default. This command disables the automatic bring down of that suspect SFM.

Related Commands

dataplane-diag disable loopback	Disable the runtime dataplane loopback test
dataplane-diag disable sfm-walk	Diable the automatic SFM walk
show diag sfm	Display the loopback test results

dataplane-diag disable sfm-walk

Disable the automatic SFM walk that is launched after an RPM-SFM runtime loopback test failure.

Syntax **dataplane-diag disable sfm-walk**

To re-enable the automatic SFM walk, use the **no dataplane-diag disable sfm-walk** command.

Defaults Enabled

Command Modes CONFIGURATION

Command History

Version 6.5.4.0	Introduced

Usage Information If a full set of SFMs are online during the runtime loopback test and a failure occurs, an automatic SFM walk is launched in an attempt to determine if the failure is due to a faulty SFM. This command disables the automatic SFM walk.

Related Commands

dataplane-diag disable loopback	Disable the runtime dataplane loopback test
dataplane-diag disable sfm-bringdown	Disable the automatic SFM bringdown.
show diag sfm	Display the loopback test results

dataplane-diag disable dfo-reporting

Disable the per-channel DFO (deskew FIFO overflow) reporting via event logging.

Syntax **dataplane-diag disable dfo-reporting**

To re-enable, use the **no dataplane-diag disable dfo-reporting** command.

Defaults Enabled

Command Modes CONFIGURATION

Command History

Version 6.5.4.0	Introduced

Usage Information The per-channel DFO error reporting via event logging is enabled by default on TeraScale chassis. The error reporting issues a warning when a temporary dataplane glitch occurs or when a persistent malfunction is detected.

When a DFO error is detected, no automatic action is initiated by the system. The message issued is similar to:

```
%RPM1-P:CP %CHMGR-2-SFM_PCDFO: PCDFO error detected for SFM4
```

This command disables the per-channel DFO reporting.

Related Commands

diag sfm	Initiate a manual dataplane loopback test.
show diag sfm	Display the loopback test results

Note: This command is not supported on the E600i chassis.

diag sfm

Execute a manual dataplane loopback test.

Syntax **diag sfm** [**all-loopback** | **rpm-loopback**]

Parameters

all-loopback	(OPTIONAL) Enter the keyword **all-loopback** to execute a dataplane loopback test from the RPMs and all line cards.
rpm-loopback	(OPTIONAL) Enter the keyword **rpm-loopback** to execute a dataplane loopback test on the RPMs only.

Defaults No default behavior or value

Command Modes EXEC

Command History

Version 6.5.4.0	Introduced

Usage Information If the RPM-SFM or line card-SFM loopback test detects an SFM failure, an attempt is made to isolate a single faulty SFM by automatically *walking* the SFMs. For this failure case, error messages similar to the runtime loopback test error are generated.

If the test passes when the switch fabric is down and there are at least (max-1) SFMs in the chassis, then the system will bring the switch fabric back up automatically. Like the runtime loopback test, the manual loopback test failure will not bring the switch fabric down.

Note: Line card-SFM loopback test failure, during the manual test, will trigger an SFM walk.

Related Commands

reset sfm	Reset the SFM and bring it back online.

logging coredump kernel disable

Disable kernel core-dump logging to the CORE_DUMP_DIR on the flash.

Syntax [**no**] **logging coredump kernel disable**

To re-enable kernel core-dump logging (return to the default), use the **no logging coredump kernel disable** command.

Defaults Enabled (core-dump logging is enabled)

Command Modes CONFIGURATION

Command History

Version 6.5.4.0	Introduced

Usage Information By default, the kernel core-dump is enable and stored in the flash directory:

- Storage Directory Name: **flash:CORE_DUMP_DIR**
  - — Kernel core-dump naming convention is: **f10rp***ProcessorID***.kcore.gz**
    For example: **F10rp1.kcore.gz**

  - — Application core-dump naming convention is:
    rp*ProcessorID* **_***ApplicationName***_***timestamp***.core.gz**

    For example: **rp1_ospf_060307172608.core.gz**
- Multiple core-dumps
  - — Application core-dumps are timestamp embedded and are not overwritten by default. Manually delete the older core-dumps to allow more space on the flash.
  - — Kernel core-dumps are overwritten whenever there is a new core-dump.

Should a crash occur, the large crash kernel file may take more than ten minutes to upload and may require more space on the flash than is available. The HA module is aware of a core-dump in process and will wait until the upload is complete before rebooting the RPM.

Note: Application core-dumps are also automatically uploaded to flash. If there is not enough available space for the kernel core-dump on the flash, the kernel upload will terminate.

Related Commands

logging coredump linecard	Enable core-dump logging on line cards
logging coredump kernel server	Save core-dump logging files to an alternate server

logging coredump kernel server

Designate the logging core-dump files to be saved to a remote server rather than flash.

Syntax **logging coredump kernel server**

To save the logging core-dump files to flash (the default), use the **no logging coredump kernel server** command.

Defaults Saved on flash

Command Modes CONFIGURATION

Command History

Version 6.5.4.0	Introduced

Related Commands

logging coredump linecard	Enable core-dump logging on line cards
logging coredump kernel disable	Disable kernel core-dump logging

logging coredump linecard

Enable line card core-dump logging on a specific line card or on all line cards.

Syntax **logging coredump linecard** [*slot_number* | **all**]

To disable line card coredump logging, use the **no logging coredump linecard** [*slot_number* | **all**] command.

Parameters

linecard *slot number*	Enter the keyword **linecard** followed by the slot number to enable core-dump logging line card details. Range: 0 to 13 on the E1200; 0 on 6 for E600/E600i, and 0 to 5 on the E300.
linecard all	(OPTIONAL) Enter the keyword **linecard all** to enable core-dump logging details on all line cards.

Defaults Disabled (core-dump logging is off)

Command Modes CONFIGURATION

Command History

Version 6.5.4.0	Introduced

Usage Information The line card core-dump is stored on flash in a directory:

- Storage Directory Name: **flash:CORE_DUMP_DIR**
  - Line Card core-dump naming convention is: **f10lp***Slot_Number*.**core.gz**
    For example: **f10lp6.core.gz**
- Multiple core-dumps
  - If multiple line cards crash, the core-dump files will upload simultaneously. However, a second core-dump from the same line card slot will overwrite the first core-dump.
  - During a line card core-dump, the line card interface remains *up* while the core-dump is being written to the directory.

Related Commands

logging coredump kernel server	Save core-dump logging files to an alternate server.
logging coredump kernel disable	Disable kernel core-dump logging.

power-off/on sfm

Power on or off a specified SFM.

Syntax **power-**{**off | on**} **sfm** *slot-number*

Parameters

power-off	Enter the keyword **power-off** to power off the SFM.
power-on	Enter the keyword **power-on** to power on the SFM
sfm *slot-number*	Enter the keyword **sfm** followed by the slot number of the SFM to power on/off. Range: 0 to 7

Defaults No default values or behavior

Command Modes EXEC

Command History

Version 6.5.4.0	Introduced

Usage Information This command is used for diagnostic purposes to isolate and identify a failed SFM when troubleshooting issues related to the chassis dataplane.

Note: Execute this command only during an offline diagnostics; this command may bring down the switch fabric.

When there are a full set of SFMs online, powering down one SFM will reduce the total bandwidth supported by the chassis, and may affect data flow. A warning message is issued at the command line that requires user confirmation to proceed with the command (Figure 79).

Example

```
Force10#power-off sfm 0
SFM0 is active. Powering it off it might impact the data traffic.
Proceed with power-off [confirm yes/no]:yes
Feb 15 23:52:53: %RPM1-P:CP %CHMGR-2-MINOR_SFM: Minor alarm: only eight working SFM
Force10#
```

Figure 79 power-off sfm command with data traffic warning message

Since this command is for diagnostic purposes, you can power off more than one SFM causing a switch fabric module to go down. A warning message is issued at the command line and requires user confirmation to proceed with the command (Figure 80).

Example

```
Force10#power-off sfm 1
WARNING!! SFM1 is active. Powering it off it will cause Switch Fabric to go down!!
Proceed with power-off [confirm yes/no]:yes
Feb 16 00:03:19: %RPM1-P:CP %TSM-6-SFM_SWITCHFAB_STATE: Switch Fabric: DOWN
Feb 16 00:03:20: %RPM1-P:CP %CHMGR-0-MAJOR_SFM: Major alarm: Switch fabric down
Force10#
```

Figure 80 power-off sfm command with switch fabric down warning message

Once the SFM is powered off, the SFM status indicates that the SFM has been powered off by the user. Use the **show sfm all** command to display the status (Figure 81).

Example

```
Force10#show sfm all
Switch Fabric State:  down   (Not enough working SFMs)
Switch Mode: SFM

--  Switch Fabric Modules  --
Slot  Status
------------------------------------------------------------------------------
  0   power off            (SFM powered off by user)
  1   power off            (SFM powered off by user)
  2   power off            (SFM powered off by user)
  3   active
  4   active
  5   active

Force10#
```

Figure 81 show sfm all command Example

Related Commands

show sfm all	Display the current SFM status.

show command-history

Display the trace command history log.

Syntax **show command-history** *line number*

line number	(OPTIONAL) Enter the number of the most recent command history lines (commands). For example, if you want to view the most recent ten command, enter the number 10.

Defaults No default behaviors or values

Command Modes EXEC

Command History

Version 7.4.1.0	Introduced

Example

```
orce10#show command-history 15
[1/15 14:59:27]: CMD-(CLI):[enable]by default from console
[1/15 15:9:15]:  CMD-(CLI):[show linecard all]by default from console
[1/15 15:9:28]:  CMD-(CLI):[interface gigabitethernet 12/0]by default from console
[1/15 15:11:51]: CMD-(CLI):[show startup-config]by default from console
[1/15 15:24:24]: CMD-(TEL46):[enable]by admin from vty0 (peer RPM)
[1/15 15:24:39]: CMD-(TEL46):[show version]by admin from vty0 (peer RPM)
[1/15 15:25:23]: CMD-(TEL46):[show interfaces managementethernet 1]by admin from vty0
(peer RPM)
[1/15 15:25:45]: CMD-(CLI):[configure]by default from console
- Repeated 1 time.
[1/15 15:25:56]: CMD-(CLI):[username mari password ******]by default from console
[1/15 15:26:33]: CMD-(CLI):[configure]by default from console
- Repeated 1 time.
[1/15 15:26:47]: CMD-(CLI):[ip ssh server enable]by default from console
[1/15 15:26:59]: CMD-(SSH47):[enable]by mari from vty0 (10.11.9.207)
[1/15 15:27:8]:  CMD-(SSH47):[show command-history 15]by mari from vty0 (10.11.9.207)
Force10#
```

Figure 82 show command-history

Usage Information

The command history output includes:

- [username *name* passowred *******] —when the command is executed via telnet
- [by default from console] —when the command is executed via console
- [by admin from vty0 (peer RPM)] —with brackets, when the command is executed to primary rpm via standby rpm using telnet-peer-rpm command.

Each command contains up to 50 characters in the display output. FTOS compares the first 50 characters of each command and if the characters are the same (i.e. the same command was issued), then the display output indicates the duplicate entry with "**Repeated *X* times**" (see Figure 82).

All commands executed by all users, except password related commands, are captured in the trace command history log. Each command has a date and time stamp (see Figure 82). The trace-log file has a separate 3000 line buffer to hold command history on a FIFO basis. When the buffer is full, the contents *wraps* (i.e. the first line is automatically deleted to make room for the last command line).This file can be analyzed by the Force10 Technical Assistance Center (TAC) to assist in troubleshooting.

Note: No password information is saved to the trace command history log.

show console

Display, onto the console, background resets, calls, initialization etc. of the designated line card.

Syntax **show console lp** *slot-number*

Parameters

lp *slot-number*	(OPTIONAL) Enter the keyword **lp** and the slot number to view information on the line-card processor in that slot. Range: 0 to 13 on a E1200, 0 to 6 on a E600/E600i, and 0 to 5 on a E300.

Defaults No default behavior or values

Command Modes EXEC privilege

Command History

Version 7.5.1.0	Introduced

Example

```
Force10#show console lp 0
MINI FIFO CONTROL     =  0x0a
MINI FIFO RPM POINTER = 0x000
MINI FIFO CPU POINTER = 0xb0b
Default case. type = 5
frrpaProcessIfmNotif(): Default case. type = 69
frrpaProcessIfmNotif(): Default case. type = 69
frrpaProcessIfmNotif(): Default case. type = 70
frrpaProcessIfmNotif(): Default case. type = 5
frrpaProcessIfmNotif(): Default case. type = 5
frrpaProcessIfmNotif(): Default case. type = 5
frrpaProcessIfmNotif(): Default case. type = 5
frrpaProcessIfmNotif(): Default case. type = 5
frrpaProcessIfmNotif(): Default case. type = 11
frrpaProcessIfmNotif(): Default case. type = 5
frrpaProcessIfmNotif(): Default case. type = 5
frrpaProcessIfmNotif(): Default case. type = 11
Force10#
```

Figure 83 show console lp 0 command Example

reset sfm

Reset a specific SFM module (power-off and then power-on).

Syntax **reset sfm** *slot-number*

Parameters

slot-number	Enter the slot number of the SFM to reset. Range: 0 to 7

Defaults No default values or behavior

Command Modes EXEC

Command History

Version 6.5.4.0	Introduced

Usage Information When an error is detected on an SFM module, this command is a manual recovery mechanism. Since this command can be used with *live* traffic running, the switch fabric will not go down if the switch fabric is in an UP state. When there is a full set of SFMs online in the chassis, resetting one SFM will reduce the total bandwidth supported by the chassis and may affect data flow. A warning message is issued at the command line and requires user confirmation to proceed. (Figure 84)

Example

```
Force10#reset sfm 0
SFM0 is active. Resetting it might temporarily impact data traffic.
Proceed with reset [confirm yes/no]:yes
Feb 16 00:39:30: %RPM1-P:CP %TSM-5-SFM_DISCOVERY: Found SFM 0
Force10#
```

Figure 84 reset sfm command with warning message

This command does not permit resetting any SFM when the system has (max-1) SFM and switch fabric is up (Figure 85)

Example

```
Force10#Force10#reset sfm 1
% Error: SFM1 is active. Resetting it will impact data traffic.
Force10#
```

Figure 85 reset sfm error message

Note: Resetting an SFM in a power-off state is not permitted. Use the command **power-on sfm** to bring the SFM back to a power-on state.

Related Commands

power-off/on sfm	Power on/off an SFM

show diag sfm

Display the results and status of the last chassis runtime/onetime loopback test.

Syntax **show diag sfm**

Defaults No default values or behavior

Command Modes EXEC

Command History

Version 6.5.4.0	Introduced

Example

```
Force10#show diag sfm

Switch Fabric Module Loopback Test:   enabled
SFM Walk-Through in Loopback Test:    enabled
SFM Bring-Down in Loopback Test:      enabled
Switch Fabric Module Loopback State:  on

--  Route Processor Modules  --
Slot  Test Status   Last Result   Time Stamp
-------------------------------------------------------
  0     on          pass         Mar 26 2007 12:41:56
  1     off         none

--  Line cards  --
Slot  Test Status   Last Result   Time Stamp
-------------------------------------------------------
  0     off         none
  1     off         none
  2     on          pass         Mar 26 2007 12:41:56
  3     off         none
  4     off         none
  5     off         none
  6     off         none
  7     off         none
  8     off         none
  9     off         none
 10     off         none
 11     on          pass         Mar 26 2007 12:41:56
 12     off         none
 13     off         none
Force10#
```

Figure 86 show diag sfm command Example

show processes communication (deprecated)

Command History

Version 7.5.1.0	Deprecated (see show processes ipc flow-control)
Version 6.5.4.0	Introduced

show processes ipc

Display IPC messaging used internally between FTOS processes.

Syntax **show processes ipc** [**recv-stats** | **send-stats**] [**cp** | **rp1** | **rp2** | **lp** *linecard-number*]

Parameters

recv-stats	(OPTIONAL) Enter the keyword **recv-stat** to display the receiver-side details of the IPC messages.
send-stats	(OPTIONAL) Enter the keyword **send-stats** to display the sender-side details of the IPC messages.
cp	(OPTIONAL) Enter the keyword **cp** to view the Control Processor's swpq statistics.
rp1	(OPTIONAL) Enter the keyword **rp1** to view the Control Processor's swpq statistics on Route Processor 1.
rp2	(OPTIONAL) Enter the keyword **rp2** to view the Control Processor's swpq statistics on Route Processor 2.
lp *linecard-number*	(OPTIONAL) Enter the keyword **lp** followed by the line card number to view the Control Processor's swpq statistics on the specified line card.

Defaults No default values or behavior

Command Modes EXEC

EXEC privilege

Command History

Version 7.5.1.0	Introduced

Example

```
Force10#show processes ipc recv-stats lp 0
IPC Receive Statistics on LP 0
Memory Used by Recv DB on this processor: 6825992 bytes
SeqNo - Last successfull Guaranteed IPC Pkt Seq No delivered from source to destination
HiWtmk - Highest socket watermark reached for destination
M-SkSize - Max socket size of destination
NonG-Rcvd - No of non-guaranteed IPC pkts received
Pri-Dr - Priority drops done for non-guaranteed pkts due to socket almost-full condition
SkFull-Dr - Any IPC packet dropped because of socket full condition

Source->          Destination   SeqNo  HiWtmk(%)    M-SkSize   NonG-Rcvd  Pri-Dr  SkFull-Dr
TME: 0 ->              TME: 3       0          0       41600           1       0          0
TME: 3 ->            LCMGR: 0       0          0       41600           1       0          0
IPC: 0 ->              IPC: 3   37557          0       41600        6376       0          0
IPC: 3 ->              TME: 3   16215          0       41600           0       0          0
CLI: 0 ->         SYSADMTSK: 3   11483          0       41600           0       0          0
Force10#
```

Figure 87 show processes ipc recv-stats Command Example

Example

```
Force10#show processes ipc send-stats
IPC Send Statistics on CP
Memory Used by Send DB on this processor: 2303000 bytes
SeqNo   -  Last sent guaranteed IPC pkt sequence no from this source to destination
Success -  No of successfull guaranteed IPC packets sent from source to destination
1st-R   -  No of first retry attempts
2nd-R   -  No of second retry attempts
Fails   -  No of guaranteed IPC pkts that could not be transmitted
RTT(ms) -  Avg. Round Trip time for guaranteed IPC packets in millisecs
NonG-S  -  No of non-guaranteed IPC pkts succesfully sent. This does not include those sent by SWP
NonG-F  -  No of non-guaranteed IPC pkt transmission failures
SWP-S   -  No of non-guaranteed SWP IPC pkts succesfully sent
SWP-F   -  No of non-guaranteed SWP IPC pkt transmission failures

Source->     Destination   SeqNo   Success   1st-R   2nd-R   Fails  RTT(ms) NonG-S  NonG-F  SWP-S  SWP-F
TME: 0 ->         TME: 1   15868         1       0       0       0       1       0       0      0      0
Force10#
```

Figure 88 show processes ipc send-stats Command Example

Usage Information

These commands should be used only when you are working directly with Force10 TAC (Technical Assistance Center) while troubleshooting a problem.

show processes ipc flow-control

Display the Single Window Protocol Queue (swpq) statistics.

Syntax

show processes ipc flow-control [**cp** | **rp1** | **rp2** | **lp** *linecard-number*]

Parameters

cp	(OPTIONAL) Enter the keyword **cp** to view the Control Processor's swpq statistics.
rp1	(OPTIONAL) Enter the keyword **rp1** to view the Control Processor's swpq statistics on Route Processor 1.
rp2	(OPTIONAL) Enter the keyword **rp2** to view the Control Processor's swpq statistics on Route Processor 2.
lp *linecard-number*	(OPTIONAL) Enter the keyword **lp** followed by the line card number to view the Control Processor's swpq statistics on the specified line card.

Defaults

No default values or behavior

Command Modes

EXEC

EXEC privilege

Command History

Version 7.5.1.0	Introduced

Example

```
Force10# show processes ipc flow-control rp2

[qid] Source->Dest       Cur High #of #of  #msg   #msg Retr total
                         Len Mark to  Retr Sent   Ackd
-------------------------------------------------------------------
[1] unknown2->unknown2   0    0    0   0    0      0    3    3
[2] l2pm0->spanMgr0      0    2    0   0    2298   2298 25   25
[3] fvrp0->macMgr0       0    0    0   0    0      0    25   25
[4] l2pm0->fvrp0         0    2    0   0    1905   1905 25   25
[5] fvrp0->l2pm0         0    0    0   0    0      0    25   25
[6] stp0->l2pm0          0    0    0   0    0      0    25   25
[7] spanMgr0->macMgr0    0    0    0   0    0      0    25   25
[8] spanMgr0->ipMgr0     0    0    0   0    0      0    25   25
Force10#
```

Figure 89 show processes ipc flow-control rp Command Example

Example

```
Force10#show processes ipc flow-control lp 10
Q Statistics on LP 10
       TxProcess  RxProcess     Cur     High   Time   Retries   Msg     Ack    Aval    Max
                                Len     Mark   Out             Sent    Rcvd   Retra   Retra
-------------------------------------------------------------------------------------------
  ACL_AGENT10          PIM0      0        0      0      0         0       0      20      20
  ACL_AGENT10          PIM0      0        0      0      0         0       0      20      20
    FRRPAGT10         FRRP0      0        0      0      0         0       0      30      30
      IFAGT10        IFMGR0      0        1      0      0         1       1       8       8
LPDMACAGENT10       MACMGR0      0        0      0      0         0       0      25      25
Force10#
```

Figure 90 show processes ipc flow-control lp Command Example

Table 17 defines the fields displayed in Figure 90.

Table 17 show processes ipc flow-control Display Definitions

Field	Description
TxProcess	Sender Process
RxProcess	Receiver Process
Cur Len	The number of messages, in the sender process, waiting to be sent to the receiver process
High Mark	The maximum number of accumulated messages (over the life of the queue), in the sender process, waiting to be sent out to the receiver process
Time Out	The time period the sender process waits for acknowledgement from the receiver process before attempting to resend the queued messages
Retries	The number of successive attempts (retries) the sender process will make to send the messages to the receiver process
Msg Sent	The accumulated number of messages sent between the sender and receiver processes from the time the queue was created.
Ack Rcvd	The number of acknowledgements received from the receiver process
Aval Retrans	The current number of attempts, for retransmission, available in the event an acknowledgement is not received. This value decrements on every retry and may fall below the initial value, of "Max Retrans" to zero, in case the receiver is not responding. This count is reset dynamically to Max Retrans value in case the queue starts to function after experiencing some acknowledgement loss
Max Retrans	The max number of retransmission attempts configured for a sender - receiver pair

Usage Information

The Single Window Protocol (SWP) provides flow-control-based reliable communication between the sending and receiving software tasks.

Important Points to Remember

- A sending task enqueues messages into the SWP queue3 for a receiving task and waits for an acknowledgement.
- If no response is received within a period of time, the SWP time-out mechanism re-submits the message at the head of the FIFO queue.
- After retrying several times, the following time-out message is generated:

  `SWP-2-NOMORETIMEOUT`
- In the display output in Figure 90, a retry (Retries) value of zero indicates that the SWP mechanism reached the maximum number of retransmissions without an acknowledgement.

show revision

Display revision numbers of all line card, RPM, and SFM components.

Syntax **show revision**

Defaults No default behavior or value

Command Modes EXEC privilege

Command History

Version 7.5.1.0	Introduced

Example

```
Force10#show revision

--  RPM 0  --
panda         : ASIC - 0x72632000
bedrock       : 0x34
helio         : 0x13
tabby         : 0x7
willow        : 0x13

--  Line card 0 --
lc pic 0         : 1.0
lc pic 1         : 1.0
marvel serdes    : 0x0
aquarius         : 0x15
galle            : 0x11
lynx             : 0x7
mini             : 0x22
pandora          : 0xd

--  Line card 1 --
lc pic 0         : 1.1
lc pic 1         : 1.1
marvel serdes    : 0xcd4
aquarius         : 0x15
galle            : 0x11
lynx             : 0x7
mini             : 0x25
pandora          : 0x9

--  SFM 0 --
simba         : 0x1
faith         : 0xc

--  SFM 1 --
simba         : 0x1
faith         : 0xc

--  SFM 2 --
simba         : 0x1
faith         : 0xc

--  SFM 3 --
simba         : 0x1
faith         : 0xc
--  SFM 4 --
simba         : 0x1
faith         : 0xc

...
```

Figure 91 show revision command Example (partial)

show tech-support

View the necessary information for the Force10 Networks Technical Assistance Center to assist and perform troubleshooting.

Syntax **show tech-support** [**page**]

Parameters

page	(OPTIONAL) Enter the keyword **page** to view 24 lines of text at a time. Press the SPACE BAR to view the next 24 lines. Press the ENTER key to view the next line of text.

Command Modes EXEC privilege

Command History

Version 6.5.4.0	Show clock included in display

Example

```
Force10#show tech-support
 ---------------------------------- show version -------------------------------
Force10 Networks Real Time Operating System Software

System image file is "flash://FTOS-EF-6.5.4.1.bin"

Chassis Type: E600
Control Processor: IBM PowerPC 750FX (Rev D2.2) with 536870912 bytes of memory.
Route Processor 1: IBM PowerPC 750FX (Rev D2.2) with 1073741824 bytes of memory.
Route Processor 2: IBM PowerPC 750FX (Rev D2.2) with 1073741824 bytes of memory.

128K bytes of non-volatile configuration memory.

  1 Route Processor Module
  9 Switch Fabric Module
  1 48-port GE line card with SFP optics (EF)
  1 4-port 10GE LAN/WAN PHY line card with XFP optics (EF)
  1 48-port 10/100/1000Base-T line card with RJ-45 interfaces (EF)
  1 FastEthernet/IEEE 802.3 interface(s)
 96 GigabitEthernet/IEEE 802.3 interface(s)
  4 Ten GigabitEthernet/IEEE 802.3 interface(s)
----------------------------------- show clock --------------------------------
18:23:19.799 UTC Fri Mar 16 2007
 ---------------------------------- show HA information ----------------------
--  RPM Status  --
-------------------------------------------------
 RPM Slot ID:               0
 RPM Redundancy Role:       Primary
 RPM State:                 Active
 RPM SW Version:            7.4.1.1
 Link to Peer:              Down
 Peer RPM:                  not present

--  RPM Redundancy Configuration  --
-------------------------------------------------
 Primary RPM:               rpm0
 Auto Data Sync:            Full
 Failover Type:             Hot Failover
 Auto reboot RPM:           Disabled
 Auto failover limit:       3 times in 60 minutes

--  RPM Failover Record  --
-------------------------------------------------
 Failover Count:            0
 Last failover timestamp:   None
 Last failover Reason:      None

 ---------------------------------- show running-config ------------------------
Current Configuration ...
! Version 6.5.4.1
!
boot system rpm0 primary flash://FTOS-EF-6.5.4.1.bin
boot system rpm0 secondary flash://FTOS-EF-6.5.4.1.bin
boot system rpm0 default flash://FTOS-EF-6.5.4.1.bin
!
redundancy auto-failover-limit count 3 period 60
redundancy auto-synchronize full
redundancy disable-auto-reboot rpm
redundancy primary rpm0
!
hostname E600-TAC-3
!
cam-ipv4flow multicast-fib 9 pbr 1 qos 8 system-flow 5 trace-list 1
!
...
```

Figure 92 partial output of the show tech-support Command Example

Usage Information

This display output is an accumulation of the same information that is displayed when you execute the one of the following show commands:

- **show cam-profile**
- **show cam-ipv4flow**
- **show chassis**
- **show clock**
- **show environment**
- **show file-system**
- **show interface**
- **show inventory**
- **show ip management-route**
- **show ip protocols**
- **show ip route summary**
- **show processes cpu**
- **show processes memory**
- **show redundancy**
- **show rpm**
- **show running-conf**
- **show sfm**
- **show version**

Without the **page** option, the command output is continuous, use CNTL-z to interrupt the command output.

Related Commands

show version	Display the FTOS version.
show linecard	Display the line card(s) status.
show environment	Display system component status.
show processes memory	Display memory usage based on running processes.

Offline Diagnostics

The offline diagnostics test suite is useful for isolating faults and debugging hardware. The tests results are written to a file in flash memory and can be displayed on screen. Detailed statistics for all tests are collected.

These statistics include:

- last execution time
- first test pass time and last test pass time
- first test failure time and last test failure time
- total run count

- total failure count
- consecutive failure count
- error code

The offline diagnostics commands are:

- diag linecard on page 240
- offline on page 241
- online on page 241
- show diag on page 242

diag linecard

Run offline diagnostics on a line card(s).

Syntax **diag linecard** *number* {**alllevels | level0 | level1 | level2**} | {**terminate**}

To terminate the offline diagnostics, use the **diag linecard** *number* **terminate** command.

Parameters

number	Enter the line card slot number. Range: 0 to 13 on a E1200, 0 to 6 on a E600, and 0 to 5 on a E300.
alllevels	Enter the keyword **alllevels** to run the complete offline diagnostic test.
level0	Enter the keyword **level0** to check the device inventory and verify the existence of the devices.
level1	Enter the keyword **Level1** to verify that the devices are accessible via the designated paths (line integrity tests) and test the internal registers of the devices.
level2	Enter the keyword **level2** to perform on-board loopback tests on various data paths (data port pipe and Ethernet).
terminate	Enter the keyword **terminate** to stop the offline diagnostics tests.

Defaults All Levels (**alllevels**)

Command Modes EXEC

EXEC privilege

Command History

Version 6.5.4.0	Introduced

offline

Place a line card in an offline state.

Syntax **offline** {**linecard** *number* }

Parameters

linecard *number*	Enter the keyword **linecard** followed by the line card slot number. Range: 0 to 13 on a E1200, 0 to 6 on a E600, and 0 to 5 on a E300.

Defaults No default behavior or values

Command Mode EXEC

EXEC privilege

Command History

Version 6.5.4.0	Introduced

online

Place a line card in an online state.

Syntax **online** {**linecard** *number* | **rpm** *number*}

Parameters

linecard *number*	Enter the keyword **linecard** followed by the line card slot number. Range: 0 to 13 on a E1200, 0 to 6 on a E600, and 0 to 5 on a E300.

Defaults No default behavior or values

Command Mode EXEC

EXEC privilege

Command History

Version 6.5.4.0	Introduced

show diag

View current diagnostics information.

Syntax **show diag** {**information**} [**linecard** *number* [**detail** | **periodic** | **summary**]]

Parameters

information	Enter the keyword **information** to view current diagnostics information in the system.
linecard *number*	(OPTIONAL) Enter the keyword **linecard** followed by the line card slot number. Range: 0 to 13 on a E1200, 0 to 6 on a E600, and 0 to 5 on a E300.
detail	(OPTIONAL) Enter the keyword **detail** to view detailed diagnostics information.
periodic	(OPTIONAL) Enter the keyword **periodic** to display diagnostics results periodically.
summary	(OPTIONAL) Enter the keyword **summary** to view a summary of the diagnostics information.

Defaults **summary**

Command Mode EXEC

EXEC privilege

Command History

Version 6.5.4.0	Introduced

Hardware Information

These commands display information from a hardware sub-component or ASIC.

Warning: These commands should be used only when you are working directly with Force10 TAC (Technical Assistance Center) while troubleshooting a problem. Do not use these command without the assistance of a Force10 TAC representative. To contact Force10 TAC for assistance:
E-mail Direct Support: support@Force10networks.com
Web: www.force10networks.com/support/
Telephone support:
US and Canada customers: 866-965-5800
International customers: 408-965-5800

The commands are:

- clear hardware btm on page 243
- clear hardware rpm mac counters on page 244

- show hardware btm on page 244
- show hardware fpc forward on page 246
- show hardware fpc lookup detail on page 249
- show hardware rpm cp on page 250
- show hardware rpm mac counters on page 252
- show hardware rpm rp1/rp2 on page 253
- show interfaces link-status on page 253
- show interfaces phy on page 254
- show interfaces transceiver on page 256
- show logging driverlog on page 257

clear hardware btm

Clear the Buffer Traffic Manager (BTM) error counters and status registers.

Syntax **clear hardware** {**rpm** | **linecard**} *number* **port-set** *pipe-number* **btm** {**egress | ingress | all**} {**errors** | **status**}

Parameters

rpm	Enter the keyword **rpm** to clear BTM error counters or status registers on the RPM.
linecard *number*	Enter the keyword **linecard** followed by the line card slot number to clear BTM error counters or status registers on the specified line card. Range: 0 to 13 on a E1200, 0 to 6 on a E600/E600i, and 0 to 5 on an E300
port-set *pipe-number*	Enter the keyword **port-set** followed by the number of the line card or RPM's port pipe. Range: 0 to 1
egress errors | **status**	(OPTIONAL) Enter the keywords **egress errors** or **egress status** to clear egress BTM error counters or ingress BTM status registers.
ingress errors | **status**	(OPTIONAL) Enter the keywords **ingress errors** or **ingress status** to clear ingress BTM error counters or ingress BTM status registers.
all errors | **status**	(OPTIONAL) Enter the keywords **all errors** or **all status** to clear both egress and ingress BTM error counters and status registers.

Defaults No default behavior or values

Command Modes EXEC

EXEC privilege

Command History

Version 6.5.4.0	Introduced

Example

```
Force10#clear hardware linecard 2 port-set 0 btm ingress errors
Force10#clear hardware rpm 1 port-set 0 btm ingress errors
Force10#clear hardware rpm 0 port-set 0 btm ingress errors
% Error: RPM 0 is not active.
Force10#
```

Related Commands

show hardware btm	Display the BTM counters

clear hardware rpm mac counters

Clear the MAC counters for the party-bus control switch on the IPC subsystem of the RPM.

Syntax **clear hardware rpm** *slot-number* **mac counters**

Parameters

slot-number	Enter the RPM slot number. Range: 0 -1

Defaults No default behavior or values

Command Mode EXEC

EXEC privilege

Command History

Version 6.5.4.0	Introduced

show hardware btm

Display the Buffer Traffic Manager (BTM) error counters, status registers, or packet queue.

Syntax **show hardware** {**rpm** | **linecard**} *number* **port-set** *pipe-number* **btm** {**egress** | **ingress** | **all**} {**errors** | **status** | **queues**} {**register** *starting-value* [*number_of_registers*]}

Parameters

rpm	Enter the keyword **rpm** to display RPM error counters, status registers, or packet queue from the BTM.
linecard *number*	Enter the keyword **linecard** followed by the line card slot number to display BTM error counters, status registers, or packet queue on the specified line card. Range: 0 to 13 on a E1200, 0 to 6 on a E600/E600i, and 0 to 5 on an E300
port-set *pipe-number*	Enter the keyword **port-set** followed by the number of the line card's port pipe. Range: 0 to 1
egress errors | **status** | **queues**	(OPTIONAL) Enter the keywords **egress errors, egress status**, or **egress queues** to view egress BTM error counters, status registers, or packet queue.
ingress errors | **status** | **queues**	(OPTIONAL) Enter the keywords **ingress errors, ingress status**, or **ingress queues** to view ingress BTM error counters, status registers, or packet queue.
all errors | **status** | **queues**	(OPTIONAL) Enter the keywords **all errors, all status**, or **all queues** to view all BTM error counters, status registers, or packet queue
register *starting-value* [*number_of_registers*]	Enter the keyword **register** followed by the starting value of the register to read from. Range: 0 to 16777212 Optionally, enter the number of registers to read from. If no value is specified, only one line is displayed. Range: 1 to 512

Defaults

No default behavior or values

Command Modes

EXEC

EXEC privilege

Command History

Version 6.5.4.0	Introduced

Example

```
Force10#show hardware linecard 1 port-set 2 btm all errors
Output for portpipe 0 Ingress
   PC_SPI4_BADPORT_CNTR   [0x000230]     =     16777216
   PC_SPI4_EOP_ABORT_CNTR [0x000234]     =     33554432
   PC_SPI4_MISS_SOP_CNTR  [0x00238]      =     50331648
Output for portpipe 0 Egress
   FC_BAD_CRC_ERR_CNTR    [0x000250]     =     150994944
Force10#
```

Related Commands

clear hardware btm	Clear the btm counters

show hardware fpc forward

Display receive and transmit counters, error counters and status registers for the forwarding functional area of the FPC (flexible packet classification engine).

Syntax **show hardware linecard** *number* **port-set** *pipe-number* **fpc forward** {**counters** | **drops** | **spi** {**err-counters** | *spichannel#* **counters**} | **status**}

Parameters

linecard *number*	Enter the keyword **linecard** followed by the line card slot number. Range: 0 to 13 on a E1200, 0 to 6 on a E600/E600i, and 0 to 5 on an E300
port-set *pipe-number*	Enter the keyword **port-set** followed by the number of the line card's port pipe. Range: 0 to 1
counters	(OPTIONAL) Enter the keyword **counters** to display the FPC receive and transmit packet, byte counters, and error counters.
drops	(OPTIONAL) Enter the keyword **drops** to display FPC drop-related error counters.
spi err-counters	(OPTIONAL) Enter the keywords **spi err-counters** to display the FPC System Packet Interface (SPI) receive and transmit packet, byte counters, error counters, and key status registers on the ingress and egress paths.
spi *spichannel#* **counters**	(OPTIONAL) Enter the keywords **spi** *spichannel#* **counters** to display the FPC System Packet Interface level 4 (SPI4) counters.
status	(OPTIONAL) Enter the keywords **status** to display FPC status registers.

Defaults No default values or behavior

Command Modes EXEC

EXEC privilege

Command History

Version 6.5.4.0	Introduced

Example

```
Force10#show hardware linecard 4 port-set 0 fpc forward drops
                 SPI 0
ICMP Drops       : 0x0
ACL Drops        : 0x0
IBC_DROP         : 0
EBC_DROP         : 0
IFA_DROP_CNT     : 0
EFA_DROP_CNT     : 0
CMB_IC_DROP      : 0
CMB_LG_DROP      : 0
CMB_SF_DROP      : 0
CMB_IPM_DROP     : 0
CMB_OPM_DROP     : 0
                 SPI 1
ICMP Drops       : 0x0
ACL Drops        : 0x0
IBC_DROP         : 0
EBC_DROP         : 0
IFA_DROP_CNT     : 0
EFA_DROP_CNT     : 0
CMB_IC_DROP      : 0
CMB_LG_DROP      : 0
CMB_SF_DROP      : 0
CMB_IPM_DROP     : 0
CMB_OPM_DROP     : 0
Force10#
```

Figure 93 show hardware fpc forward drops Command Example

Example

```
Force10#show hardware linecard 4 port-set 0 fpc forward counters
Portpipe 0
Ingress Counters                    SPI 0
    SPI4_ABORT                       : 0
    MAC_2_T2_DIP2                    : 0
    MAC_2_T2_DIP4                    : 0
    SPI4_LOSS_CNT                    : 0
    MAC_2_T2_RX_PKT_COUNTER_CRC      : 0
    MAC_2_T2_RX_PKT_COUNTER_LO       : 0
    MAC_2_T2_RX_PKT_COUNTER_HI       : 0
    IBC_DROP                         : 0
    IFA_TX_PKT_LO                    : 0
    IFA_TX_PKT_HI                    : 0
Egress Counters                     SPI 0
    SPI4_ABORT                       : 0
    C2_TO_T2_DIP2                    : 0
    C2_TO_T2_DIP4                    : 0
    SPI4_LOSS_CNT1                   : 0
    C2_TO_T2_RX_PKT_COUNTER_CRC      : 0
    C2_TO_T2_RX_PKT_COUNTER_LO       : 0
    C2_TO_T2_RX_PKT_COUNTER_HI       : 0
    EBC_DROP                         : 0
    EFA_TX_PKT_LO                    : 0
    EFA_TX_PKT_HI                    : 0
    EGRESS_DROP_COUNT                : 0
CMB_IC_DROP                 : 0
CMB_LG_DROP                 : 0
CMB_SF_DROP                 : 0

CMB_IPM_DROP                : 0
CMB_OPM_DROP                : 0
Portpipe 0
Ingress Counters                    SPI 1
    SPI4_ABORT                       : 0
    MAC_2_T2_DIP2                    : 0
    MAC_2_T2_DIP4                    : 0
    SPI4_LOSS_CNT                    : 0
    MAC_2_T2_RX_PKT_COUNTER_CRC      : 0
    MAC_2_T2_RX_PKT_COUNTER_LO       : 0
    MAC_2_T2_RX_PKT_COUNTER_HI       : 0
    IBC_DROP                         : 0
    IFA_TX_PKT_LO                    : 0
    IFA_TX_PKT_HI                    : 0
Egress Counters                     SPI 1
    SPI4_ABORT                       : 0
    C2_TO_T2_DIP2                    : 0
    C2_TO_T2_DIP4                    : 0
    SPI4_LOSS_CNT1                   : 0
    C2_TO_T2_RX_PKT_COUNTER_CRC      : 0
    C2_TO_T2_RX_PKT_COUNTER_LO       : 0
    C2_TO_T2_RX_PKT_COUNTER_HI       : 0
    EBC_DROP                         : 0
    EFA_TX_PKT_LO                    : 0
    EFA_TX_PKT_HI                    : 0
    EGRESS_DROP_COUNT                : 0
CMB_IC_DROP                 : 0
CMB_LG_DROP                 : 0
CMB_SF_DROP                 : 0
CMB_IPM_DROP                : 0
CMB_OPM_DROP                : 0
Force10#
```

Figure 94 show hardware fpc forward counters Command Example

Related Commands

show hardware fpc lookup detail	Display fpc lookup information.

show hardware fpc lookup detail

Display diagnostic and debug information related to the lookup functional area of the Flexible Packet Classification (FPC).

Syntax **show hardware linecard** *number* **port-set** *pipe-number* **fpc lookup detail**

Parameters

linecard *number*	Enter the keyword **linecard** followed by the line card slot number. Range: 0 to 13 on a E1200, 0 to 6 on a E600/E600i, and 0 to 5 on an E300
port-set *pipe-number*	Enter the keyword **port-set** followed by the number of the line card's port pipe. Range: 0 to 1

Defaults No default values or behavior

Command Modes EXEC

EXEC privilege

Command History

Version 6.5.4.0	Introduced

Example

```
Force10#show hardware linecard 0 port-set 0 fpc lookup detailed

Summary of Error Registers
------- -- ----- ---------

0 Counters Enabled :
Cyclone 1.5 ChassisMap           : 0x00000000
Cyclone 1.5 MixedMode            : 0x00000000
T2L party Status                : No Errors
    partyType           ErrorCount
    ----------           ----------

 Summary of Last 16 CamSearches
============================================================
I                 CamKey                P   T    R    P E  N
n                                       a   a    P    o g  W
d                                       r   b    I    r r  I
e                                       i   l    D    t e  I
x                                       t   e         I s  n
                                        y   T         d s  d
                                            y              e
                                            p              x
21554 50697065.5f302045.72726f72.2026204d.61736b20 0x52656769
0x73746572 0x2044756d 1879719229 1027423549 1027423549

Summary of Last 16 CamHits
==========================================
I   Hit0/     Hit1/     S    R    P E  N
n   Index0    Index1    r    P    o g  W
d                       c    I    r r  I
e                       H    D    t e  I
x                       C         I s  n
                        o         d s  d
                        d              e
                        e              x
 0 0/0x00000 0/0x00000 0x00 0x00 00 0 00
 1 0/0x00000 0/0x00000 0x00 0x00 00 0 00
 2 0/0x00000 0/0x00000 0x00 0x00 00 0 00
 3 0/0x00000 0/0x00000 0x00 0x00 00 0 00
 4 0/0x00000 0/0x00000 0x00 0x00 00 0 00
 5 0/0x00000 0/0x00000 0x00 0x00 00 0 00
 6 0/0x00000 0/0x00000 0x00 0x00 00 0 00
 7 0/0x00000 0/0x00000 0x00 0x00 00 0 00
 8 0/0x00000 0/0x00000 0x00 0x00 00 0 00
 9 0/0x00000 0/0x00000 0x00 0x00 00 0 00
10 0/0x00000 0/0x00000 0x00 0x00 00 0 00
11 0/0x00000 0/0x00000 0x00 0x00 00 0 00
12 0/0x00000 0/0x00000 0x00 0x00 00 0 00
13 0/0x00000 0/0x00000 0x00 0x00 00 0 00
Force10#
```

Related Commands

show hardware fpc forward	Display information related to FPC forward.

show hardware rpm cp

Display advanced debugging information for the RPM processors.

Syntax **show hardware rpm** *slot-number* **cp** {**data-plane** | **management-port**} | **party-bus**} {**counters** | **statistics**}

Parameters

slot-number	Enter the RPM slot number 0 or 1.
data-plane	(OPTIONAL) Enter the keywords **data-plane** to display information about the dataplane interface on the control processor of the specified RPM.
management-port	(OPTIONAL) Enter the keywords **management-port** to display information about the managment-port interface of the conrol processor on the specified RPM.
party-bus	(OPTIONAL) Enter the keywords **party-bus** to display control processor information on the party-bus of the specified RPM.
counters	(OPTIONAL) Enter the keyword **counters** to display the standard Ethernet counters.
statistics	(OPTIONAL) Enter the keyword **statistics** to display driver-related counters

Defaults

No default values or behavior

Command Modes

EXEC

EXEC privilege

Command History

Version 6.5.4.0	Introduced

Example

```
Force10#show hardware rpm 0 cp data-plane counters
Input statistics
     31262 Bytes, 319 Frames,
     31262 Total Bytes, 319 Total Frames,
     0 Broadcasts, 0 Multicasts,
     0 CRC, 0 Oversize,
     0 Fragments, 0 Jabber,
     0 64-byte Frames, 638 127-byte Frames,
     0 255-byte Frames, 0 511-byte Frames,
     0 1023-byte Frames, 0 Max Frames,
     0 Error, 0 Dropped,
     0 Undersized

Output statistics
     31262 Bytes, 319 Frames, 357822480 Total Bytes,
     0 Collisions, 0 Late collisions,
     0 Broadcasts, 0 Multicasts

Force10#show hardware rpm 0 cp data-plane statistics
Input statistics
   640 Interrupts, 0 Ticks,
   0 DMA Errors, 0 Stopped,
   0 Cleanup, 0 Throttle Drops,
   0 Status Error, 0 Too Large,
   0 Buff Err0, 320 Receive Interrupts,
   320 Readied for Protocols, 0 Jumbo,
   0 Jumbo Error, 0 Ignored,
   0 Jumbo Missing first, 0 Jumbo Dup First,
   0 Jumbo Mget Failed,
   0 Jumbo ClGet Failed, 0 No Mem,
   0 Overflow fix count,
   0 Mget Failed, 0 ClGet Failed

Output statistics
   0 Pause, 0 Watchdog,
   0 Late Collision, 0 Underrun,
   0 Retransmit Limit, 0 Out Frames,
   0 No Mem, 0 Phy Syncs
Force10#
```

Figure 95 show hardware rpm command Examples

show hardware rpm mac counters

Display receive- and transmit-counters for the party-bus control switch on the IPC subsystem of the RPM.

Syntax **show hardware rpm** *slot-number* **mac counters** [**port** *port-number*]

Parameters

slot-number	Enter the RPM slot number 0 or 1.
port *port-number*	(OPTIONAL) Enter the keyword **port** followed by the port number of the pairty-bus control switch. Range: 0 to 24

Defaults No default values or behavior

Command Modes EXEC

EXEC privilege

Command History

Version 6.5.4.0	Introduced

Example

```
Force10#show hardware rpm 0 mac counters
 PORT#              RX Frames TX Frames
--------------------------------------
   0 [LC0     ]          0          5
   1 [LC1     ]      25171       2119
   2 [LC2     ]      13967       2108
   3 [LC3     ]      13964       2108
   4 [LC4     ]          0          5
   5 [LC5     ]      25134       2108
   6 [LC6     ]          0          5
   7 [LC7     ]          0          5
   8 [LC8     ]          0          5
   9 [LC9     ]          0          5
  10 [LC10    ]          0          5
  11 [LC11    ]          0          5
  12 [LC12    ]          0          5
  13 [LC13    ]          0          5
  20 [LOC-CP  ]      23232     101339
  21 [LOC-RP1]        5248       1097
  22 [LOC-RP2]        5250       1104
  23 [UNUSED  ]          0          0
  24 [REM-RPM]      12617      12630
Force10#
```

Figure 96 show hardware rpm mac counters Command Example

Table 18 defines the fields displayed in Figure 96.

Table 18 show hardware rpm mac counters Command Example Information

Slot ID #	Port number on the party-bus control switch.
RX Frames	Number of packets received by the party-bus switch from the processor in the specified slot.
TX Frames	Number of packets sent by the party-bus switch to the processor in the specified slot.

show hardware rpm rp1/rp2

Display advanced debugging information for the RPM processors.

Syntax **show hardware rpm** *slot-number* {**rp1** | **rp2**} {**data-plane | party-bus**} {**counters | statistics**}

Parameters

slot-number	Enter the RPM slot number 0 or 1.
rp1 | **rp2**	Enter either the keyword **rp1** or **rp2** to designate which route processor debug information to display.
data-plane	(OPTIONAL) Enter the keywords **data-plane** to display control processor information on the dataplane of the specified RPM.
party-bus	(OPTIONAL) Enter the keywords **party-bus** to display control processor information on the party-bus of the specified RPM.
counters	(OPTIONAL) Enter the keyword **counters** to display the standard Ethernet counters.
statistics	(OPTIONAL) Enter the keyword **statistics** to display driver-related counters

Defaults No default values or behavior

Command Modes EXEC

EXEC privilege

Usage Information If the "dropped cell" field is non-zero, look for a pattern such as burstiness when the counters increment. It is normal to see a small number of continuous cell drops. Burstiness may indicate congestion on the internal switch at a particular point in time.

Command History

Version 6.5.4.0	Introduced

show interfaces link-status

Displays 10-Gigabit Ethernet link fault signaling and port status information.

Syntax **show interfaces tenGigabitEthernet** *slot/port* **link-status**

Parameters

tenGigabitEthernet	Enter the keyword **tenGigabitEthernet** followed by the slot/port information.

Command Modes EXEC

EXEC privilege

Command History

Version 6.5.4.0	Introduced

Example 1

```
Force10#show interfaces tengigabitethernet 4/0 link-status
Port Status
    Loss of Signal             : FALSE (XFP has power)
    RX Signal Lock Error       : TRUE (Lock detected)
PCS Link State                 : Down
Link Faults
    Remote                     : None (No Fault)
    Local                      : Fault (Fault present)
    Idle Error                 : False (Not received)
    Illegal Symbol             : False (Not received)
    Error Symbol               : False (Not received)
Force10#
```

Figure 97 show interfaces tengigabitethernet Command Example

Table 19 defines the information displayed in Figure 97.

Table 19 Lines in show interfaces tengigabitethernet Command Example

Line	Description
Loss of Signal	Indicates if the interface has detected the required number of digital bit transitions (from 1 to 0 and 0 to 1) on the incoming signal. A 10 GE link must detect a certain number of such transitions for proper synchronization.
Rx Signal Lock Error	Indicates a loss of timing condition. The receive clock must be recovered from the incoming data stream to allow the receiving physical layer to synchronize with the incoming electrical pulses.
PCS Link State	Display the state of the PCS (Physical Coding sub-layer). The state is either up or down.
Link Fault Remote.	Indicates if the remote device has detected a fault, is inhibiting transmission of frames, and may be continuously transmitting idle messages.
Link Fault Local.	Indicates if a local fault is detected that may inhibit transmission of frames, and may be continuously transmitting remote fault signals.
Link Fault Idle Error	Indicates the detections of a non-idle symbol during an idle period.
Link Fault Illegal Symbol	Indicates the detections of an illegal symbol, other than an error symbol, while receiving data frames.
Link Fault Error Symbol.	Indicates the detections of an error symbol while receiving data frames.

show interfaces phy

Displays auto-negotiation and link partner information.

Syntax **show interfaces gigabitethernet** *slot/port* **phy**

Parameters

gigabitethernet	Enter the keyword **gigabitethernet** followed by the slot/port information.

Command Modes EXEC

EXEC privilege

Command History

Version 6.5.4.0	Introduced

Example

```
Force10#show int gigabitethernet 1/0 phy
Mode Control:
   SpeedSelection:              10b
   AutoNeg:                     ON
   Loopback:                    False
   PowerDown:                   False
   Isolate:                     False
   DuplexMode:                  Full
Mode Status:
   AutoNegComplete:             False
   RemoteFault:                 False
   LinkStatus:                  False
   JabberDetect:                False
AutoNegotation Advertise:
   100MegFullDplx:              True
   100MegHalfDplx:              True
   10MegFullDplx:               False
   10MegHalfDplx:               True
   Asym Pause:                  False
   Sym  Pause:                  False
AutoNegotiation Remote Partner's Ability:
   100MegFullDplx:              False
   100MegHalfDplx:              False
   10MegFullDplx:               False
   10MegHalfDplx:               False
   Asym Pause:                  False
   Sym  Pause:                  False
AutoNegotiation Expansion:
   ParallelDetectionFault:      False
...
```

Figure 98 show interfaces gigabitethernet phy Command Example (Partial)

Table 19 defines the information displayed in Figure 97.

Table 20 Lines in show interfaces gigabitethernet Command Example

Line	Description
Mode Control	Indicates if auto negotiation is enabled. If so, indicates the selected speed and duplex.
Mode Status	Displays auto negotiation fault information. When the interface completes auto negotiation successfully, the autoNegComplete field and the linkstatus field read “True.”
AutoNegotiation Advertise	Displays the control words advertised by the local interface during negotiation. Duplex is either half or full. Asym- and Sym Pause is the types of flow control supported by the local interface.

Table 20 Lines in show interfaces gigabitethernet Command Example

Line	Description
AutoNegotiation Remote Partner's Ability	Displays the control words advertised by the remote interface during negotiation. Duplex is either half or full. Asym- and Sym Pause is the types of flow control supported by the remote interface
AutoNegotiation Expansion	ParallelDetectionFault is the handshaking scheme in which the link partner continuously transmit an "idle" data packet using the Fast Ethernet MLT-3 waveform. Equipment that does not support auto-negotiation must be configured to exactly match the mode of operation as the link partner or else no link can be established.
1000Base-T Control	1000Base-T requires auto-negotiation. The IEEE Ethernet standard does not support setting a speed to 1000 Mbps with the speed command without auto-negotiation. E-Series line cards support both full-duplex and half-duplex 1000BaseT.
Phy Specific Control	Values are: 0 - Manual MDI 1 - Manual MDIX 2 - N/A 3 - Auto MDI/MDIX
Phy Specific Status	Displays PHY-specific status information. Cable length represents a rough estimate in meters: 0 - < 50 meters 1 - 50 - 80 meters 2 - 80 - 110 meters 3 - 110 - 140 meters 4 - 140 meters. Link Status: Up or Down Speed: Auto 1000MB 100MB 10MB

show interfaces transceiver

View the physical status and operational status of an installed transceiver. The output also displays the transceiver's serial number.

Syntax **show interfaces gigabitethernet** *slot/port* **transceiver**

Parameters

gigabitethernet	Enter the keyword **gigabitethernet** followed by the slot/port information.

Command Modes EXEC

EXEC privilege

Command History

Version 6.5.4.0	Introduced

Example

```
Force10#show interfaces gigabitethernet 1/0 transceiver
SFP is present.

SFP 0 Serial Base ID fields
SFP 0 Id                   = 0x03
SFP 0 Ext Id               = 0x04
SFP 0 Connector           = 0x07
SFP 0 Transciever Code     = 0x00 0x00 0x00 0x01 0x20 0x40 0x0c 0x05
SFP 0 Encoding            = 0x01
SFP 0 BR Nominal            = 0x15
SFP 0 Length(9um)    Km     = 0x00
SFP 0 Length(9um)    100m   = 0x00
SFP 0 Length(50um)   10m    = 0x1e
SFP 0 Length(62.5um) 10m    = 0x0f
SFP 0 Length(Copper) 10m    = 0x00
SFP 0 Vendor Name          = FINISAR CORP.
SFP 0 Vendor OUI            = 0x00 0x90 0x65
SFP 0 Vendor PN             = FTRJ8519P1BNL
SFP 0 Vendor Rev           = A
SFP 0 Laser Wavelength      = 850 nm
SFP 0 CheckCodeBase         = 0x66
SFP 0 Serial Extended ID fields
SFP 0 Options= 0x00 0x12
SFP 0 BR max= 0
SFP 0 BR min= 0
SFP 0 Vendor SN= P5N1ACE
SFP 0 Datecode             = 040528
SFP 0 CheckCodeExt        = 0x5b

Force10#
```

Figure 99 show interfaces gigabitethernet transceiver Command Example

show logging driverlog

View the driver log for the RPM CP processor or for the line card CPU in the specified slot.

Syntax **show logging driverlog** [**linecard** *number*]

Parameters

linecard *number*	(OPTIONAL) Enter the keyword **linecard** followed by the line card slot number to display the driver log for the specified line card. Range: 0 to 13 on a E1200, 0 to 6 on a E600/E600i, and 0 to 5 on an E300

Defaults No default values or behavior

Command Modes EXEC

EXEC privilege

Command History

Version 6.5.4.0	Introduced

Usage Information

This command displays internal software driver information which may be useful during troubleshooting line card initialization errors, such as downed port pipe.

Chapter 7 sFlow Commands

Platform Specific Feature: sFlow is supported on E-Series only.

FTOS sFlow monitoring system includes an sFlow Agent and an sFlow Collector. The sFlow Agent combines the flow samples and interface counters into sFlow datagrams and forwards them to the sFlow Collector. The sFlow Collector analyses the sFlow Datagrams received from the different devices and produces a network-wide view of traffic flows.

Important Points to Remember

- Force10 Networks recommends that the sFlow Collector be connected to the Force10 chassis through a line card port rather than the RPM Management Ethernet port.
- Community list and local preference fields are not filled up in extended gateway element in sFlow datagram.
- 802.1P source priority field is not filled up in extended switch element in sFlow datagram.
- Only Destination and Destination Peer AS number are packed in the dst-as-path field in extended gateway element
- If packet being sampled is redirected using PBR (Policy-Based Routing), sFlow datagram may contain incorrect extended gateway/router information.
- sFlow does not support packing extended information for IPv6 packets. Only the first 128 bytes of the IPv6 packet is shipped in the datagram.
- Source VLAN field in the extended switch element will not be packed in case of routed packet.
- Destination VLAN field in the extended switch element will not be packed in case of Multicast packet.
- The maximum number of packets that can be sampled and processed per second is:
  - — 7500 packets when no extended information packing is enabled
  - — 7500 packets when only extended-switch information packing is enabled (see sflow extended-switch enable on page 264)
  - — 1600 packets when extended-router and/or extended-gateway information packing is enabled (see sflow extended-router enable on page 263 and sflow extended-gateway enable on page 262)

The sFlow commands include:

- sflow collector on page 260
- sflow enable (Global) on page 261
- sflow enable (Interface) on page 262
- sflow extended-gateway enable on page 262
- sflow extended-router enable on page 263
- sflow extended-switch enable on page 264
- sflow polling-interval (Global) on page 265
- sflow polling-interval (Interface) on page 265
- sflow sample-rate (Global) on page 266
- sflow sample-rate (Interface) on page 267
- show sflow on page 267
- show sflow linecard on page 269

sflow collector

C-Series	No
E-Series	✓

Specify a collector(s) to which sFlow datagram are forwarded.

Syntax **sflow collector** *ip-address* **agent-addr** *ip-address* [*number* [**max-datagram-size** *number*]] | [**max-datagram-size** *number*]

To delete the specified collector(s), use the **no sflow collector** *ip-address* **agent-addr** *ip-address* [*number* [**max-datagram-size** *number*]] | [**max-datagram-size** *number*] command

Parameters

ip-address	Enter the ip address of the collector in dotted decimal format.
agent-addr *ip-address*	Enter the keyword **agent-addr** followed by the sFlow agent IP address in dotted decimal format.
number	(OPTIONAL) Enter the udp port number (User Datagram Protocol). Range: 0 to 65535 Default: 6343
max-datagram-size *number*	(OPTIONAL) Enter the keyword **max-datagram-size** followed by the size number in bytes. Range: 400 to 1500 Default: 1400

Defaults Not configured

Command Modes CONFIGURATION

Command History

Version 6.5.1.0	Expanded the no form of the command to mirror the syntax used to configure
Version 6.2.1.1	Introduced

Usage Information Users can specify up to 2 sFlow collectors. If 2 collectors are specified, the samples will be sent to both.

As part of the sFlow-MIB, if the SNMP request originates from a configured collector, FTOS will return the corresponding configured agent IP in MIB requests. FTOS checks to ensure that two entries are not configured for the same collector IP with a different agent IP. Should that happen, FTOS generates the following error:

%Error: Different agent-addr attempted for an existing collector

sflow enable (Global)

C-Series	**No**
E-Series	✓

Enable sFlow globally.

Syntax **sflow enable**

To disable sFlow, use the **no sflow enable** command.

Defaults sFlow is disabled by default

Command Modes CONFIGURATION

Command History

Version 6.2.1.1	Introduced

Usage Information sFlow is disabled by default. In addition to this command, sFlow needs to be enable on individual interfaces where sFlow sampling is desired.

Related Commands

sflow enable (Interface)	Enable sFlow on Interfaces.

sflow enable (Interface)

C-Series	No
E-Series	✓

Enable sFlow on Interfaces.

Syntax **sflow enable**

To disable sFlow, use the **no sflow enable** command.

Defaults sFlow is disabled by default on all interfaces

Command Modes INTERFACE

Command History

Version 6.2.1.1	Introduced

Usage Information When sFlow is enable on an interface, flow sampling is done on any traffic going out of the interface.

Note: Once a physical port is a member of a LAG, it will inherit the sFlow configuration from the LAG port.

Related Commands

sflow enable (Global)	Turn sFlow on globally

sflow extended-gateway enable

C-Series	No
E-Series	✓

Enable packing information on an extended gateway.

Syntax **sflow extended-gateway** [**extended-router**] [**extended-switch**] **enable**

To disable packing information, use the **no sflow extended-gateway** [**extended-router**] [**extended-switch**] **enable** command.

Parameters

extended-router	Enter the keyword **extended-router** to collect extended router information.
extended-switch	Enter the keyword **extended-switch** to collect extended switch information.
enable	Enter the keyword **enable** to enable global extended information.

Defaults Disabled

Command Modes CONFIGURATION

Command History

Version 7.4.1.0	Introduced

Usage Information The **show sflow** command displays the configured global extended information.

Example

```
Force10#show sflow
sFlow services are enabled
Global default sampling rate: 64
Global default counter polling interval: 1000
Global extended information enabled: gateway, router, switch
1 collectors configured
Collector IP addr: 20.20.20.2, Agent IP addr: 10.11.201.7, UDP port: 6343
1732336 UDP packets exported
0 UDP packets dropped
12510225 sFlow samples collected
0 sFlow samples dropped due to sub-sampling
Force10#
```

Related Commands

show sflow	Display the sFlow configuration

sflow extended-router enable

C-Series	**No**
E-Series	✓

Enable packing information on a router and switch.

Syntax **sflow extended-router** [**extended-switch**] **enable**

To disable packing information, use the **no sflow extended-router** [**extended-switch**] **enable** command.

Parameters

extended-switch	Enter the keyword **extended-switch** to collect extended switch information.
enable	Enter the keyword **enable** to enable global extended information.

Defaults Disabled

Command Modes CONFIGURATION

Command History

Version 7.4.1.0	Introduced

Related Commands

sflow extended-gateway enable	Enable packing information on an extended gateway
sflow extended-switch enable	Enable packing information on a switch.
show sflow	Display the sFlow configuration

sflow extended-switch enable

C-Series	**No**
E-Series	✓

Enable packing information on a switch only.

Syntax **sflow extended-switch enable**

To disable packing information, use the **no sflow extended-switch** [**enable**] command.

Parameters

enable	Enter the keyword **enable** to enable global extended information.

Defaults Disabled

Command Modes CONFIGURATION

Command History

Version 7.4.1.0	Introduced

Related Commands

sflow extended-gateway enable	Enable packing information on an extended gateway.
sflow extended-router enable	Enable packing information on a router.
show sflow	Display the sFlow configuration

sflow polling-interval (Global)

C-Series	No
E-Series	✓

Syntax **sflow polling-interval** *interval value*

To return to the default, use the **no sflow polling-interval** *interval* command.

Parameters

interval value	Enter the interval value in seconds. Range: 15 to 86400 seconds Default: 20 seconds

Defaults 20 seconds

Command Modes CONFIGURATION

Command History

Version 6.2.1.1	Introduced

Usage Information The polling interval for an interface is the maximum number of seconds between successive samples of counters to be sent to the collector. This command changes the global default counter polling (20 seconds) interval. You can configure an interface to use a different polling interval.

Related Commands

sflow polling-interval (Interface)	Set the polling interval for an interface

sflow polling-interval (Interface)

C-Series	No
E-Series	✓

Syntax **sflow polling-interval** *interval value*

To return to the default, use the **no sflow polling-interval** *interval* command.

Parameters

interval value	Enter the interval value in seconds. Range: 15 to 86400 seconds Default: The global counter polling interval

Defaults The same value as the current global default counter polling interval

Command Modes INTERFACE

Command History

Version 6.2.1.1	Introduced

Usage Information

This command sets the counter polling interval for an interface.

Related Commands

sflow polling-interval (Global)	Globally set the polling interval

sflow sample-rate (Global)

C-Series	**No**
E-Series	✓

Change the global default sampling rate.

Syntax **sflow sample-rate** *value*

To return to the default sampling rate, enter the **no sflow sample-rate**.

Parameters

value	Enter the sampling rate value. Range: 2 to 8388608 (in powers of 2 only, for example 4096, 8192, 16384 etc.) Default: 32768

Defaults 32768

Command Modes CONFIGURATION

Command History

Version 6.2.1.1	Introduced

Usage Information

Sample-rate is the average number of packets skipped before the sample is taken. This command changes the global default sampling rate. You can configure an interface to use a different sampling rate than the global sampling rate. If the value entered is not a correct power of 2, the command generates an error message with the previous and next power of 2 value. Select one of these two number and re-enter the command.

Related Commands

sflow sample-rate (Interface)	Change the Interface sampling rate.

sflow sample-rate (Interface)

C-Series	No
E-Series	✓

Change the Interface default sampling rate.

Syntax **sflow sample-rate** *value*

To return to the default sampling rate, enter the **no sflow sample-rate**.

Parameters

value	Enter the sampling rate value. Range: 2 to 8388608 (in powers of 2 only, for example 4096, 8192, 16384 etc.) Default: The Global default sampling

Defaults The Global default sampling

Command Modes CONFIGURATION

Command History

Version 6.2.1.1	Introduced

Usage Information This command changes the sampling rate for an Interface. By default, the sampling rate of an interface is set to the same value as the current global default sampling rate. If the value entered is not a correct power of 2, the command generates an error message with the previous and next power-of-2 value. Select one of these two number and re-enter the command.

Related Commands

sflow sample-rate (Global)	Change the sampling rate globally.

show sflow

C-Series	No
E-Series	✓

Display the current sFlow configuration

Syntax **show sflow** [*interface*]

interface	(OPTIONAL) Enter the following keywords and slot/port or number information: • For an 100/1000 Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For a Loopback interface, enter the keyword **loopback** followed by a number from 0 to 16383. • For a SONET interface, enter the keyword **sonet** followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information.

Command Modes EXEC

Command History

Version 6.2.1.1	Introduced

Example

```
Force10#show sflow
sFlow services are enabled
Global default sampling rate: 32768
Global default counter polling interval: 20
1 collectors configured
Collector IP addr: 133.33.33.53, Agent IP addr: 133.33.33.116, UDP port: 6343
77 UDP packets exported
0 UDP packets dropped
165 sFlow samples collected
69 sFlow samples dropped due to sub-sampling

Linecard 1 Port set 0 H/W sampling rate 8192
  Gi 1/16: configured rate 8192, actual rate 8192, sub-sampling rate 1
  Gi 1/17: configured rate 16384, actual rate 16384, sub-sampling rate 2

Linecard 3 Port set 1 H/W sampling rate 16384
  Gi 3/40: configured rate 16384, actual rate 16384, sub-sampling rate 1
Force10#
```

Figure 100 show sflow Command Example

show sflow linecard

C-Series	No
E-Series	✓

Display the sFlow information on a line card.

Syntax **show sflow linecard** {*slot number*}

Parameters

slot number	(OPTIONAL) Enter a slot number to view information on the line card in that slot. Range: 0 to 13 on a E1200, 0 to 6 on a E600/E600i, and 0 to 5 on a E300.

Command Modes EXEC

Command History

Version 6.2.1.1	Introduced

Example

```
Force10#show sflow linecard 1
Linecard 1
  Samples rcvd from h/w            :165
  Samples dropped for sub-sampling :69
  Total UDP packets exported       :77
  UDP packets exported via RPM     :77
  UDP packets dropped              :
Force10#
```

Figure 101 show sflow linecard Command Example

Chapter 8 CAM Profiling

Platform Specific Feature: CAM Profiling is supported on E-Series only.

FTOS supports both CAM Profiling and CAM IPv4 Flow commands. This chapter includes the following sections:

- CAM Profiling Commands on page 271
- CAM IPv4flow Commands on page 294

CAM Profiling Commands

CAM Profiling features allow you to partition the CAM entries to optimize your application. For example:

- When deployed as a switch, more Layer 2 FIB entries can be configured
- When deployed as a router, more Layer 3 FIB entries can be configured
- When IPv6 is not employed, additional CAM space can be allocated for ACL

Warning: The CAM Profiling features are for users that do not want to use the default CAM Profile. If you are using these features for the first time, contact Force10 TAC (Technical Assistance Center) for assistance:

E-mail Direct Support: support@Force10networks.com
Web: www.force10networks.com/support/
Telephone support:
US and Canada customers: 866-965-5800
International customers: 408-965-5800

Important Points to Remember

- CAM Profiling is a E-Series TeraScale only feature.
- CAM Profiling commands are similar to Boot commands; you must save your new CAM Profile configuration (copy running-config startup-config duplicate) and then reboot your chassis to apply the new CAM Profile.
- When budgeting your CAM allocations for ACLs and QoS configurations, remember to take into account that TCP and UDP rules with port range options may require more than one CAM entry (see deny tcp, deny udp, permit tcp, and permit udp).
- Your chassis, RPMs, and all online line cards must have the same CAM Profile.
- CAM Profiling includes Configuration and EXEC level commands. Contact Force10 TAC before you use the EXEC level commands.

The commands for CAM Profiling are:

- cam-profile default microcode on page 273
- cam-profile default microcode chassis on page 275
- cam-profile default microcode linecard on page 275
- cam-profile eg-default on page 276
- cam-profile eg-default microcode default on page 277
- cam-profile ipv4-320k on page 278
- cam-profile ipv4-320k microcode (Configuration) on page 278
- cam-profile ipv4-320k microcode (EXE) on page 280
- cam-profile ipv4-egacl-16k microcode on page 281
- cam-profile ipv4-egacl-16k microcode chassis on page 282
- cam-profile ipv4-egacl-16k microcode linecard on page 283
- cam-profile l2-ipv4-inacl microcode on page 283
- cam-profile unified-default microcode on page 284
- show cam-profile on page 285
- show cam-profile default microcode on page 287
- show cam-profile eg-default microcode on page 288
- show cam-profile ipv4-320k microcode on page 288
- show cam-profile ipv4-egacl-16k microcode on page 289
- show cam-usage on page 290

cam-profile default microcode

C-Series	No
E-Series	✓

Set the default CAM Profile and the required microcode.

Syntax **cam-profile default microcode** [**default** | **lag-hash-mpls** | **lag-hash-align**]

Parameters

default	Enter the keyword **default** to designate the default microcode. **Note**: This is the microcode that comes with the TeraScale chassis by default.
lag-hash-mpls	(OPTIONAL) Enter the keyword **lag-hash-mpls** to designate the lag-hash-mpls microcode.
lag-hash-align	(OPTIONAL) Enter the keyword **lag-hash-align** to designate the lag-hash-align microcode.

Defaults cam-profile default microcode default

Command Modes CONFIGURATION

Command History

Version 7.4.1.0	Hashing based on MPLS header behavior added
Version 6.3.1.0	Introduced

Usage Information The default CAM Profile contains the following CAM partitions:

Profile Name	DEFAULT
L2FIB	32K entries
L2ACL	1K entries
IPv4FIB	256K entries
IPv4ACL	12K entries
IPv4Flow	24K entries
EgL2ACL	1K entries
EgIPv4ACL	1K entries
Reserved	8K entries
IPv6FIB	0 entries
IPv6ACL	0 entries
IPv6Flow	0 entries
EgIPv6ACL	0 entries

A microcode allows you to provide a slightly different behavior for features. Save the running configuration by executing the **copy running config** command. This will write the CAM profile to the NVRAM of the primary and secondary RPM and EEPROM of all the online line cards. The change will take effect only after the next boot.

lag-hash-mpls

With the **default** microcode, MPLS packets are distributed over a LAG based on MAC SA and DA. With the **lag-hash-mpls** microcode loaded, MPLS packets are distributed across the LAG based on IP SA, DA and IP protocol. This is applicable for MPLS packets with 5 labels or less than 5 labels deep (FTOS can look 5 labels deep into MPLS packets). When the IP header is not available after the 5th label, hashing for default load-blance is based on MPLS labels. For more than 5 label MPLS packets, hashing is always based on MAC SA and DA.

lag-hash-align

If you require LAG hashing so that both directions of a bidirectional flow (for example, VoIP call or P2P file sharing) are mapped to the same output link in the LAG bundle, then use the **lag-hash-align** microcode.

Related Commands

copy running config	Save the running configuration

cam-profile default microcode chassis

C-Series	No
E-Series	✓

Set the default CAM Profile and the required microcode for the chassis.

Syntax **cam-profile default microcode** [**default** | **lag-hash-mpls** | **lag-hash-align**] **chassis**

Parameters

default	Enter the keyword **default** to designate the default microcode. **Note**: This is the microcode that comes with the TeraScale chassis by default.
lag-hash-mpls	(OPTIONAL) Enter the keyword **lag-hash-mpls** to designate the lag-hash-mpls microcode.
lag-hash-align	(OPTIONAL) Enter the keyword **lag-hash-align** to designate the lag-hash-align microcode.
chassis	Enter the keyword **chassis** to update chassis-wide including CP and all online line cards.

Defaults cam-profile default microcode default

Command Modes EXEC

Command History

Version 6.3.1.0	Introduced

Usage Information This is a chassis-wide command. Setting the CAM profile with this command will set the CAM profile for the chassis and all online line cards. The change will take effect only after the next boot

Note: This is a troubleshooting command; Force10 strongly recommends using this command only for troubleshooting purposes.

Related Commands

cam-profile default microcode linecard	Designate the microcode for a specific line card.

cam-profile default microcode linecard

C-Series	No
E-Series	✓

Set the default CAM Profile and the required microcode.

Syntax **cam-profile default microcode** [**default** | **lag-hash-mpls** | **lag-hash-align**] **linecard** *number*

Parameters

default	Enter the keyword **default** to designate the default microcode. **Note**: This is the microcode that comes with the TeraScale chassis by default.
lag-hash-mpls	(OPTIONAL) Enter the keyword **lag-hash-mpls** to designate the lag-hash-mpls microcode.
lag-hash-align	(OPTIONAL) Enter the keyword **lag-hash-align** to designate the lag-hash-align microcode.
linecard *number*	Enter the keyword **linecard** followed by the line card slot number. Range: 0 to 13 on a E1200, 0 to 6 on a E600, and 0 to 5 on a E300.

Defaults cam-profile default microcode default

Command Modes EXEC

Command History

Version 6.3.1.0	Introduced

Usage Information This is a line card specific command. The change will take effect only after the next boot.

Note: This is a troubleshooting command; Force10 strongly recommend using this command only for troubleshooting purposes.

Related Commands

cam-profile default microcode chassis	Set the default CAM Profile to the specified microcode chassis-wide.

cam-profile eg-default

C-Series	No
E-Series	✓

Enable the CAM profile to the eg-default microcode (for EG-Series line cards only).

Syntax **cam-profile eg-default microcode default**

Parameters

microcode	Enter the keyword **microcode** to enable the eg-default microcode
default	Enter the keyword **default** to enable the default CAM profile.

Defaults cam-profile default microcode default

Command Modes CONFIGURATION

Command History

Version 6.5.1.0	Introduced

Related Commands

show cam-profile eg-default microcode	Display the eg-default CAM profile

cam-profile eg-default microcode default

C-Series	No
E-Series	✓

Set the CAM to the eg-default CAM microcode profile for EG-Series line cards only.

Syntax **cam-profile eg-default microcode default** [**chassis** | **linecard** *number*]

Parameters

default	Enter the keyword **default** to enable the default CAM profile.
chassis	Enter the keyword **chassis** to update the chassis including CP and all online line cards with the new CAM profile.
linecard *number*	Enter the keyword **linecard** followed by the line card slot number. Range: 0 to 13 on a E1200, 0 to 6 on a E600/E600i, and 0 to 5 on a E300.

Defaults No default behavior or values

Command Modes EXEC

Command History

Version 6.5.1.0	Introduced

Usage Information The **chassis** option is a chassis-wide command. Setting the CAM profile using the **chassis** option will set the CAM profile for the chassis and all online line cards. The change will take effect only after the next boot.

The **linecard** *number* option is a line card specific command. The change will take effect only after the next boot.

Related Commands

show cam-profile eg-default microcode	Display the eg-default CAM profile

cam-profile ipv4-320k

C-Series	No
E-Series	✓

Enable the CAM to the IPv4-320K CAM microcode profile.

Syntax **cam-profile ipv4-320k microcode ipv4-320k**

Parameters

microcode	Enter the keyword **microcode** to change the microcode profile.
ipv4-320k	Enter the keyword **ipv4-320k** to enable the 320K microcode.

Defaults cam-profile default microcode default

Command Modes CONFIGURATION

Command History

Version 6.5.1.0	Introduced

Usage Information The IPv4-320K CAM profile increases the size of the Layer 3 FIB to 320K (from 256K) for the default CAM profile. It also reduces the IPv4 Flow CAM size from 24K to 12K.

Note: Once the CAM profile is changed to IPv4-320K and is saved to NVRAM, no subsequent changes to the CAM profile can be made before reloading the chassis (any changes will lead to unexpected behavior). Once the chassis has reloaded the IPv4-320K CAM profile, then changes can be made to the IPv4 Flow CAM size.

Related Commands

show cam-profile ipv4-320k microcode	Display the IPv4-e320k CAM profile settings.

cam-profile ipv4-320k microcode (Configuration)

C-Series	No
E-Series	✓

Configure the CAM to the IPv4-320K CAM microcode profile.

Syntax **cam-profile ipv4-320k microcode** {**default** | **lag-hash** }

Parameters

default	Enter the keyword **default** to designate the default microcode. **Note**: This is the microcode that comes with the TeraScale chassis by default.
lag-hash-mpls	Enter the keyword **lag-hash-mpls** to designate the lag-hash-mpls microcode.

Defaults

cam-profile default microcode default

Command Modes

CONFIGURATION

Command History

Version 7.4.2.0	Introduced

Usage Information

The IPv4-320K CAM profile increases the size of the Layer 3 FIB to 320K (from 256K) for the default CAM profile. It also reduces the IPv4 Flow CAM size from 24K to 12K.

lag-hash-mpls

With the **default** microcode, MPLS packets are distributed over a LAG based on MAC SA and DA. With the **lag-hash-mpls** microcode loaded, MPLS packets are distributed across the LAG based on IP SA, DA and IP protocol. This is applicable for MPLS packets with 5 labels or less than 5 labels deep (FTOS can look 5 labels deep into MPLS packets). When the IP header is not available after the 5th label, hashing for default load-blance is based on MPLS labels. For more than 5 label MPLS packets, hashing is always based on MAC SA and DA.

The **lag-hash-mpls** microcode contains the following CAM partitions. The CAM partitions containing value changes, from the default microcode, are shown in bold type

Profile Name	IPv4-320K
L2FIB	32K entries
L2ACL	1K entries
IPv4FIB	**320K entries**
IPv4ACL	12K entries
IPv4Flow	**12K entries**
EgL2ACL	1K entries
EgIPv4ACL	1K entries
Reserved	**4K entries**
IPv6FIB	0 entries
IPv6ACL	0 entries
IPv6Flow	0 entries
EgIPv6ACL	0 entries
MicroCode Name	**LAG-Hash-MPLS**

Related Commands

show cam-profile ipv4-320k microcode	Display the IPv4-320k CAM profile settings.

cam-profile ipv4-320k microcode (EXE)

C-Series	No
E-Series	✓

Set the CAM to the IPv4-320K CAM microcode profile.

Syntax

cam-profile ipv4-320k microcode ipv4-320k [**chassis** | **linecard** *number*]

Parameters

ipv4-320k	Enter the keyword **ipv4-320k** to enable the 320K microcode.
chassis	Enter the keyword **chassis** to update chassis-wide including CP and all online line cards.
linecard *number*	Enter the keyword **linecard** followed by the line card slot number. Range: 0 to 13 on a E1200, 0 to 6 on a E600/E600i, and 0 to 5 on a E300.

Defaults

cam-profile default microcode default

Command Modes

EXEC

Command History

Version 6.5.1.0	Introduced

Usage Information

The IPv4-320K CAM profile increases the size of the Layer 3 FIB to 320K (from 256K) for the default CAM profile. It also reduces the IPv4 Flow CAM size from 24K to 12K.

Note: Once the CAM profile is changed to IPv4-320K and is saved to NVRAM, no subsequent changes to the CAM profile can be made before reloading the chassis (any changes will lead to unexpected behavior). Once the chassis has reloaded the IPv4-320K CAM profile, then changes can be made to the IPv4 Flow CAM size.

The **chassis** option is a chassis-wide command. Setting the CAM profile using the **chassis** option will set the CAM profile for the chassis and all online line cards. The change will take effect only after the next boot.

The **linecard** *number* option is a line card specific command. The change will take effect only after the next boot.

Related Commands

show cam-profile ipv4-320k microcode	Display the IPv4-e320k CAM profile settings.

cam-profile ipv4-egacl-16k microcode

C-Series	No
E-Series	✓

Set the IPv4-egacl-16K CAM Profile with the ACL group microcode.

Syntax **cam-profile ipv4-egacl-16k microcode** {**acl-group**}

Parameters

acl-group	Enter the keyword **acl-group** to designate the acl-group microcode.

Defaults cam-profile default microcode default

Command Modes CONFIGURATION

Command History

Version 6.3.1.0	Introduced

Usage Information The **acl-group** microcode is for users that want to use the VLAN ACL Group feature which permits group VLANs for the IP egress ACL.

Save the running configuration by executing the **copy running config** command. This will write the CAM profile to the NVRAM of the primary and secondary RPM and EEPROM of all the online line cards. The change will take effect only after the next boot.

Note: Do not use this CAM Profile for Layer 2 egress ACLs.

The IPv4-egacl-16 CAM Profile contains the following CAM partitions. The CAM partitions containing value changes, from the default microcode, are shown in bold type

Profile Name	IPv4-egACL-16k
L2FIB	32K entries
L2ACL	**7K entries**
IPv4FIB	**192K entries**
IPv4ACL	**8K entries**
IPv4Flow	24K entries
EgL2ACL	**0 entries**
EgIPv4ACL	**16K entries**
Reserved	8K entries
IPv6FIB	0 entries
IPv6ACL	0 entries
IPv6Flow	0 entries
EgIPv6ACL	0 entries

Related Commands		
	copy running config	Save the running configuration

cam-profile ipv4-egacl-16k microcode chassis

C-Series	No
E-Series	✓

Set the IPv4-egacl-16K CAM Profile and to the ACL group microcode chassis-wide.

Syntax **cam-profile ipv4-egacl-16k microcode** {**acl-group**} **chassis**

Parameters		
	acl-group	Enter the keyword **acl-group** to designate the acl-group microcode.
	chassis	Enter the keyword **chassis** to update chassis-wide including CP and all online line cards.

Defaults cam-profile default microcode default

Command Modes EXEC

Command History		
	Version 6.3.1.0	Introduced

Usage Information

The **acl-group** microcode is for users that want to use the VLAN ACL Group feature which permits group VLANs for the IP egress ACL.

This is a chassis-wide command. Setting the IPv4-egacl-16k CAM profile with this command will set the CAM profile for the chassis and all online line cards. The change will take effect only after the next boot.

Note: This is a troubleshooting command; Force10 strongly recommend using this command only for troubleshooting purposes.

Related Commands		
	cam-profile ipv4-egacl-16k microcode linecard	Set the IPv4-egacl-16K CAM Profile for a specific line card.

cam-profile ipv4-egacl-16k microcode linecard

C-Series	No
E-Series	✓

Set the IPv4-egacl-16K CAM Profile and the ACL group microcode to a specific line card.

Syntax **cam-profile ipv4-egacl-16k microcode** {**acl-group**}**linecard** *number*

Parameters

acl-group	Enter the keyword **acl-group** to designate the acl-group microcode.
linecard *number*	Enter the keyword **linecard** followed by the line card slot number. Range: 0 to 13 on a E1200, 0 to 6 on a E600, and 0 to 5 on a E300.

Defaults cam-profile default microcode default

Command Modes EXEC

Command History

Version 6.3.1.0	Introduced

Usage Information This is a line card specific command. The change will take effect only after the next boot

Note: This is a troubleshooting command; Force10 strongly recommend using this command only for troubleshooting purposes.

Related Commands

cam-profile ipv4-egacl-16k microcode chassis	Set the IPv4-egacl-16K CAM Profile with the ACL group microcode chassis-wide.

cam-profile l2-ipv4-inacl microcode

C-Series	No
E-Series	✓

Enable CAM profile with 32K Layer 2 and 28K IPv4 ingress ACL

Syntax **cam-profile ipv4-320k microcode** {**default** }

Parameters

default	Enter the keyword **default** to designate the default microcode. **Note**: This is the microcode that comes with the TeraScale chassis by default.

Defaults cam-profile default microcode default

Command Modes CONFIGURATION

Command History

Version 7.4.2.0	Introduced

Usage Information The L2-IPv4-inACL contains the partitions listed below. The CAM partitions containing value changes, from the default microcode, are shown in bold type.

Profile Name	l2-ipv4-inacl
L2FIB	32K entries
L2ACL	**32K entries**
IPv4FIB	**64K entries**
IPv4ACL	**27K entries**
IPv4Flow	**8K entries**
EgL2ACL	**2K entries**
EgIPv4ACL	**2K entries**
Reserved	**2K entries**
IPv6FIB	0K entries
IPv6ACL	0K entries
IPv6Flow	0K entries
EgIPv6ACL	0K entries
MicroCode Name	Default

cam-profile unified-default microcode

C-Series	No
E-Series	✓

Enable default unified CAM profile.

Syntax **cam-profile unified-default microcode ipv6-extacl**

Parameters

ipv6-extacl	Enter the keyword **ipv6-extacl** to enable microcode with IPv6 extended ACL.

Defaults cam-profile default microcode defaul

Command Modes CONFIGURATION

Command History

Version 7.4.2.0	Introduced

Usage Information

The unified CAM profile uses the IPv6-ExtACL microcode. This microcode maintains the CAM allocations for IPv6 and IPv4 FIB, while allocating more CAM space for L2ACL, EgL2ACL, and IPv4ACL regions.

The IPv6-ExtACL contains the following partitions. The CAM partitions containing value changes, from the default microcode, are shown in bold type.

Profile Name	Unified
L2FIB	32K entries
L2ACL	**2K entries**
IPv4FIB	**192K entries**
IPv4ACL	**9K entries**
IPv4Flow	**8K entries**
EgL2ACL	**2K entries**
EgIPv4ACL	**2K entries**
Reserved	**2K entries**
IPv6FIB	**6K entries**
IPv6ACL	**2K entries**
IPv6Flow	**4K entries**
EgIPv6ACL	**2K entries**
MicroCode Name	IPv6-ExtACL

show cam-profile

C-Series	No
E-Series	✓

Display the CAM profile and the microcode name currently configured for the chassis and all the online line cards.

Syntax **show cam-profile** [**summary**]

Parameters

summary	(OPTIONAL) Enter the keyword **summary** to view a summary listing.

Defaults No default behavior or values

Command Modes EXEC

Command History

Version 6.3.1.0	Introduced

Usage Information

If the CAM profile has been changed, this command displays the current CAM profile setting in one column and in the other column displays the CAM profile and the microcode name that will be configured for the chassis and all online line cards *after the next boot*.

Example 1

```
Force10#show cam-profile summary

-- Chassis CAM Profile --
                 : Current Settings : Next Boot
Profile Name     : Default          : Default
MicroCode Name   : Default          : Default

                 : Current Settings : Next Boot
-- Line card 1 --
Profile Name     : Default          : Default
MicroCode Name   : Default          : Default

                 : Current Settings : Next Boot
-- Line card 6 --
Profile Name     : Default          : Default
MicroCode Name   : Default          : Default
Force10#
```

Figure 102 show cam-profile summary command

Example 2

```
Force10#show cam-profile

-- Chassis Cam Profile --

CamSize          : 18-Meg
                 : Current Settings : Next Boot
Profile Name     : DEFAULT          : DEFAULT
L2FIB            : 32K entries      : 32K entries
L2ACL            : 1K entries       : 1K entries
IPv4FIB          : 256K entries     : 256K entries
IPv4ACL          : 12K entries      : 12K entries
IPv4Flow         : 24K entries      : 24K entries
EgL2ACL          : 1K entries       : 1K entries
EgIPv4ACL        : 1K entries       : 1K entries
Reserved         : 8K entries       : 8K entries
IPv6FIB          : 0  entries       : 0  entries
IPv6ACL          : 0  entries       : 0  entries
IPv6Flow         : 0  entries       : 0  entries
EgIPv6ACL        : 0  entries       : 0  entries
MicroCode Name   : Default          : Default

-- Line card 0 --
CamSize          : 18-Meg
                 : Current Settings : Next Boot
Profile Name     : DEFAULT          : DEFAULT
L2FIB            : 32K entries      : 32K entries
L2ACL            : 1K entries       : 1K entries
IPv4FIB          : 256K entries     : 256K entries
IPv4ACL          : 12K entries      : 12K entries
IPv4Flow         : 24K entries      : 24K entries
EgL2ACL          : 1K entries       : 1K entries
EgIPv4ACL        : 1K entries       : 1K entries
Reserved         : 8K entries       : 8K entries
IPv6FIB          : 0  entries       : 0  entries
IPv6ACL          : 0  entries       : 0  entries
IPv6Flow         : 0  entries       : 0  entries
EgIPv6ACL        : 0  entries       : 0  entries
MicroCode Name   : Default          : Default
Force10#
```

Figure 103 show cam-profile command

show cam-profile default microcode

C-Series	No
E-Series	✓

Display the default CAM Profile partition settings and the selected microcode name.

Syntax **show cam-profile default microcode** [**default** | **lag-hash-mpls** | **lag-hash-align**]

Parameters

default	Enter the keyword **default** to designate the default microcode. **Note**: This is the microcode that comes with the TeraScale chassis by default.
lag-hash-mpls	(OPTIONAL) Enter the keyword **lag-hash-mpls** to designate the lag-hash-mpls microcode.
lag-hash-align	(OPTIONAL) Enter the keyword **lag-hash-align** to designate the lag-hash-align microcode.

Defaults No default behavior or value

Command Modes EXEC

Command History

Version 6.3.1.0	Introduced

Example

```
Force10#show cam-profile default microcode default

---  Sample Configuration of CAM Profile  ---

CamSize           : 18-Meg
                  : Settings
Profile Name      : DEFAULT
L2FIB             : 32K entries
L2ACL             : 1K entries
IPv4FIB           : 256K entries
IPv4ACL           : 12K entries
IPv4Flow          : 24K entries
EgL2ACL           : 1K entries
EgIPv4ACL         : 1K entries
Reserved          : 8K entries
IPv6FIB           : 0  entries
IPv6ACL           : 0  entries
IPv6Flow          : 0  entries
EgIPv6ACL         : 0  entries
MicroCode Name    : Default
Force10#
```

Figure 104 show cam-profile default microcode command

Usage Information This command allows you to view the default CAM allocation before you designate another microcode.

Note: This command is intended as a Help command allowing you to view a sample CAM allocation prior to designating a CAM profile or microcode.

show cam-profile eg-default microcode

C-Series	No
E-Series	✓

Display the eg-default CAM profile.

Syntax **show cam-profile eg-default microcode default**

Parameters

default	Enter the keyword **default** to display the default microcode

Defaults No default behavior or values

Command Modes EXEC

Command History

Version 6.5.1.0	Introduced

Example

```
Force10#show cam-profile eg-default microcode default

CamSize           : 36-Meg
                  : Settings
Profile Name      : EG_Default
L2FIB             : 32K entries
L2ACL             : 1K entries
IPv4FIB           : 512K entries
IPv4ACL           : 13K entries
IPv4Flow          : 24K entries
EgL2ACL           : 1K entries
EgIPv4ACL         : 1K entries
Reserved          : 8K entries
IPv6FIB           : 32K entries
IPv6ACL           : 6K entries
IPv6Flow          : 8K entries
EgIPv6ACL         : 2K entries
MicroCode Name    : Default
```

Usage Information This CAM profile is used for EG-Series line cards only.

Related Commands

cam-profile eg-default microcode default	Set the CAM to the eg-default CAM microcode profile.

show cam-profile ipv4-320k microcode

C-Series	No
E-Series	✓

Display the IPv4-320k CAM profile settings.

Syntax **show cam-profile ipv4-320k microcode ipv4-320k**

Parameters		
	ipv4-320k	Enter **ipv4-320k** to enable the default 320K CAM microcode.

Defaults No default behavior or values

Command Modes EXEC

Command History		
	Version 6.5.1.0	Introduced

Example

```
Force10#show cam-profile ipv4-320k microcode ipv4-320k

CamSize           : 18-Meg
                  : Settings
Profile Name      : IPv4-320K
L2FIB             : 32K entries
L2ACL             : 1K entries
IPv4FIB           : 320K entries
IPv4ACL           : 13K entries
IPv4Flow          : 12K entries
EgL2ACL           : 1K entries
EgIPv4ACL         : 1K entries
Reserved          : 4K entries
IPv6FIB           : 0  entries
IPv6ACL           : 0  entries
IPv6Flow          : 0  entries
EgIPv6ACL         : 0  entries
MicroCode Name    : Default

Force10#
```

Related Commands		
	cam-profile ipv4-320k microcode (EXE)	Set the CAM to the IPv4-320K CAM microcode profile.

show cam-profile ipv4-egacl-16k microcode

C-Series	No
E-Series	✔

Display the IPv4-egacl-16k CAM profile partition settings with the ACL group microcode.

Syntax **show cam-profile ipv4-egacl-16k microcode** {**acl-group**}

Parameters		
	acl-group	Enter the keyword **acl-group** to designate the acl-group microcode.

Defaults No default behavior or values

Command Modes EXEC

Command History

Version 6.3.1.0	Introduced

This command allows you to view the IPv4-egacl-16k CAM allocation with the ACL group microcode before executing any new configuration.

Note: This command is intended as a Help command that allows you to view a sample CAM allocation prior to designating a CAM profile or microcode.

show cam-usage

C-Series	No
E-Series	✓

Display the CAM usage on the ACL, router, or switch.

Syntax

show cam-usage [**acl**] [**router**] [**switch**]

Parameters

acl	Enter the keyword **acl** to display the Layer 2 and Layer 3 ACL CAM usage of the following: • Layer 2 Partition details: Ingress ACL Egress ACL • Layer 3 Partition details: Ingress ACL Egress ACL

router	Enter the keyword **router** to display the Layer 3 CAM usage of the following. • Layer 3 Partition details: Ingress ACL L3 Flow System Flow Trace List Multicast FIB QOS PBR L3 FIB Egress ACL
switch	Enter the keyword **switch** to display the Layer 2 CAM usage of the following. • Layer 2 Partition details: Ingress ACL L2 FIB Egress ACL

Defaults No default behavior or values

Command Modes EXEC

Command History

Version 6.5.1.0	Introduced

Example

```
Force10#show cam-usage

Linecard|Portpipe| CAM Partition   | Total CAM   |  Used CAM   |Available CAM
========|========|=================|=============|=============|==============
   11   |   0    | IN-L2 ACL       |      7152   |          0  |      7152
        |        | IN-L2 FIB       |     32768   |       1081  |     31687
        |        | IN-L3 ACL       |      8192   |          3  |      8189
        |        | IN-L3 FIB       |    196607   |          1  |    196606
        |        | IN-L3-SysFlow   |      2878   |          0  |      2878
        |        | IN-L3-TrcList   |      1024   |          0  |      1024
        |        | IN-L3-McastFib  |      9215   |          0  |      9215
        |        | IN-L3-Qos       |      8192   |          0  |      8192
        |        | IN-L3-PBR       |      1024   |          0  |      1024
        |        | OUT-L2 ACL      |         0   |          0  |         0
        |        | OUT-L3 ACL      |     16384   |          0  |     16384
   11   |   1    | IN-L2 ACL       |      7152   |          0  |      7152
        |        | IN-L2 FIB       |     32768   |       1081  |     31687
        |        | IN-L3 ACL       |      8192   |          3  |      8189
        |        | IN-L3 FIB       |    196607   |          1  |    196606
        |        | IN-L3-SysFlow   |      2878   |          0  |      2878
        |        | IN-L3-TrcList   |      1024   |          0  |      1024
        |        | IN-L3-McastFib  |      9215   |          0  |      9215
        |        | IN-L3-Qos       |      8192   |          0  |      8192
        |        | IN-L3-PBR       |      1024   |          0  |      1024
        |        | OUT-L2 ACL      |         0   |          0  |         0
        |        | OUT-L3 ACL      |     16384   |          0  |     16384

Force10#
```

Figure 105 show cam-usage Command

Example

```
Force10#show cam-usage acl

Linecard|Portpipe| CAM Partition   | Total CAM   |  Used CAM   |Available CAM
========|========|=================|=============|=============|==============
   11   |   0    | IN-L2 ACL       |      1008   |          0  |      1008
        |        | IN-L3 ACL       |     12288   |          2  |     12286
        |        | OUT-L2 ACL      |      1024   |          2  |      1022
        |        | OUT-L3 ACL      |      1024   |          0  |      1024

Force10#
```

Figure 106 show cam-usage acl Command

Example

```
Force10#show cam-usage router

Linecard|Portpipe| CAM Partition   | Total CAM   |  Used CAM   |Available CAM
========|========|=================|=============|=============|==============
   11   |   0    | IN-L3 ACL       |      8192   |          3  |      8189
        |        | IN-L3 FIB       |    196607   |          1  |    196606
        |        | IN-L3-SysFlow   |      2878   |          0  |      2878
        |        | IN-L3-TrcList   |      1024   |          0  |      1024
        |        | IN-L3-McastFib  |      9215   |          0  |      9215
        |        | IN-L3-Qos       |      8192   |          0  |      8192
        |        | IN-L3-PBR       |      1024   |          0  |      1024
        |        | OUT-L3 ACL      |     16384   |          0  |     16384
   11   |   1    | IN-L3 ACL       |      8192   |          3  |      8189
        |        | IN-L3 FIB       |    196607   |          1  |    196606
        |        | IN-L3-SysFlow   |      2878   |          0  |      2878
        |        | IN-L3-TrcList   |      1024   |          0  |      1024
        |        | IN-L3-McastFib  |      9215   |          0  |      9215
        |        | IN-L3-Qos       |      8192   |          0  |      8192
        |        | IN-L3-PBR       |      1024   |          0  |      1024
        |        | OUT-L3 ACL      |     16384   |          0  |     16384

Force10#
```

Figure 107 show cam-usage router Command

Example

```
Force10#show cam-usage switch

Linecard|Portpipe| CAM Partition   | Total CAM   |  Used CAM   |Available CAM
========|========|=================|=============|=============|==============
   11   |   0    | IN-L2 ACL       |      7152   |          0  |      7152
        |        | IN-L2 FIB       |     32768   |       1081  |     31687
        |        | OUT-L2 ACL      |         0   |          0  |         0
   11   |   1    | IN-L2 ACL       |      7152   |          0  |      7152
        |        | IN-L2 FIB       |     32768   |       1081  |     31687
        |        | OUT-L2 ACL      |         0   |          0  |         0

Force10#
```

Figure 108 show cam-usage switch

Usage Information

This command provides a mechanism to display the utilization of the CAM for various partitions of each port pipe.

CAM IPv4flow Commands

The 18 megabit user configurable CAM is divided into multiple regions such as Layer 2 FIB, Layer 3 FIB, IPv4Flow, IPv4 Ingress ACL, etc. Within these regions, the IPv4Flow region is further sub-divided into 5 regions:

- System Flow
- QOS
- PBR
- Trace-lists
- Multicast FIB & ACL

Each of these sub-regions, in the IPv4Flow, is allocated certain default memory space in the CAM during chassis bootup. To change the default allocation of CAM space within IPv4Flow, use the **cam-ipv4flow** command. There are two commands to change the IPv4Flow: **cam-ipv4flow** command in CONFIGURATION mode and **cam ipv4flow** command in EXEC mode. The EXEC mode command is used primarily to change the IPv4flow settings on line cards and RPMs which are frequently moved from one chassis to another running different FTOS versions and different IPv4Flow settings.

Warning: The CAM IPv4flow feature is for users that do not want to use the default CAM IPv4flow. If you are using these features for the first time, contact Force10 TAC (Technical Assistance Center) for assistance:

E-mail Direct Support: support@Force10networks.com
Web: www.force10networks.com/support/
Telephone support:
US and Canada customers: 866-965-5800
International customers: 408-965-5800

Important Points to Remember

- CAM IPv4Flow commands are available on both EtherScale and TeraScale chassis. When used on an EtherScale platform, these commands set the CAM spaces for the IPv4Flow sub-regions as well as the IPv4 ACL region.
- CAM IPv4Flow commands under CONFIGURATION mode is similar to Boot commands; you must save your new IPv4Flow settings (copy running config) and reboot your chassis to apply the new IPv4Flow settings.
- Your Chassis, RPMs and all online line cards must have the same CAM IPv4Flow settings.
- CAM IPv4Flow commands include CONFIGURATION and EXEC level commands. Contact Force10 TAC before you use the EXEC level commands.

The commands to change and view the CAM IPv4flow are:

- cam-ipv4flow (EtherScale) on page 295
- cam-ipv4flow (TeraScale) on page 296
- cam ipv4flow chassis all (EtherScale) on page 297
- cam ipv4flow chassis all (TeraScale) on page 299
- cam ipv4flow linecard (EtherScale) on page 300
- cam ipv4flow linecard (TeraScale) on page 302
- show cam-ipv4flow on page 303

cam-ipv4flow (EtherScale)

C-Series	No
E-Series	✓

Configure the CAM IPv4flow entries.

Syntax **cam-ipv4flow** [**default** {**acl** *value*} {**multicast-fib** *value*} {**pbr** *value***}** {**qos** *value*} {**system-flow** *value*} {**trace-list** *value*}]

Parameters

default	Enter the keyword **default** to reset the IPV4 Flow entries to their default setting.
acl *value*	Enter the keyword **acl** followed by the value for the Access Control List entries. Range: 1 to 32 KB Default: 8 KB
multicast-fib *value*	Enter the keyword **multicast-fib** followed by the value for the multicast fib entries. Range: 1 to 32 KB Default: 9 KB
pbr *value*	Enter the keyword **pbr** followed by the value for the PBR entires. Range: 1 to 32 KB Default: 1 KB
qos *value*	Enter the keyword **qos** followed by the value for the Quality of Service entries. Range: 1 to 32 KB Default: 8 KB

system-flow *value*	Enter the keyword **system-flow** followed by the value for the system flow entries. Range: 4 to 32 KB Default: 5 KB
trace-list *value*	Enter the keyword **trace-list** followed by the value for the trace list entries. Range: 1 to 32 KB Default: 1 KB

Defaults As above

Command Modes CONFIGURATION

Command History

Version 6.3.1.0	Introduced

Usage Information This is a chassis-wide command. Setting the CAM IPv4Flow with this command will set the CAM IPv4Flow for the chassis and all online line cards. Save the running configuration by executing the **copy running config** command. This will write the CAM IPv4Flow to the NVRAM of the primary and secondary RPM and EEPROM of all the online line cards. The change will take effect only after the next boot.

Related Commands

show cam-ipv4flow	Display the CAM IPv4flow entries.

cam-ipv4flow (TeraScale)

C-Series	No
E-Series	✓

Configure the CAM IPv4flow entries.

Syntax **cam-ipv4flow** [**default** {**multicast-fib** *value*} {**pbr** *value*} {**qos** *value*} {**system-flow** *value*} {**trace-list** *value*}]

Parameters

default	Enter the keyword **default** to reset the IPV4 Flow entries to their default setting.
multicast-fib *value*	Enter the keyword **multicast-fib** followed by the value for the multicast fib entries. Range: 1 to 32 KB Default: 9 KB

pbr *value*	Enter the keyword **pbr** followed by the value for the PBR entires. Range: 1 to 32 KB Default: 1 KB
qos *value*	Enter the keyword **qos** followed by the value for the Quality of Service entries. Range: 1 to 32 KB Default: 8 KB
system-flow *value*	Enter the keyword **system-flow** followed by the value for the system flow entries. Range: 4 to 32 KB Default: 5 KB
trace-list *value*	Enter the keyword **trace-list** followed by the value for the trace list entries. Range: 1 to 32 KB Default: 1 KB

Defaults As above

Command Modes CONFIGURATION

Command History

Version 6.3.1.0	Introduced

Usage Information This is a chassis-wide command. Setting the CAM IPv4Flow with this command will set the CAM IPv4Flow for the chassis and all online line cards. Save the running configuration by executing the **copy running config** command. This will write the CAM IPv4Flow to the NVRAM of the primary and secondary RPM and EEPROM of all the online line cards. The change will take effect only after the next boot.

Related Commands

show cam-ipv4flow	Display the CAM IPv4flow entries.

cam ipv4flow chassis all (EtherScale)

C-Series	No
E-Series	✓

Configure IPV4 Flow entries on an EtherScale chassis and all line cards in the chassis.

Syntax **cam ipv4flow chassis all** {**default**} | {**acl** *value*} {**multicast-fib** *value*} {**pbr** *value*} {**qos** *value*} {**system-flow** *value*} {**trace-list** *value*}

Parameters

default	Enter the keyword **default** to reset the IPV4 Flow entries to their default setting.
acl *value*	Enter the keyword **acl** followed by the value for the Access Control List entries. Range: 1 to 32 KB Default: 8 KB
multicast-fib *value*	Enter the keyword **multicast-fib** followed by the value for the multicast fib entries. Range: 1 to 32 KB Default: 9 KB
pbr *value*	Enter the keyword **pbr** followed by the value for the PBR entires. Range: 1 to 32 KB Default: 1 KB
qos *value*	Enter the keyword **qos** followed by the value for the Quality of Service entries. Range: 1 to 32 KB Default: 8 KB
system-flow *value*	Enter the keyword **system-flow** followed by the value for the system flow entries. Range: 4 to 32 KB Default: 5 KB
trace-list *value*	Enter the keyword **trace-list** followed by the value for the trace list entries. Range: 1 to 32 KB Default: 1 KB

Defaults

As above

Command Modes

EXEC

Command History

Version 6.3.1.0	Introduced

Usage Information

Execute this command to configure the chassis IPV4 Flow setting *before* configuring the IPV4 Flow setting on a line card—cam ipv4flow linecard (EtherScale) command. Note that the total of the entries configured must be 32K.The change will take effect only after the next boot.

Related Commands

cam ipv4flow linecard (EtherScale)	Configure the IPV4 Flow on an EtherScale line card.
show cam-ipv4flow	Display the IPV4 Flow entries.

cam ipv4flow chassis all (TeraScale)

C-Series	No
E-Series	✓

Configure IPV4 Flow entries on a TeraScale chassis and all line cards in the chassis.

Syntax

cam ipv4flow chassis all {**default**} | {**multicast-fib** *value*} {**pbr** *value*} {**qos** *value*} {**system-flow** *value*} {**trace-list** *value*}

Parameters

default	Enter the keyword **default** to reset the IPV4 Flow entries to their default setting.
multicast-fib *value*	Enter the keyword **multicast-fib** followed by the value for the multicast fib entries. Range: 1 to 32 KB Default: 9 KB
pbr *value*	Enter the keyword **pbr** followed by the value for the PBR entires. Range: 1 to 32 KB Default: 1 KB
qos *value*	Enter the keyword **qos** followed by the value for the Quality of Service entries. Range: 1 to 32 KB Default: 8 KB
system-flow *value*	Enter the keyword **system-flow** followed by the value for the system flow entries. Range: 4 to 32 KB Default: 5 KB
trace-list *value*	Enter the keyword **trace-list** followed by the value for the trace list entries. Range: 1 to 32 KB Default: 1 KB

Defaults

As above

Command Modes

EXEC

Command History

Version 6.3.1.0	Introduced

Example

```
Force10#cam ipv4flow chassis all multicast-fib 9 ?
pbr                    Set pbr entries
Force10#cam ipv4flow chassis all multicast-fib 9 pbr ?
<1-32>                 Number of cam entries multiple of 1K
Force10#cam ipv4flow chassis all multicast-fib 1 pbr ?
<1-32>                 Number of cam entries multiple of 1K
Force10#cam ipv4flow chassis all multicast-fib 9 pbr 1 ?
qos                    Set qos entries
Force10#cam ipv4flow chassis all multicast-fib 1 pbr 1 qos ?
<1-32>                 Number of cam entries multiple of 1K
Force10#cam ipv4flow chassis all multicast-fib 9 pbr 1 qos 8 ?
system-flow            Set system flow entries
Force10#cam ipv4flow chassis all multicast-fib 9 pbr 1 qos 8 system-flow ?
<4-32>                 Number of cam entries multiple of 1K
Force10#cam ipv4flow chassis all multicast-fib 9 pbr 1 qos 8 system-flow 5
trace-list             Set trace list entries
Force10#cam ipv4flow chassis all multicast-fib 9 pbr 1 qos 8 system-flow 5 trace-list ?
<1-32>                 Number of cam entries multiple of 1K
Force10#cam ipv4flow chassis all multicast-fib 9 pbr 1 qos 8 system-flow 5 trace-list 1
<cr>
Force10#
```

Usage Information

Execute this command to configure the chassis IPV4 Flow setting *before* configuring the IPV4 Flow setting on a line card—cam ipv4flow linecard (TeraScale) command. Note that the total of the entries configured must be 24K. The change will take effect only after the next boot

Related Commands

cam ipv4flow linecard (TeraScale)	Configure the IPV4 Flow on a TeraScale line card.
show cam-ipv4flow	Display the IPV4 Flow entries.

cam ipv4flow linecard (EtherScale)

C-Series	**No**
E-Series	✓

Configure IPV4 Flow entries on a EtherScale line cards (ED, EE, and EE3 series).

Syntax

cam ipv4flow linecard *slot number* {**default**} | {**acl** *value*} {**multicast-fib** *value*} {**pbr** *value*} {**qos** *value*} {**system-flow** *value*} {**trace-list** *value*}

Parameters

slot number	Enter the line card slot ID number. Range: 0 to 13 on the E1200; 0 on 6 for E600, and 0 to 5 on the E300.
default	Enter the keyword **default** to reset the IPV4 Flow entries to their default setting.
acl *value*	Enter the keyword **acl** followed by the value for the Access Control List entries. Range: 1 to 32 KB Default: 8 KB

multicast-fib *value*	Enter the keyword **multicast-fib** followed by the value for the multicast fib entries. Range: 1 to 32 KB Default: 9 KB
pbr *value*	Enter the keyword **pbr** followed by the value for the PBR entires. Range: 1 to 32 KB Default: 1 KB
qos *value*	Enter the keyword **qos** followed by the value for the Quality of Service entries. Range: 1 to 32 KB Default: 8 KB
system-flow *value*	Enter the keyword **system-flow** followed by the value for the system flow entries. Range: 4 to 32 KB Default: 5 KB
trace-list *value*	Enter the keyword **trace-list** followed by the value for the trace list entries. Range: 1 to 32 KB Default: 1 KB
multicast-fib *value*	Enter the keyword **multicast-fib** followed by the value for the multicast fib entries. Range: 1 to 32 KB Default: 9 KB

Defaults

As above

Command Modes

EXEC

Command History

Version 6.3.1.0	Introduced

Usage Information

If the cam ipv4flow chassis all (EtherScale) command has been configured on the chassis, use this command to configure IPV4 Flow entries to newly added line cards or to correct a line card that has a mismatch IPV4 Flow entry. For more information on CAM Profiling and mismatch entries, refer to the *FTOS Configuration Guide*.

Note: The change will take effect only after the next boot.

Related Commands

cam ipv4flow chassis all (EtherScale)	Configure the IPV4 Flow entries chassis-wide.
show cam-ipv4flow	Display the IPV4 Flow entries.

cam ipv4flow linecard (TeraScale)

C-Series	No
E-Series	✓

Configure IPV4 Flow entries on a TeraScale line cards (EF and EF3 series).

Syntax

cam ipv4flow linecard *slot number* [**default** | {**multicast-fib** *value*} {**pbr** *value*} {**qos** *value*} {**system-flow** *value*} {**trace-list** *value*}]

Parameters

slot number	Enter the line card slot ID number. Range: 0 to 13 on the E1200; 0 on 6 for E600, and 0 to 5 on the E300.
default	Enter the keyword **default** to reset the IPV4 Flow entries to their default setting.
multicast-fib *value*	Enter the keyword **multicast-fib** followed by the value for the multicast fib entries. Range: 1 to 32 KB Default: 9 KB
pbr *value*	Enter the keyword **pbr** followed by the value for the PBR entires. Range: 1 to 32 KB Default: 1 KB
qos *value*	Enter the keyword **qos** followed by the value for the Quality of Service entries. Range: 1 to 32 KB Default: 8 KB
system-flow *value*	Enter the keyword **system-flow** followed by the value for the system flow entries. Range: 4 to 32 KB Default: 5 KB
trace-list *value*	Enter the keyword **trace-list** followed by the value for the trace list entries. Range: 1 to 32 KB Default: 1 KB

Defaults

As above

Command Modes

EXEC

Command History

Version 6.3.1.0	Introduced

Example

```
Force10#cam ipv4flow linecard ?
<0-5>                   Line card slot id
Force10#cam ipv4flow linecard 0 ?
default                 Reset ipv4flow cam entries to default setting
multicast-fib           Set multicast fib entries
Force10#cam ipv4flow linecard 0 multicast-fib ?
<1-32>                  Number of cam entries multiple of 1K
Force10#cam ipv4flow linecard 0 multicast-fib 9 ?
pbr                     Set pbr entries
Force10#cam ipv4flow linecard 0 multicast-fib 9 pbr 1 ?
qos                     Set qos entries
Force10#cam ipv4flow linecard 0 multicast-fib 9 pbr 1 qos ?
<1-32>                  Number of cam entries multiple of 1K
Force10#cam ipv4flow linecard 0 multicast-fib 9 pbr 1 qos 8 ?
system-flow             Set system flow entries
Force10#cam ipv4flow linecard 0 multicast-fib 9 pbr 1 qos 8 system-flow ?
<4-32>                  Number of cam entries multiple of 1K
Force10#cam ipv4flow linecard 0 multicast-fib 9 pbr 1 qos 8 system-flow 5 ?
trace-list              Set trace list entries
Force10#cam ipv4flow linecard 0 multicast-fib 9 pbr 1 qos 8 system-flow 5 trace-list ?
<1-32>                  Number of cam entries multiple of 1K
Force10#cam ipv4flow linecard 0 multicast-fib 9 pbr 1 qos 8 system-flow 5 trace-list 1 ?
<cr>
Force10#cam ipv4flow linecard 0 multicast-fib 9 pbr 1 qos 8 system-flow 5 trace-list 1

New linecard cam ipv4flow setting:
multicastFibAcl = 9K
pbr             = 1K
qos             = 8K
sysFlow         = 5K
traceList       = 1K

Nov 3 21:54:04: %RPM0-P:CP %CHMGR-3-IPV4FLOW_CHANGE: Changed linecard 0 CAM IPv4Flow
setting
Force10#
```

Usage Information

If the cam ipv4flow chassis all (TeraScale) command has been configured on the chassis, use this command to configure IPV4 Flow entries to newly added line cards or to correct a line card that has a mismatch IPV4 Flow entry. For more information on CAM Profiling and mismatch entries, refer to the *FTOS Configuration Guide*.

Note: The change will take effect only after the next boot.

Related Commands

cam ipv4flow chassis all (TeraScale)	Configure the IPV4 Flow entries chassis-wide.
show cam-ipv4flow	Display the IPV4 Flow entries.

show cam-ipv4flow

C-Series	**No**
E-Series	✓

Display the CAM IPv4 Flow entries. If the CAM IPv4 Flow entries have been changed, this command will display the current IPv4 Flow entries in one column and in the other column display the CAM IPv4 Flow entries that will be configured *after the next boot*.

Syntax **show cam-ipv4flow**

Command Modes EXEC

Command History

Version 6.3.1.0	Introduced

Example

```
Force10#show cam-ipv4flow

-- Chassis Cam Ipv4Flow --
                     Current Settings   Next Boot
Acl                :   8K                 5K
Multicast Fib/Acl  :   9K                12K
Pbr                :   1K                 1K
Qos                :   8K                 8K
System Flow        :   5K                 5K
Trace Lists        :   1K                 1K

-- Line card 2 --
                     Current Settings   Next Boot
Acl                :   5K                 0K
Multicast Fib/Acl  :   9K                12K
Pbr                :   1K                 1K
Qos                :   8K                 8K
System Flow        :   5K                 5K
Trace Lists        :   1K                 1K

-- Line card 8 --
                     Current Settings   Next Boot
Acl                :   5K                 0K
Multicast Fib/Acl  :   9K                12K
Pbr                :   1K                 1K
Qos                :   8K                 8K
System Flow        :   5K                 5K
Trace Lists        :   1K                 1K

-- Line card 13 --
                     Current Settings   Next Boot
Acl                :   5K                 0K
Multicast Fib/Acl  :   9K                12K
Pbr                :   1K                 1K
Qos                :   8K                 8K
System Flow        :   5K                 5K
Trace Lists        :   1K                 1K
Force10#
```

Figure 109 show cam-ipv4flow (EtherScale) Command

Example

```
Force10#show cam-ipv4flow

-- Chassis Cam Ipv4Flow --
                      Current Settings   Next Boot
Multicast Fib/Acl :  10K                 8K
Pbr               :   2K                 6K
Qos               :   6K                 4K
System Flow       :   5K                 5K
Trace Lists       :   1K                 1K

-- Line card 1 --
                      Current Settings   Next Boot
Multicast Fib/Acl :  10K                 8K
Pbr               :   2K                 6K
Qos               :   6K                 4K
System Flow       :   5K                 5K
Trace Lists       :   1K                 1K

-- Line card 10 --
                      Current Settings   Next Boot
Multicast Fib/Acl :  10K                 8K
Pbr               :   2K                 6K
Qos               :   6K                 4K
System Flow       :   5K                 5K
Trace Lists       :   1K                 1K

-- Line card 13 --
                      Current Settings   Next Boot
Multicast Fib/Acl :  10K                 8K
Pbr               :   2K                 6K
Qos               :   6K                 4K
System Flow       :   5K                 5K
Trace Lists       :   1K                 1K

Force10#
```

Figure 110 show cam-ipv4flow (TeraScale) Command

Related Commands

cam ipv4flow linecard (EtherScale)	Configure the IPV4 Flow entries on EtherScale line cards
cam ipv4flow linecard (TeraScale)	Configure the IPV4 Flow entries on TeraScale line cards
cam ipv4flow chassis all (EtherScale)	Configure the IPV4 Flow entries on EtherScale chassis
cam ipv4flow chassis all (TeraScale)	Configure the IPV4 Flow entries on TeraScale chassis

Chapter 9 ACL VLAN Group

C-Series	NO
E-Series	✓

Platform Specific Feature: ACL VLAN Group is supported on E-Series only.

Since VLAN ACLs exist as multiple ACLs in the CAM, the size of the ACLs can be limited in the CAM. The ACL VLAN Group feature permits you to group VLANs and apply ACLs to the group so that ACLs exist as a single ACL in the CAM.

Note: This feature can only be used with the ipv4-egacl-16k CAM Profile with the acl-group microcode. See Chapter 8, “CAM Profiling.

The ACL VLAN Group commands are:

- acl-vlan-group on page 307
- description on page 308
- ip access-group on page 309
- member vlan on page 309
- show acl-vlan-group on page 310
- show config on page 311
- show running config acl-vlan-group on page 312

acl-vlan-group

C-Series	No
E-Series	✓

Create an ACL VLAN group

Syntax **acl-vlan-group** {*group name*}

Parameters

group name	Specify the name of the ACL VLAN group (maximum 16 characters).

Defaults No default behavior or values

Command Modes CONFIGURATION

Command History

Version 6.3.1.0	Introduced

Usage Information At a maximum, you can have 8 different ACL VLAN groups at any given time.

Related Commands

show acl-vlan-group	Display the ACL VLAN groups

description

C-Series	**No**
E-Series	✓

Add a description to the ACL VLAN group.

Syntax **description** {*description*}

To remove the description from the ACL VLAN group, use the **no description** {*description*} command.

Parameters

description	Enter a description to identify the ACL VLAN group (80 characters maximum).

Defaults No default behavior or values

Command Modes CONFIGURATION (conf-acl-vl-grp)

Command History

Version 6.3.1.0	Introduced

Related Commands

show acl-vlan-group	Display the ACL VLAN groups

ip access-group

C-Series	No
E-Series	✓

Apply an egress IP ACL to the ACL VLAN group.

Syntax **ip access-group** {*group name*} **out implicit-permit**

To remove the egress IP ACLs from the ACL VLAN group, use the **no ip access-group** {*group name*} **out** command.

Parameters

group name	Enter the name of the ACL VLAN group where you want the egress IP ACLs applied.

Defaults No default behavior or values

Command Modes CONFIGURATION (conf-acl-vl-grp)

Command History

Version 6.3.1.0	Introduced

Usage Information **Note:** Only an egress IP ACL can be applied on an ACL VLAN group.

Related Commands

acl-vlan-group	Create an ACL VLAN Group and name

member vlan

C-Series	No
E-Series	✓

Add VLAN member(s) to an ACL VLAN group.

Syntax **member vlan** {*VLAN-range*}

To remove a VLAN member from a ACL VLAN group, use the **no member vlan** {*VLAN-range*} command.

Parameters

VLAN-range	Enter the comma separated VLAN ID set. For example, 1-10,400-410,500

Defaults No default behavior or values

Command Modes CONFIGURATION (conf-acl-vl-grp)

Command History

Version 6.3.1.0	Introduced

Usage Information At a maximum, there can be only 32 VLAN members in all ACL VLAN groups. A VLAN can belong to only one group at any given time.

Related Commands

show acl-vlan-group	Display the ACL VLAN Groups

show acl-vlan-group

C-Series	**No**
E-Series	✓

Display all the ACL VLAN Groups or display a specific ACL VLAN Group by name.

Syntax **show acl-vlan-group** {*group name*}

Parameters

group name	(Optional) Display only the ACL VLAN Group that is specified.

Defaults No default behavior or values

Command Modes EXEC

Command History

Version 6.3.1.0	Introduced

Example

```
Force10#show acl-vlan-group

Group Name        Egress IP Acl     Vlan Members
group1                 acl1         1-10,400-410,500
group2                 acl2         20
Force10#
```

Figure 111 show acl-vlan-group command example

Example

```
Force10#show acl-vlan-group group1

Group Name       Egress IP Acl      Vlan Members
group1                acl1          1-10,400-410,500

Force10#
```

Figure 112 show acl-vlan-group group1 command example

show config

C-Series	**No**
E-Series	✓

Display the current configuration of the ACL VLAN Group.

Syntax **show config**

Defaults No default behavior or values

Command Modes EXEC

Command History

Version 6.3.1.0	Introduced

Example

```
Force10(conf-acl-vl-grp)#show config
!
acl-vlan-group group1
 description Acl Vlan Group1
 member vlan 1-10,400-410,500
 ip access-group acl1 out implicit-permit
Force10#
```

Figure 113 show config command example

show running config acl-vlan-group

C-Series	No
E-Series	✓

Display the running configuration of all or a given ACL VLAN Group.

Syntax **show running config acl-vlan-group** {*group name*}

Parameters

group name	(Optional) Display only the ACL VLAN Group that is specified.

Defaults No default behavior or values

Command Modes EXEC

Command History

Version 6.3.1.0	Introduced

Example

```
Force10#show running-config acl-vlan-group
!
acl-vlan-group group1
 description Acl Vlan Group1
 member vlan 1-10,400-410,500
 ip access-group acl1 out implicit-permit
!
acl-vlan-group group2
 member vlan 20
 ip access-group acl2 out
Force10#

Force10#show running-config acl-vlan-group group1
!
acl-vlan-group group1
 description Acl Vlan Group1
 member vlan 1-10,400-410,500
 ip access-group acl1 out implicit-permit

Force10#
```

Figure 114 show running-config acl-vlan-group command example

Chapter 10 LLDP

Platform Specific Feature: LLDP is supported on E-Series only.

Link Layer Detection Protocol (LLDP) advertises connectivity and management from the local station to the adjacent stations on an IEEE 802 LAN. LLDP facilitates multi-vendor interoperability by using standard management tools to discover and make available physical topology for Network Management. FTOS implementation of LLDP is based on IEEE standard 801.1ab.

The information distributed by LLDP is stored, by its recipients, in a standard MIB (Management Information Base). The information can be accessed by a Network Management System via a management protocol such as SNMP.

The LLDP commands are:

- advertise dot1-tlv on page 314
- advertise dot3-tlv on page 314
- advertise management on page 315
- clear lldp counters on page 315
- clear lldp neighbors on page 316
- debug lldp interface on page 316
- disable on page 317
- hello on page 318
- mode on page 318
- multiplier on page 319
- protocol lldp (Configuration) on page 319
- protocol lldp (Interface) on page 320
- show lldp neighbors on page 320
- show lldp statistics on page 321
- show running-config lldp on page 322

advertise dot1-tlv

C-Series	No
E-Series	✓

Advertise dot1 TLVs (Type, Length, Value).

Syntax **advertise dot1-tlv** {**port-protocol-vlan-id** | **port-vlan-id**}

To remove advertised dot1-tlv, use the **no advertise dot1-tlv** {**port-protocol-vlan-id** | **port-vlan-id**} command.

Parameters

port-protocol-vlan-id	(OPTIONAL) Enter the keywords **port-protocol-vlan-id** to advertise the port protocol VLAN identification TLV.
port-vlan-id	(OPTIONAL) Enter the keywords **port-vlan-id** to advertise the port VLAN identification TLV.

Defaults Disabled

Command Modes CONFIGURATION (conf-lldp) and INTERFACE (conf-if-*interface*-lldp)

Command History

Version 7.4.1.0	Introduced

advertise dot3-tlv

C-Series	No
E-Series	✓

Advertise dot3 TLVs (Type, Length, Value).

Syntax **advertise dot3-tlv** {**max-frame-size**}

To remove advertised dot3-tlv, use the **no advertise dot3-tlv** {**max-frame-size** } command.

Parameters

max-frame-size	Enter the keyword **max-frame-size** to advertise the dot3 maximum frame size.

Defaults No default values or behavior

Command Modes CONFIGURATION (conf-lldp) and INTERFACE (conf-if-*interface*-lldp)

Command History

Version 7.4.1.0	Introduced

advertise management

C-Series	No
E-Series	✓

Advertise management TLVs (Type, Length, Value).

Syntax **advertise management -tlv** {**system-capabilities** | **system-description**}

To remove advertised management TLVs, use the **no advertise management -tlv** {**system-capabilities** | **system-description**} command.

Parameters

system-capabilities	(OPTIONAL) Enter the keyword **system-capabilities** to advertise the system capabilities TLVs.
system-description	(OPTIONAL) Enter the keyword **system-description** to advertise the system description TLVs.

Defaults No default values or behavior

Command Modes CONFIGURATION (conf-lldp)

Command History

Version 7.4.1.0	Introduced

clear lldp counters

C-Series	No
E-Series	✓

Clear LLDP transmitting and receiving counters for all physical interfaces or a specific physical interface.

Syntax **clear lldp counters** {*interface*}

Parameters

interface	Enter the following keywords and slot/port or number information: • For a Fast Ethernet interface, enter the keyword **FastEthernet** followed by the slot/port information. • For a 1-Gigabit Ethernet interface, enter the keyword **gigabitEthernet** followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **tenGigabitEthernet** followed by the slot/port information.

Defaults No default values or behavior

Command Modes EXEC privilege

Command History

Version 7.4.1.0	Introduced

clear lldp neighbors

C-Series	No
E-Series	✓

Clear LLDP neighbor information for all interfaces or a specific interfaces.

Syntax **clear lldp neighbors** {*interface*}

Parameters

interface	Enter the following keywords and slot/port or number information: • For a Fast Ethernet interface, enter the keyword **FastEthernet** followed by the slot/port information. • For a 1-Gigabit Ethernet interface, enter the keyword **gigabitEthernet** followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **tenGigabitEthernet** followed by the slot/port information.

Defaults No default values or behavior

Command Modes EXEC privilege

Command History

Version 7.4.1.0	Introduced

debug lldp interface

C-Series	No
E-Series	✓

Enable LLDP debugging to display timer events, neighbor additions or deletions, and other information about incoming and outgoing packets.

Syntax **debug lldp interface** {*interface* | **all** }{**events**} {**packet** {**brief** | **detail**} {**tx** | **rx** | **both**}}

To disable debugging, use the **no debug lldp interface** {*interface* | **all** }{**events**} {**packet** {**brief** | **detail**} {**tx** | **rx** | **both**}} command.

Parameters

interface	Enter the following keywords and slot/port or number information: • For a Fast Ethernet interface, enter the keyword **FastEthernet** followed by the slot/port information. • For a 1-Gigabit Ethernet interface, enter the keyword **gigabitEthernet** followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **tenGigabitEthernet** followed by the slot/port information.
all	(OPTIONAL) Enter the keyword **all** to display information on all interfaces.
events	(OPTIONAL) Enter the keyword **events** to display major events such as timer events.
packet	(OPTIONAL) Enter the keyword **packet** to display information regarding packets coming in or going out.
brief	(OPTIONAL) Enter the keyword **brief** to display brief packet information.
detail	(OPTIONAL) Enter the keyword **detail** to display detailed packet information.
tx	(OPTIONAL) Enter the keyword **tx** to display transmit only packet information.
rx	(OPTIONAL) Enter the keyword **rx** to display receive only packet information
both	(OPTIONAL) Enter the keyword **both** to display both receive and transmit packet information.

Defaults No default values or behavior

Command Modes EXEC privilege

Command History

Version 7.4.1.0	Introduced

disable

C-Series	No
E-Series	✓

Enable or disable LLDP.

Syntax **disable**

To enable LLDP, use the **no disable**

Defaults Enabled, that is **no disable**

Command Modes CONFIGURATION (conf-lldp) and INTERFACE (conf-if-*interface*-lldp)

Command History

Version 7.4.1.0	Introduced

hello

C-Series	No
E-Series	✓

Configure the rate at which the LLDP control packets are sent to its peer.

Syntax **hello** {*seconds*}

To revert to the default, use the **no hello** {*seconds*} command.

Parameters

seconds	Enter the rate, in seconds, at which the control packets are sent to its peer. Rate: 5 - 180 seconds Default: 30 seconds

Defaults 30 seconds

Command Modes CONFIGURATION (conf-lldp) and INTERFACE (conf-if-*interface*-lldp)

Command History

Version 7.4.1.0	Introduced

mode

C-Series	No
E-Series	✓

Set the LLDP to receive or transmit.

Syntax **mode** {**tx** | **rx**}

To return to the default, use the **no mode** {**tx** | **rx**} command.

Parameters

tx	Enter the keyword **tx** to set the mode to transmit.
rx	Enter the keyword **rx** to set the mode to receive.

Defaults Both transmit and receive

Command Modes CONFIGURATION (conf-lldp) and INTERFACE (conf-if-*interface*-lldp)

Command History

Version 7.4.1.0	Introduced

multiplier

C-Series	No
E-Series	✓

Set the number of consecutive misses before LLDP declares the interface dead.

Syntax **multiplier** {*integer*}

To return to the default, use the **no multiplier** {*integer*} command.

Parameters

integer	Enter the number of consecutive misses before the LLDP declares the interface dead. Range: 2 - 10

Defaults 4 x hello

Command Modes CONFIGURATION (conf-lldp) and INTERFACE (conf-if-*interface*-lldp)

Command History

Version 7.4.1.0	Introduced

protocol lldp (Configuration)

C-Series	No
E-Series	✓

Enable LLDP globally on the E-Series chassis.

Syntax **protocol lldp**

To disable LLDP globally on the chassis, use the **no protocol lldp** command.

Defaults Disabled

Command Modes CONFIGURATION (conf-lldp)

Command History

Version 7.4.1.0	Introduced

protocol lldp (Interface)

C-Series	No
E-Series	✓

Enter the LLDP protocol in the INTERFACE mode.

Syntax **protocol lldp**

To return to the global LLDP configuration mode, use the **no protocol lldp** command from the Interface mode.

Defaults Disabled, that is LLDP is not enabled on the interface

Command Modes INTERFACE (conf-if-*interface*-lldp)

Command History

Version 7.4.1.0	Introduced

Usage Information When you enter the LLDP protocol in the Interface context, it overrides all global configurations. When you execute the **no protocol lldp** from the INTERFACE mode, interfaces will begin to inherit configuration from the global LLDP CONFIGURATION mode.

show lldp neighbors

C-Series	No
E-Series	✓

Display LLDP neighbor information for all interfaces or a specified interface.

Syntax **show lldp neighbors** [*interface*] [**detail**]

Parameters

interface	(OPTIONAL) Enter the following keywords and slot/port or number information: • For a Fast Ethernet interface, enter the keyword **FastEthernet** followed by the slot/port information. • For a 1-Gigabit Ethernet interface, enter the keyword **gigabitEthernet** followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **tenGigabitEthernet** followed by the slot/port information.
detail	(OPTIONAL) Enter the keyword **detail** to display all the TLV information, timers, and LLDP tx and rx counters.

Defaults No default values or behavior

Command Modes EXEC privilege

Command History

Version 7.4.1.0	Introduced

Example

```
Force10# show lldp neighbors
Local Intf      Rem PortId      Rem ChassisID
Gi 0/1          Gi 3/1          Extreme-1
Gi 0/1          Gi 3/2          Hp-ProCurve
Gi 0/2          Gi 4/1          00:08:23:12:99:01
Force10#
```

Usage Information Omitting the keyword **detail** displays only the remote chassis ID, Port ID, and Dead Interval.

show lldp statistics

C-Series	**No**
E-Series	✓

View the LLDP statistical information.

Syntax **show lldp statistics**

Defaults No default values or behavior

Command Modes EXEC privilege

Command History

Version 7.4.1.0	Introduced

Example

```
Force10#show lldp statistics
Total number of neighbors:   300
Last table change time   :   Mon Oct 02 16:00:52 2006
Number of Table Inserts  :   1621
Number of Table Deletes  :   200
Number of Table Drops    :   0
Number of Table Age Outs :   400
Force10#
```

show running-config lldp

C-Series	No
E-Series	✓

Display the current global LLDP configuration.

Syntax **show running-config lldp**

Defaults No default values or behavior

Command Modes EXEC privilege

Command History

Version 7.4.1.0	Introduced

Example

```
Force10#show running-config lldp
!
protocol lldp
 advertise dot1-tlv port-protocol-vlan-id port-vlan-id
 advertise dot3-tlv max-frame-size
 advertise management-tlv system-capabilities system-description
 hello 15
 multiplier 3
 no disable
Force10#
```

Chapter 11 SNMP and Syslog Commands

This section contains commands to configure and monitor SNMP v1/v2/v3 and Syslog and contains the following sections:

- SNMP Commands on page 323
- Syslog Commands on page 339

SNMP Commands

The Simple Network Management Protocol (SNMP) is used to communicate management information between the network management stations and the agents in the network elements. The FTOS supports SNMP versions 1, 2c, and 3, supporting both read-only and read-write modes. FTOS sends SNMP traps, which are messages informing the SNMP manager about the network. The software supports up to 16 SNMP trap receivers.

FTOS SNMP implementation conforms to RFC 1157 and RFC 2274 and the enterprise-specific MIB Force10-COPY-CONFIG-MIB, which supports SNMP SET requests.

Important Points to Remember

- Typically, 5-second timeout and 3-second retry values on an SNMP server are sufficient for both LAN and WAN applications. If you experience a timeout with these values, Force10 recommended best practice is to increase the timeout and retry values on your SNMP server to the following to accommodate the high port density provided by the E-Series and C-Series:

  SNMP Timeout—greater than 3 seconds

  SNMP Retry count—greater than 2 seconds
- If you want to query the chassis using SNMP v1/v2/v3 with an IPv6 address, configure the IPv6 address on an non-management port on the chassis.
- If you want to send SNMP v1/v2/v3 traps from the chassis using an IPv6 address, use a non-management port.
- SNMP v3 informs are not currently supported with IPv6 addresses.
- If you are using ACLs in SNMP v3 configuration, group ACL overrides user ACL if the user is part of that group.
- SNMP operations are not supported on a VLAN.

The SNMP commands available in FTOS are:

- show snmp on page 324
- show snmp engineID on page 325
- show snmp group on page 325
- show snmp user on page 326
- snmp-server community on page 326
- snmp-server contact on page 328
- snmp-server enable traps on page 328
- snmp-server engineID on page 329
- snmp-server group on page 330
- snmp-server host on page 332
- snmp-server location on page 334
- snmp-server trap-source on page 334
- snmp-server user on page 335
- snmp-server view on page 338
- snmp trap link-status on page 338

show snmp

View the status of SNMP network elements.

Syntax **show snmp**

Example

```
Force10#show snmp
      32685 SNMP packets input
          0 Bad SNMP version errors
          0 Unknown community name
          0 Illegal operation for community name supplied
          0 Encoding errors
      96988 Number of requested variables
          0 Number of altered variables
      31681 Get-request PDUs
        968 Get-next PDUs
          0 Set-request PDUs
      61727 SNMP packets output
          0 Too big errors (Maximum packet size 1500)
          9 No such name errors
          0 Bad values errors
          0 General errors
      32649 Response PDUs
      29078 Trap PDUs
Force10#
```

Figure 115 show snmp Command Example

Command Modes EXEC

EXEC privilege

Related Commands		
	snmp-server community	Enable SNMP and set community string.

show snmp engineID

View the identification of the local SNMP engine and all remote engines that are configured on the router.

Syntax **show snmp engineID**

Example

```
Force10#show snmp engineID
Local SNMP engineID: 0000178B02000001E80214A8
Remote Engine ID                IP-addr         Port
80001F88043132333435            172.31.1.3      5009
80001F88043938373635            172.31.1.3      5008

Force10#
```

Figure 116 show snmp engineID Command

Command Modes EXEC

EXEC privilege

Related Commands		
	snmp-server engineID	Configure local and remote SNMP engines on the router

show snmp group

Display the group name, security model, view status, and storage type of each group.

Syntax **show snmp group**

Example

```
Force10#show snmp group

  groupname: ngroup                        security model: v3 auth
  readview : nview                        writeview: no write view specified
  notifyview: nview
  row status: active

Force10#
```

Figure 117 show snmp group Command Example

Command Modes EXEC

EXEC privilege

Usage Information The example in Figure 117 displays a group named **ngroup**. The ngroup has a security model of version 3 (**v3**) with authentication (**auth**), the read and notify name is **nview** with no write view name specified, and finally the row status is active.

Related Commands

snmp-server group	Configure an SNMP server group

show snmp user

View the information configured on each SNMP user name.

Syntax **show snmp user**

Example

```
Force10#show snmp user
  User name: v1v2creadu
  Engine ID: 0000178B02000001E80214A8
  storage-type: nonvolatile        active
  Authentication Protocol: None
  Privacy Protocol: None

Force10#
```

Figure 118 show snmp user Command Example

Command Modes EXEC

EXEC privilege

snmp-server community

Configure a new community string access for SNMPv1, v2, and v3.

Syntax **snmp-server community** *community-name* {**ro** | **rw**} [**security-name** *name* [*access-list-name* | **ipv6** *access-list-name* | *access-list-name* **ipv6** *access-list-name*]]

To remove access to a community, use the **no snmp-server community** *community-string* {**ro** | **rw**} [**security-name** *name* [*access-list-name* | **ipv6** *access-list-name* | *access-list-name* **ipv6** *access-list-name*]] command.

Parameters

community-name	Enter a text string (up to 20 characters long) to act as a password for SNMP.
ro	Enter the keyword **ro** to specify Read Only permissions.
rw	Enter the keyword **rw** to specify Read Write permissions.
security-name *name*	(Optional) Enter the keywords **security-name** followed by the security name as defined by the community MIB.
access-list-name	(Optional) Enter the standard IPv4 access list name (a string up to 16 characters long).
ipv6 *access-list-name*	(Optional) Enter the keyword **ipv6** followed by the IPv6 access list name (a string up to 16 characters long)
access-list-name **ipv6** *access-list-name*	(Optional) Enter both an IPv4 and IPv6 access list name.

Defaults

No default behavior or values

Command Modes

CONFIGURATION

Usage Information

The example below configures a community named **public** that is mapped to the security named **guestuser** with Read Only (**ro**) permissions.

Example

```
Force10#conf
Force10(conf)# snmp-server community public ro
Force10(conf)# snmp-server community guest ro security-name guestuser
Force10(conf)#
```

The **security-name** parameter maps the community string to an SNMPv3 user/security name as defined by the community MIB.

If a community string is configured without a security-name (for example, **snmp-server community public ro**), the community is mapped to a default security-name/group:

- `v1v2creadu / v1v2creadg` — maps to a community with **ro** permissions
- `v1v2cwriteu/ v1v2cwriteg` — maps to a community with **rw** permissions

This command is indexed by the community-name parameter.

If the snmp-server community command is not configured, you cannot query SNMP data. Only Standard IPv4 ACL and IPv6 ACL is supported in the optional *access-list-name*.

Note: For IPv6 ACLs, only IPv6 and UDP types are valid for SNMP; TCP, ICMP rules are not valid for SNMP. In IPv6 ACLs port rules are not valids for SNMP.

Related Commands		
	show running-config snmp	View the current SNMP configuration and defaults.

snmp-server contact

Configure contact information for troubleshooting this SNMP node.

Syntax **snmp-server contact** *text*

To delete the SNMP server contact information, use the **no snmp-server contact** command.

Parameters		
	text	Enter an alphanumeric text string, up to 55 characters long.

Defaults Not configured.

Command Modes CONFIGURATION

snmp-server enable traps

Enable and configure SNMP traps.

Syntax **snmp-server enable traps** [*notification-type*] [*notification-option*]

To disable traps, use the **no snmp-server enable traps** [*notification-type*] [*notification-option*] command.

Parameters

notification-type	Enter the type of notification from the list below: • **bgp**—for notification of changes in BGP process • **envmon**—for Force10 Networks device notifications when an environmental threshold is exceeded • **snmp**—for notification of the RFC 1157 traps.
notification-option	For the **envmon** notification-type, enter one of the following optional parameters: • fan • supply • temperature For the **snmp** notification-type, enter one of the following optional parameters: • authentication • coldstart • linkdown • linkup

Defaults

Not enabled.

Command Modes

CONFIGURATION

Usage Information

FTOS supports up to 16 SNMP trap receivers.

If this command is not configured, no traps controlled by this command are sent. If you do not specify a *notification-type* and *notification-option*, all traps are enabled.

Related Commands

snmp-server community	Enable SNMP and set the community string.

snmp-server engineID

Configure name for both the local and remote SNMP engines on the router.

Syntax

snmp-server engineID [**local** *engineID*] [**remote** *ip-address* **udp-port** *port-number engineID*]

To return to the default, use the **no snmp-server engineID** [**local** *engineID*] [**remote** *ip-address* **udp-port** *port-number engineID*] command

Parameters

local *engineID*	Enter the keyword **local** followed by the engine ID number that identifies the copy of the SNMP on the *local* device. Format (as specified in RFC 3411): 12 octets. • The first 4 octets are set to the private enterprise number. • The remaining 8 octets are the MAC address of the chassis.
remote *ip-address*	Enter the keyword **remote** followed by the IP address that identifies the copy of the SNMP on the *remote* device.
udp-port *port-number engineID*	Enter the keyword **udp-port** followed by the UDP (User Datagram Protocol) port number on the remote device. Range: 0 to 65535 Default: 162

Defaults As above

Command Modes CONFIGURATION

Usage Information Changing the value of the SNMP Engine ID has important side effects. A user's password (entered on the command line) is converted to an MD5 (Message Digest Algorithm) or SHA (Secure Hash Algorithm) security digest. This digest is based on both the password and the local Engine ID. The command line password is then destroyed, as required by RFC 2274. Because of this deletion, if the local value of the Engine ID changes, the security digests of SNMPv3 users will be invalid, and the users will have to be reconfigured.

For the remote Engine ID, the host IP and UDP port are the indexes to the command that are matched to either overwrite or remove the configuration.

Related Commands

show snmp engineID	Display SNMP engine and all remote engines that are configured on the router
show running-config snmp	Display the SNMP running configuration

snmp-server group

Configure a new SNMP group or a table that maps SNMP users to SNMP views.

Syntax **snmp-server group** [*group_name* {**1** | **2c** | **3** {**auth** | **noauth** | **priv**}}] [**read** *name*] [**write** *name*] [**notify** *name*] [*access-list-name* | **ipv6** *access-list-name* | *access-list-name* **ipv6** *access-list-name*]]

To remove a specified group, use the **no snmp-server group** [*group_name* {**v1** | **v2c** | **v3** {**auth** | **noauth** | **priv**}}] [**read** *name*] [**write** *name*] [**notify** *name*] [*access-list-name* | **ipv6** *access-list-name* | *access-list-name* **ipv6** *access-list-name*]] command.

Parameters

group_name	Enter a text string (up to 20 characters long) as the name of the group. Defaults: The following groups are created for mapping to read/write community/security-names. • `v1v2creadg` — maps to a community/security-name with **ro** permissions • `1v2cwriteg` — maps to a community/security-name **rw** permissions
1 | **2c** | **3**	(OPTIONAL) Enter the security model version number (**1**, **2c**, or **3)**. • **1** is the least secure version • **3** is the most secure of the security modes. • **2c** allows transmission of informs and counter 64, which allows for integers twice the width of what is normally allowed. Default: **1**
auth	(OPTIONAL) Enter the keyword **auth** to specify authentication of a packet without encryption.
noauth	(OPTIONAL) Enter the keyword **noauth** to specify no authentication of a packet.
priv	(OPTIONAL) Enter the keyword **priv** to specify both authentication and then scrambling of the packet.
read *name*	(OPTIONAL) Enter the keyword **read** followed by a name (a string of up to 20 characters long) as the read view name. Default: GlobalView is set by default and is assumed to be every object belonging to the Internet (1.3.6.1) OID space.
write *name*	(OPTIONAL) Enter the keyword **write** followed by a name (a string of up to 20 characters long) as the write view name.
notify *name*	(OPTIONAL) Enter the keyword **notify** followed by a name (a string of up to 20 characters long) as the notify view name.
access-list-name	(Optional) Enter the standard IPv4 access list name (a string up to 16 characters long).
ipv6 *access-list-name*	(Optional) Enter the keyword **ipv6** followed by the IPv6 access list name (a string up to 16 characters long)
access-list-name **ipv6** *access-list-name*	(Optional) Enter both an IPv4 and IPv6 access list name.

Defaults

As defined above

Command Modes

CONFIGURATION

Usage Information

The following example specifies the group named **harig** as a version **3** user requiring both authentication and encryption and read access limited to the read named **rview**.

Note: For IPv6 ACLs, only IPv6 and UDP types are valid for SNMP; TCP, ICMP rules are not valid for SNMP. In IPv6 ACLs port rules are not valids for SNMP.

Example

```
Force10#conf
Force10(conf)# snmp-server group harig 3 priv read rview
Force10#
```

Note: The number of configurable groups is limited to 16 groups.

Related Commands

show snmp group	Display the group name, security model, view status, and storage type of each group.
show running-config snmp	Display the SNMP running configuration

snmp-server host

Configure the recipient of an SNMP trap operation.

Syntax

snmp-server host *ip-address* | *ipv6-address* [**traps | informs**] [**version 1** | **2c | 3**] [**auth** | **no auth** | **priv**] [*community-string*] [**udp-port** *port-number*] [*notification-type*]

To remove the SNMP host, use the **no snmp-server host** *ip-address* [**traps | informs**] [**version 1** | **2c | 3**] [**auth** | **noauth** | **priv**] [*community-string*] [**udp-port** *number*] [*notification-type*] command.

Parameters

ip-address	Enter the keyword **host** followed by the IP address of the host (configurable hosts is limited to 16).
ipv6-address	Enter the keyword **host** followed by the IPv6 address of the host in the **x:x:x:x::x** format. The **::** notation specifies successive hexadecimal fields of zero
traps	(OPTIONAL) Enter the keyword **traps** to send trap notifications to the specified host. Default: traps
informs	(OPTIONAL) Enter the keyword **informs** to send inform notifications to the specified host. Default: traps
version 1 | **2c** | **3**	(OPTIONAL) Enter the keyword **version** to specify the security model followed by the security model version number **1**, **2c**, or **3**. • Version **1** is the least secure version • version **3** is the most secure of the security modes. • Version **2c** allows transmission of informs and counter 64, which allows for integers twice the width of what is normally allowed. Default: Version **1**
auth	(OPTIONAL) Enter the keyword **auth** to specify authentication of a packet without encryption.
noauth	(OPTIONAL) Enter the keyword **noauth** to specify no authentication of a packet.

priv	(OPTIONAL) Enter the keyword **priv** to specify both authentication and then scrambling of the packet.
community-string	Enter a text string (up to 20 characters long) as the name of the SNMP community. **Note:** For version 1 and version 2c security models, this string represents the name of the SNMP community. The string can be set using this command, however it is recommended that you set the community string using the **snmp-server community** command before executing this command. For version 3 security model, this string is the USM user security name.
udp-port *port-number*	(OPTIONAL) Enter the keywords **udp-port** followed by the port number of the remote host to use. Range: 0 to 65535. Default: 162
notification-type	(OPTIONAL) Enter one of the following keywords as the type of trap to be sent to the host: • **bgp** - allow BGP state change traps • **envmon** - allows environment monitor traps • **snmp** - Allows SNMP-type notification (RFC 1157) traps. Default: All trap types are sent to host

Defaults

As shown

Command Modes

CONFIGURATION

Usage Information

In order to configure the router to send SNMP notifications, you must enter at least one **snmp-server host** command. If you enter the command with no keywords, all trap types are enabled for the host. If you do not enter an **snmp-server host** command, no notifications are sent.

In order to enable multiple hosts, you must issue a separate s**nmp-server host** command for each host. You can specify multiple notification types in the command for each host.

When multiple **snmp-server host** commands are given for the same host and type of notification (trap or inform), each succeeding command overwrites the previous command. Only the last **snmp-server host** command will be in effect. For example, if you enter an **snmp-server host inform** command for a host and then enter another s**nmp-server host inform** command for the same host, the second command will replace the first.

The **snmp-server host** command is used in conjunction with the **snmp-server enable** command. Use the snmp-server enable command to specify which SNMP notifications are sent globally. For a host to receive most notifications, at least one **snmp-server enable** command and the **snmp-server host** command for that host must be enabled.

Note: For v1 / v2c trap configuration, if the community-string is not defined using the **snmp-server community** command prior to using this command, the default form of the **snmp-server community** command will automatically be configured, with the community-name the same as specified in the **snmp-server host** command.

Configuring Informs

To send an inform, follow the step below.

1. Configure a remote engine ID
2. Configure a remote user
3. Configure a group for this user with access rights
4. Enable traps
5. Configure a host to receive informs

Related Commands

snmp-server enable traps	Enable SNMP traps.
snmp-server community	Configure a new community SNMPv1 or SNMPv2c

snmp-server location

Configure the location of the SNMP server.

Syntax **snmp-server location** *text*

To delete the SNMP location, enter **no snmp-server location**.

Parameters

text	Enter an alpha-numeric text string, up to 256 characters long.

Defaults Not configured.

Command Modes CONFIGURATION

snmp-server trap-source

Configure a specific interface as the source for SNMP traffic.

Syntax **snmp-server trap-source** *interface*

To disable sending traps out a specific interface, enter **no snmp trap-source**.

Parameter		
	interface	Enter the following keywords and slot/port or number information: • For an 100/1000 Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For a Loopback interface, enter the keyword **loopback** followed by a number from 0 to 16383. • For a SONET interface, enter the keyword **sonet** followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information.

Defaults The IP address assigned to the management interface is the default.

Command Modes CONFIGURATION

Usage Information For this snmp-server trap-source command to be enabled, you must configure an IP address on the interface and enable the interface configured as an SNMP trap source.

Related Commands

snmp-server community	Set the community string.

snmp-server user

Configure a new user to an SNMP group.

Syntax **snmp-server user** *name* {*group_name* **remote** *ip-address* **udp-port** *port-number*} [**1** | **2c | 3**] [**encrypted**] [**auth** {**md5** | **sha**} *auth-password*] [**priv des56** *priv password*] [*access-list-name* | **ipv6** *access-list-name* | *access-list-name* **ipv6** *access-list-name*]

To remove a user from the SNMP group, use the **no snmp-server user** *name* {*group_name* **remote** *ip-address* **udp-port** *port-number*} [**1** | **2c | 3**] [**encrypted**] [**auth** {**md5** | **sha**} *auth-password*] [**priv des56** *priv password*] [*access-list-name* | **ipv6** *access-list-name* | *access-list-name* **ipv6** *access-list-name*] command.

Parameters		
	name	Enter the name of the user (not to exceed 20 characters), on the host, that connects to the agent.
	group_name	Enter a text string (up to 20 characters long) as the name of the group. Defaults: The following groups are created for mapping to read/write community/security-names. • `v1v2creadu` — maps to a community with **ro** permissions • `1v2cwriteu` — maps to a community **rw** permissions
	remote *ip-address*	Enter the keyword **remote** followed by the IP address that identifies the copy of the SNMP on the *remote* device.

udp-port *port-number*	Enter the keyword **udp-port** followed by the UDP (User Datagram Protocol) port number on the remote device. Range: 0 to 65535. Default: 162
1 | **2c** | **3**	(OPTIONAL) Enter the security model version number (**1**, **2c**, or **3)**. • **1** is the least secure version • **3** is the most secure of the security modes. • **2c** allows transmission of informs and counter 64, which allows for integers twice the width of what is normally allowed. Default: **1**
encrypted	(OPTIONAL) Enter the keyword **encrypted** to specify the password appear in encrypted format (a series of digits, masking the true characters of the string).
auth	(OPTIONAL) Enter the keyword **auth** to specify authentication of a packet without encryption.
md5 | **sha**	(OPTIONAL) Enter the keyword **md5** or **sha** to designate the authentication level. **md5** — Message Digest Algorithm **sha** — Secure Hash Algorithm
auth-password	(OPTIONAL) Enter a text string (up to 20 characters long) password that will enable the agent to receive packets from the host. Minimum: 8 characters long
priv des56	(OPTIONAL) Enter the keyword **priv des56** to initiate a privacy authentication level setting using the CBC-DES privacy authentication algorithm (**des56**).
priv password	(OPTIONAL) Enter a text string (up to 20 characters long) password that will enables the host to encrypt the contents of the message it sends to the agent. Minimum: 8 characters long
access-list-name	(Optional) Enter the standard IPv4 access list name (a string up to 16 characters long).
ipv6 *access-list-name*	(Optional) Enter the keyword **ipv6** followed by the IPv6 access list name (a string up to 16 characters long)
access-list-name **ipv6** *access-list-name*	(Optional) Enter both an IPv4 and IPv6 access list name.

Defaults As above

Command Modes CONFIGURATION

Usage Information

Note: For IPv6 ACLs, only IPv6 and UDP types are valid for SNMP; TCP, ICMP rules are not valid for SNMP. In IPv6 ACLs port rules are not valids for SNMP.

No default values exist for authentication or privacy algorithms and no default password exist. If you forget a password, you cannot recover it; the user must be reconfigured. You can specify either a plain-text password or an encrypted cypher-text password. In either case, the password will be stored in the configuration in an encrypted form and displayed as encrypted in the show running-config command.

If you have an encrypted password, you can specify the encrypted string instead of the plain-text password. The following command is an example of how to specify the command with an encrypted string:

Example

```
Force10# snmp-server user privuser v3group v3 encrypted auth md5
9fc53d9d908118b2804fe80e3ba8763d priv des56 d0452401a8c3ce42804fe80e3ba8763d

Force10#
```

The following command is an example of how to enter a plain-text password as the string **authpasswd** for user **authuser** of group **v3group**.

Example

```
Force10#conf
Force10(conf)# snmp-server user authuser v3group v3 auth md5 authpasswd

Force10#
```

The following command configures a remote user named **n3user** with a **v3** security model and a security level of **authNOPriv**.

Example

```
Force10#conf
Force10(conf)# snmp-server user n3user ngroup remote 172.31.1.3 udp-port 5009 3
auth md5 authpasswd

Force10#
```

Note: The number of configurable users is limited to 16.

Related Commands

show snmp user	View the information configured on each SNMP user name.

snmp-server view

Configure an SNMPv3 view.

Syntax **snmp-server view** *view-name oid-tree* {**included** | **excluded**}

To remove an SNMPv3 view, use the **no snmp-server view** *view-name oid-tree* {**included** | **excluded**} command.

Parameters

view-name	Enter the name of the view (not to exceed 20 characters).
oid-tree	Enter the OID sub tree for the view (not to exceed 20 characters).
included	(OPTIONAL) Enter the keyword **included** to include the MIB family in the view.
excluded	(OPTIONAL) Enter the keyword **excluded** to exclude the MIB family in the view.

Defaults No default behavior or values

Command Modes CONFIGURATION

Usage Information The *oid-tree* variable is a full sub-tree starting from 1.3.6 and can not specify the name of a sub-tree or a MIB. The following example configures a view named **rview** that allows access to all objects under 1.3.6.1

Example

```
Force10# conf
Force10#(conf) snmp-server view rview 1.3.6.1 included

Force10#
```

Related Commands

show running-config snmp	Display the SNMP running configuration

snmp trap link-status

Enable the interface to send SNMP link traps, which indicate whether the interface is up or down.

Syntax **snmp trap link-status**

To disable sending link trap messages, enter **no snmp trap link-status**.

Defaults Enabled.

Command Modes INTERFACE

Usage Information If the interface is expected to flap during normal usage, you could disable this command.

Syslog Commands

The following commands allow you to configure logging functions on the E-Series.

- clear logging on page 339
- default logging buffered on page 340
- default logging console on page 340
- default logging monitor on page 341
- default logging trap on page 341
- logging on page 341
- logging buffered on page 342
- logging console on page 343
- logging facility on page 343
- logging history on page 344
- logging history size on page 345
- logging monitor on page 346
- logging on on page 346
- logging source-interface on page 347
- logging synchronous on page 347
- logging trap on page 348
- show logging on page 349
- terminal monitor on page 350

clear logging

Clear the messages in the logging buffer.

Syntax **clear logging**

Defaults None.

Command Modes EXEC privilege

Related Commands

show logging	View logging settings and system messages in the internal buffer.

default logging buffered

Return to the default setting for messages logged to the internal buffer.

Syntax **default logging buffered**

Defaults size = 40960; level = 7 or debugging

Command Modes CONFIGURATION

Related Commands

logging buffered	Set the logging buffered parameters.

default logging console

Return the default settings for messages logged to the console.

Syntax **default logging console**

Defaults level = 7 or debugging

Command Modes CONFIGURATION

Related Commands

logging console	Set the logging console parameters.

default logging monitor

Return to the default settings for messages logged to the terminal.

Syntax **default logging monitor**

Defaults level = 7 or debugging

Command Modes CONFIGURATION

Related Commands

logging monitor	Set the logging monitor parameters.
terminal monitor	Send system messages to the terminal/monitor.

default logging trap

Return to the default settings for logging messages to the Syslog servers.

Syntax **default logging trap**

Defaults level = 6 or informational

Command Modes CONFIGURATION

Related Commands

logging trap	Limit messages logged to the Syslog servers based on severity.

logging

Configure an IP address or host name of a Syslog server where logging messages will be sent.

Syntax **logging** {*ip-address* | *hostname*}

To disable logging, enter **no logging**.

Parameters

ip-address	Enter the IP address in dotted decimal format.
hostname	Enter the name of a host already configured and recognized by the E-Series.

Defaults Disabled

Command Modes CONFIGURATION

Related Commands

logging on	Enables the logging asynchronously to logging buffer, console, Syslog server, and terminal lines.
logging trap	Enables logging to the Syslog server based on severity.

logging buffered

Enable logging and specify which messages are logged to an internal buffer. By default, all messages are logged to the internal buffer.

Syntax **logging buffered** [*level*] [*size*]

To return to the default values, enter **default logging buffered**. To disable logging stored to an internal buffer, enter **no logging buffered**.

Parameters

level	(OPTIONAL) Indicate a value from 0 to 7 or enter one of the following parameters: emergencies, alerts, critical, errors, warnings, notifications, informational, or debugging. Default: 7 or debugging.
size	(OPTIONAL) Indicate the size, in bytes, of the logging buffer. The number of messages buffered depends on the size of each message. Range: 40960 to 524288. Default: 40960 bytes.

Defaults *level* = 7; *size* = 40960 bytes

Command Modes CONFIGURATION

Usage Information When you decrease the buffer size, all messages stored in the buffer are lost. Increasing the buffer size does not affect messages stored in the buffer.

Related Commands

clear logging	Clear the logging buffer.
default logging buffered	Returns the logging buffered parameters to the default setting.
show logging	View the logging setting and system messages in the internal buffer.

logging console

Specify which messages are logged to the console.

Syntax **logging console** [*level*]

To return to the default values, enter default logging console. To disable logging to the console, enter **no logging console**.

Parameters

level	(OPTIONAL) Indicate a value from 0 to 7 or enter one of the following parameters: emergencies, alerts, critical, errors, warnings, notifications, informational, or debugging. Default: 7 or debugging.

Defaults 7 or debugging

Command Modes CONFIGURATION

Related Commands

clear logging	Clear logging buffer.
default logging console	Returns the logging console parameters to the default setting.
show logging	View logging settings and system messages in the internal buffer.

logging facility

Configure the Syslog facility, used for error messages sent to Syslog servers.

Syntax **logging facility** [*facility-type*]

To return to the default values, enter **no logging facility**.

Parameters

facility-type	(OPTIONAL) Enter one of the following parameters. • auth (authorization system) • cron (Cron/at facility) • deamon (system deamons) • kern (kernel) • local0 (local use) • local1 (local use) • local2 (local use) • local3 (local use) • local4 (local use) • local5 (local use) • local6 (local use) • local7 (local use) • lpr (line printer system) • mail (mail system) • news (USENET news) • sys9 (system use) • sys10 (system use) • sys11 (system use) • sys12 (system use) • sys13 (system use) • sys14 (system use) • syslog (Syslog process) • user (user process) • uucp (Unix to Unix copy process) The default is local7.

Defaults local7

Command Modes CONFIGURATION

Related Commands

logging	Enable logging to a Syslog server.
logging on	Enables logging.

logging history

Specify which messages are logged to the E-Series history table and the SNMP network management station.

Syntax **logging history** *level*

To return to the default values, enter **no logging history**.

Parameters

level	Indicate a value from 0 to 7 or enter one of the following parameters: emergencies, alerts, critical, errors, warnings, notifications, informational, or debugging. The default is 4.

Defaults 4 or warnings

Command Modes CONFIGURATION

Usage Information When you configure the snmp-server trap-source command, the system messages logged to the E-Series history table are also sent to the SNMP network management station.

Related Commands

show logging history	View information logged to the history buffer.

logging history size

Specify the number of messages stored in the FTOS logging history table.

Syntax **logging history size** *size*

To return to the default values, enter **no logging history size**.

Parameters

size	Indicate a value as the number of messages to be stored. Range: 0 to 500. Default: 1 message.

Defaults 1 message

Command Modes CONFIGURATION

Usage Information When the number of messages reaches the limit you set with the logging history size command, older messages are deleted as newer ones are added to the table.

Related Commands

show logging history	View information logged to the history buffer.

logging monitor

Specify which messages are logged to Telnet applications.

Syntax **logging monitor** [*level*]

To disable logging to terminal connections, enter **no logging monitor**.

Parameters

level	Indicate a value from 0 to 7 or enter one of the following parameters: emergencies, alerts, critical, errors, warnings, notifications, informational, or debugging. The default is 7 or debugging.

Defaults 7 or debugging

Command Modes CONFIGURATION

Related Commands

default logging monitor	Returns the logging monitor parameters to the default setting.

logging on

Specify that debug or error messages are asynchronously logged to multiple destinations, such as logging buffer, Syslog server, or terminal lines.

Syntax **logging on**

To disable logging to logging buffer, Syslog server and terminal lines, enter **no logging on**.

Defaults Enabled

Command Modes CONFIGURATION

Usage Information When you enter **no logging on**, messages are logged only to the console.

Related Commands

logging	Enable logging to Syslog server.
logging buffered	Set the logging buffered parameters.
logging console	Set the logging console parameters.
logging monitor	Set the logging parameters for the terminal connections.

logging source-interface

Specify that the IP address of an interface is the source IP address of Syslog packets sent to the Syslog server.

Syntax **logging source-interface** *interface*

To disable this command and return to the default setting, enter **no logging source-interface**.

Parameters

interface	Enter the following keywords and slot/port or number information: • For an 100/1000 Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For a Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For Loopback interfaces, enter the keyword **loopback** followed by a number from zero (0) to 16383. • For the management interface on the RPM, enter the keyword **ManagementEthernet** followed by the slot/port information. The slot range is 0-1 and the port range is 0. • For a Port Channel, enter the keyword **port-channel** followed by a number: C-Series Range: 1-128 E-Series Range: 1-32 for EtherScale, 1-255 for TeraScale, • For a SONET interface, enter the keyword **sonet** followed by the slot/port information. • For a Ten Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information. • For VLAN interface, enter the keyword **vlan** followed by a number from 1 to 4094.

Defaults Not configured.

Command Modes CONFIGURATION

Usage Information Syslog messages contain the IP address of the interface used to egress the router. By configuring the logging source-interface command, the Syslog packets contain the IP address of the interface configured.

Related Commands

logging	Enable the logging to another device.

logging synchronous

Synchronize unsolicited messages and FTOS output.

Syntax **logging synchronous** [**level** *level* | **all**] [**limit** *number-of-buffers*]

To disable message synchronization, use the **no logging synchronous** [**level** *level* | **all**] [**limit** *number-of-buffers*] command.

Parameters

all	Enter the keyword **all** to ensure that all levels are printed asynchronously.
level *level*	Enter the keyword **level** followed by a number as the severity level. A high number indicates a low severity level and visa versa. Range: 0 to 7. Default: 2
all	Enter the keyword all to turn off all
limit *number-of-buffers*	Enter the keyword **limit** followed by the number of buffers to be queued for the terminal after which new messages are dropped Range: 20 to 300 Default: 20

Defaults Disabled. If enabled without *level* or *number-of-buffers* options specified, *level* = 2 and *number-of-buffers* = 20 are the defaults.

Command Modes LINE

Usage Information When logging synchronous is enabled, unsolicited messages appear between software prompts and outputs. Only the messages with a severity at or below the set level are sent to the console.

If the message queue limit is reached on a terminal line and messages are discarded, a system message appears on that terminal line. Messages may continue to appear on other terminal lines.

Related Commands

logging on	Enables logging.

logging trap

Specify which messages are logged to the Syslog server based the messages' severity.

Syntax **logging trap** [*level*]

To return to the default values, enter **default logging trap**. To disable logging, enter **no logging trap**.

Parameters

level	Indicate a value from 0 to 7 or enter one of the following parameters: emergencies, alerts, critical, errors, warnings, notifications, informational, or debugging. The default is 6.

Defaults 6 or informational

Command Modes CONFIGURATION

Related Commands

logging	Enable the logging to another device.
logging on	Enables logging.

show logging

View the logging settings and system messages logged to the E-Series internal buffer.

Syntax **show logging [***number* {**history} {reverse}] | [summary**]

Parameters

number	(OPTIONAL) Enter the number of message to be displayed on the output. Range: 1 to 65535
history	(OPTIONAL) Enter the keyword **history** to view only information in the Syslog history table.
reverse	(OPTIONAL) Enter the keyword **reverse** to view the Syslog messages in an FIFO (first in, first out) order.
summary	(OPTIONAL) Enter the keyword **summary** to view a table showing the number of messages per type and per slot. Slots *7* and *8* represent RPMs.

Command Modes EXEC

EXEC privilege

```
Force10#show logging
Syslog logging: enabled
    Console logging: level debugging
    Monitor logging: level debugging
    Buffer logging: level debugging, 5604 Messages Logged, Size (524288 bytes)
    Trap logging: level informational
Oct 8 09:25:37: %RPM1:RP1 %BGP-5-ADJCHANGE: Connection with neighbor 223.80.255.254 closed. Hold time
expired
Oct 8 09:25:38: %RPM1:RP1 %BGP-5-ADJCHANGE: Neighbor 192.200.13.2 Up
Oct 8 09:25:38: %RPM1:RP1 %BGP-5-ADJCHANGE: Neighbor 192.1.1.13 Up
Oct 8 09:25:38: %RPM1:RP1 %BGP-5-ADJCHANGE: Neighbor 1.1.14.2 Up
Oct 8 09:25:38: %RPM1:RP1 %BGP-5-ADJCHANGE: Neighbor 192.1.1.14 Up
Oct 8 09:25:38: %RPM1:RP1 %BGP-5-ADJCHANGE: Neighbor 1.1.11.2 Up
Oct 8 09:25:38: %RPM1:RP1 %BGP-5-ADJCHANGE: Neighbor 192.1.1.5 Up
Oct 8 09:25:38: %RPM1:RP1 %BGP-5-ADJCHANGE: Neighbor 192.4.1.3 Up
Oct 8 09:25:38: %RPM1:RP1 %BGP-5-ADJCHANGE: Neighbor 192.1.1.4 Up
Oct 8 09:25:38: %RPM1:RP1 %BGP-5-ADJCHANGE: Neighbor 192.1.1.6 Up
Oct 8 09:25:38: %RPM1:RP1 %BGP-5-ADJCHANGE: Neighbor 192.1.1.12 Up
Oct 8 09:25:38: %RPM1:RP1 %BGP-5-ADJCHANGE: Neighbor 192.1.1.15 Up
Oct 8 09:25:38: %RPM1:RP1 %BGP-5-ADJCHANGE: Neighbor 192.1.1.3 Up
Oct 8 09:25:38: %RPM1:RP1 %BGP-5-ADJCHANGE: Neighbor 192.200.12.2 Up
Oct 8 09:25:38: %RPM1:RP1 %BGP-5-ADJCHANGE: Neighbor 1.1.10.2 Up
Oct 8 09:25:38: %RPM1:RP1 %BGP-5-ADJCHANGE: Session closed by neighbor 1.1.10.2 (Hold time expired)
Oct 8 09:25:38: %RPM1:RP1 %BGP-5-ADJCHANGE: Neighbor 192.200.14.7 Up
Oct 8 09:26:25: %RPM1:RP1 %BGP-5-ADJCHANGE: Connection with neighbor 1.1.11.2 closed. Neighbor recycled
Oct 8 09:26:25: %RPM1:RP1 %BGP-5-ADJCHANGE: Connection with neighbor 1.1.14.2 closed. Neighbor recycled
--More--
```

Figure 119 show logging Command Example (Partial)

```
Force10#show logging history
Syslog History Table: 1 maximum table entries,
saving level Warnings or higher
  SNMP notifications not Enabled
%RPM:0:0 %CHMGR-2-LINECARDDOWN - Line card 3 down - IPC timeout
Force10#
```

Figure 120 show logging history Command Example

terminal monitor

Configure the FTOS to display messages on the monitor/terminal.

Syntax **terminal monitor**

To return to default settings, enter **terminal no monitor**.

Defaults Disabled.

Command Modes EXEC

EXEC privilege

Related Commands

logging monitor	Set the logging parameters on the monitor/terminal.

Chapter 12 RMON

FTOS Remote Network Monitoring (RMON) is implemented based on industry RFC standards providing both 32bit and 64bit monitoring, and long term statistics collection on Force10 chassis. FTOS RMON supports the following RMON Groups as defined in RFC-2819, RFC-3273, and RFC-3434:

- Ethernet Statistics Table RFC-2819
- Ethernet Statistics High-Capacity Table RFC-3273, 64bits
- Ethernet History Control Table RFC-2819
- Ethernet History Table RFC-2819
- Ethernet History High-Capacity Table RFC-3273, 64bits
- Alarm Table RFC-2819
- High-Capacity Alarm Table (64bits) RFC-3434, 64bits
- Event Table RFC-2819
- Log Table RFC-2819

The RMON commands are:

- rmon alarm on page 354
- rmon collection history on page 355
- rmon collection statistics on page 356
- rmon event on page 356
- rmon hc-alarm on page 357
- show rmon on page 358
- show rmon alarms on page 359
- show rmon events on page 360
- show rmon hc-alarm on page 361
- show rmon history on page 362
- show rmon log on page 363
- show rmon statistics on page 364

Important Points to Remember

- Only SNMP GET/GETNEXT access is supported. Configure RMON using the RMON commands.
- Collected data is lost during a chassis reboot.
- FTOS RMON does not support the following statistics:
  - etherStatsCollisions
  - etherHistoryCollisions
  - etherHistoryUtilization

rmon alarm

Set an alarm on any MIB object.

Syntax **rmon alarm** *number variable interval* {**delta** | **absolute**} **rising-threshold** *value event-number* **falling-threshold** *value event-number* [**owner** *string*]

To disable the alarm, use the **no rmon alarm** *number* command.

Parameters

number	Enter the alarm integer number from 1 to 65535. The value must be unique in the RMON Alarm Table.
variable	The MIB object to monitor. The variable must be in the SNMP OID format, for example, 1.3.6.1.2.1.1.3 The object type must be a 32 bit integer.
interval	Time, in seconds, the alarm monitors the MIB variables; this is the alarmSampleType in the RMON Alarm table. Range: 5 to 3600 seconds
delta	Enter the keyword **delta** to test the change between MIB variables. This is the alarmSampleType in the RMON Alarm table.
absolute	Enter the keyword **absolute** to test each MIB variable directly. This is the alarmSampleType in the RMON Alarm table.
rising-threshold *value event-number*	Enter the keyword **rising-threshold** followed by the value (32bit) the rising-threshold alarm is either triggered or reset. Then enter the event-number to trigger when the rising threshold exceeds its limit. This value is the same as the alarmRisingEventIndex or alarmTable of the RMON MIB. If there is no corresponding rising-threshold event, the value is zero.
falling-threshold *value event-number*	Enter the keyword **falling-threshold** followed by the value (32bit) the falling-threshold alarm is either triggered or reset. Then enter the event-number to trigger when the falling threshold exceeds its limit. This value is the same as the alarmFallingEventIndex or the alarmTable of the RMON MIB. If there is no corresponding falling-threshold event, the value is zero.
owner *string*	(OPTIONAL) Enter the keyword **owner** followed by the owner name to specify an owner for the alarm. This is the alarmOwner object in the alarmTable of the RMON MIB.

Default owner

Command Modes CONFIGURATION

Command History

Version 6.1.1.0	Introduced

rmon collection history

Enable the RMON MIB history group of statistics collection on an interface.

Syntax **rmon collection history** {**controlEntry** *integer*} [**owner** *name*] [**buckets** *number*] [**interval** *seconds*]

To remove a specified RMON history group of statistics collection, use the **no rmon collection history** {**controlEntry** *integer*} command.

Parameters

controlEntry *integer*	Enter the keyword **controlEntry** to specify the RMON group of statistics using a value. Then enter an integer value from 1 to 65535 that identifies the RMON group of statistics. The integer value must be a unique index in the RMON History Table.
owner *name*	(OPTIONAL) Enter the keyword **owner** followed by the owner name to record the owner of the RMON group of statistics.
buckets *number*	(OPTIONAL) Enter the keyword **buckets** followed the number of buckets for the RMON collection history group of statistics. Bucket Range: 1 to 1000 Default: 50
interval *seconds*	(OPTIONAL) Enter the keyword **interval** followed the number of seconds in each polling cycle. Range: 5 to 3600 seconds Default: 1800 seconds

Defaults No default behavior

Command Modes CONFIGURATION INTERFACE (config-if)

Command History

Version 6.1.1.0	Introduced

rmon collection statistics

Enable RMON MIB statistics collection on an interface.

Syntax **rmon collection statistics** {**controlEntry** *integer*} [**owner** *name*]

To remove RMON MIB statistics collection on an interface, use the **no rmon collection statistics** {**controlEntry** *integer*} command.

Parameters

controlEntry *integer*	Enter the keyword **controlEntry** to specify the RMON group of statistics using a value. Then enter an integer value from 1 to 65535 that identifies the RMON Statistic Table. The integer value must be a unique in the RMON Statistic Table.
owner *name*	(OPTIONAL) Enter the keyword **owner** followed by the owner name to record the owner of the RMON group of statistics.

Defaults No default behavior

Command Modes CONFIGURATION INTERFACE (config-if)

Command History

Version 6.1.1.0	Introduced

rmon event

Add an event in the RMON event table.

Syntax **rmon event** *number* [**log**] [**trap** *community*] [**description** *string*] [**owner***name*]

To disable RMON on an interface, use the **no rmon event** *number* [**log**] [**trap** *community*] [**description** *string*] command.

Parameters

number	Assign an event number in integer format from 1 to 65535. The number value must be unique in the RMON Event Table.
log	(OPTIONAL) Enter the keyword **log** to generate an RMON log entry. The log entry is triggered and sets the eventType in the RMON MIB to log or log-and-trap. Default: No log
trap *community*	(OPTIONAL) Enter the keyword **trap** followed by an SNMP community string to configure the eventType setting in the RMON MIB. This sets either snmp-trap or log-and-trap. Default: public

description *string*	(OPTIONAL) Enter the keyword **description** followed by a string describing the event.
owner *name*	(OPTIONAL) Enter the keyword **owner** followed by the name of the owner of this event.

Defaults as describe above

Command Modes CONFIGURATION

Command History

Version 6.1.1.0	Introduced

rmon hc-alarm

Set an alarm on any MIB object.

Syntax **rmon hc-alarm** *number variable interval* {**delta** | **absolute**} **rising-threshold** *value event-number* **falling-threshold** *value event-number* [**owner** *string*]

To disable the alarm, use the **no rmon hc-alarm** *number* command.

Parameters

number	Enter the alarm integer number from 1 to 65535. The value must be unique in the RMON Alarm Table.
variable	The MIB object to monitor. The variable must be in the SNMP OID format, for example, 1.3.6.1.2.1.1.3 The object type must be a 64 bit integer.
interval	Time, in seconds, the alarm monitors the MIB variables; this is the alarmSampleType in the RMON Alarm table. Range: 5 to 3600 seconds
delta	Enter the keyword **delta** to test the change between MIB variables. This is the alarmSampleType in the RMON Alarm table.
absolute	Enter the keyword **absolute** to test each MIB variable directly. This is the alarmSampleType in the RMON Alarm table.
rising-threshold *value event-number*	Enter the keyword **rising-threshold** followed by the value (64 bit) the rising-threshold alarm is either triggered or reset. Then enter the event-number to trigger when the rising threshold exceeds its limit. This value is the same as the alarmRisingEventIndex or alarmTable of the RMON MIB. If there is no corresponding rising-threshold event, the value is zero.

falling-threshold *value event-number*	Enter the keyword **falling-threshold** followed by the value (64 bit) the falling-threshold alarm is either triggered or reset. Then enter the event-number to trigger when the falling threshold exceeds its limit. This value is the same as the alarmFallingEventIndex or the alarmTable of the RMON MIB. If there is no corresponding falling-threshold event, the value is zero.
owner *string*	(OPTIONAL) Enter the keyword **owner** followed the owner name to specify an owner for the alarm. This is the alarmOwner object in the alarmTable of the RMON MIB.

Defaults owner

Command Modes CONFIGURATION

Command History

Version 6.1.1.0	Introduced

show rmon

Display the RMON running status including the memory usage.

Syntax **show rmon**

Defaults No default behavior

Command Modes EXEC

Command History

Version 6.1.1.0	Introduced

Example

```
Force10# show rmon
RMON status
    total memory used 218840 bytes.
    ether statistics table: 8 entries, 4608 bytes
    ether history table: 8 entries, 6000 bytes
    alarm table: 390 entries, 102960 bytes
    high-capacity alarm table: 5 entries, 1680 bytes
    event table: 500 entries, 206000 bytes
    log table: 2 entries, 552 bytes
Force10#
```

Figure 121 show rmon Command Example

show rmon alarms

Display the contents of the RMON Alarm Table.

Syntax **show rmon alarms** [*index*] [**brief**]

Parameters

index	(OPTIONAL) Enter the table index number to display just that entry.
brief	(OPTIONAL) Enter the keyword **brief** to display the RMON Alarm Table in an easy-to-read format.

Defaults No default behavior

Command Modes EXEC

Command History

Version 6.1.1.0	Introduced

Example 1

```
Force10#show rmon alarm  1
RMON alarm entry 1
    sample Interval: 5
    object: 1.3.6.1.2.1.1.3
    sample type: absolute value.
    value: 255161
    alarm type: rising or falling alarm.
    rising threshold: 1, RMON event index: 1
    falling threshold: 501, RMON event index: 501
    alarm owner: 1
    alarm status: OK
Force10#
```

Figure 122 show rmon alarms *index* Command Example

Example 2

```
Force10#show rmon alarm br
index           SNMP OID
------------------------------------------------------------------------
-
1               1.3.6.1.2.1.1.3
2               1.3.6.1.2.1.1.3
3               1.3.6.1.2.1.1.3
4               1.3.6.1.2.1.1.3
5               1.3.6.1.2.1.1.3
6               1.3.6.1.2.1.1.3
7               1.3.6.1.2.1.1.3
8               1.3.6.1.2.1.1.3
9               1.3.6.1.2.1.1.3
10              1.3.6.1.2.1.1.3
11              1.3.6.1.2.1.1.3
12              1.3.6.1.2.1.1.3
13              1.3.6.1.2.1.1.3
14              1.3.6.1.2.1.1.3
15              1.3.6.1.2.1.1.3
16              1.3.6.1.2.1.1.3
17              1.3.6.1.2.1.1.3
18              1.3.6.1.2.1.1.3
19              1.3.6.1.2.1.1.3
20              1.3.6.1.2.1.1.3
21              1.3.6.1.2.1.1.3
22              1.3.6.1.2.1.1.3
Force10#
```

Figure 123 show rmon alarms brief Command Example

show rmon events

Display the contents of RMON Event Table.

Syntax **show rmon events** [*index*] [**brief**]

Parameters

index	(OPTIONAL) Enter the table index number to display just that entry.
brief	(OPTIONAL) Enter the keyword **brief** to display the RMON Event Table in an easy-to-read format.

Defaults No default behavior

Command Modes EXEC

Command History

Version 6.1.1.0	Introduced

Example 1

```
Force10#show rmon event 1
RMON event entry 1
    description: 1
    event type: LOG and SNMP TRAP.
    event community: public
    event last time sent: none
    event owner: 1
    event status: OK
Force10#
```

Figure 124 show rmon event *index* Command Example

Example 2

```
Force10#show rmon event br
index           description
--------------------------------------------------------------------------
1               1
2               2
3               3
4               4
5               5
6               6
7               7
8               8
9               9
10              10
11              11
12              12
13              13
14              14
15              15
16              16
17              17
18              18
19              19
20              20
21              21
22              22
Force10#
```

Figure 125 show rmon event brief Command Example

show rmon hc-alarm

Display the contents of RMON High-Capacity Alarm Table.

Syntax **show rmon hc-alarm** [*index*] [**brief**]

Parameters

index	(OPTIONAL) Enter the table index number to display just that entry.
brief	(OPTIONAL) Enter the keyword **brief** to display the RMON High-Capacity Alarm Table in an easy-to-read format.

Defaults No default behavior

Command Modes EXEC

Command History

Version 6.1.1.0	Introduced

Example 1

```
Force10#show rmon hc-alarm brief
index           SNMP OID
----------------------------------------------------------------------
1               1.3.6.1.2.1.1.3
2               1.3.6.1.2.1.1.3
3               1.3.6.1.2.1.1.3
4               1.3.6.1.2.1.1.3
5               1.3.6.1.2.1.1.3
Force10#
```

Figure 126 show rmon hc-alarm brief Command Example

Example 2

```
Force10#show rmon hc-alarm 1
RMON high-capacity alarm entry 1
    object: 1.3.6.1.2.1.1.3
    sample interval: 5
    sample type: absolute value.
    value: 185638
    alarm type: rising or falling alarm.
    alarm rising threshold value: positive.
    rising threshold: 1001, RMON event index: 1
    alarm falling threshold value: positive.
    falling threshold: 999, RMON event index: 6
    alarm sampling failed 0 times.
    alarm owner: 1
    alarm storage type: non-volatile.
    alarm status: OK
Force10#
```

Figure 127 show rmon hc-alarm *index* Command Example

show rmon history

Display the contents of the RMON Ethernet History table.

Syntax **show rmon history** [*index*] [**brief**]

Parameters

index	(OPTIONAL) Enter the table index number to display just that entry.
brief	(OPTIONAL) Enter the keyword **brief** to display the RMON Ethernet History table in an easy-to-read format.

Defaults No default behavior

Command Modes EXEC

Command History

Version 6.1.1.0	Introduced

Example 1

```
Force10#show rmon history 6001
RMON history control entry 6001
    interface: ifIndex.100974631 GigabitEthernet 2/0
    bucket requested: 1
    bucket granted: 1
    sampling interval: 5 sec
    owner: 1
    status: OK
Force10#
```

Figure 128 show rmon history *index* Command Example

Example 2

```
Force10#show rmon history brief
index           ifIndex         interface
------------------------------------------------------------------
-
6001            100974631       GigabitEthernet 2/0
6002            100974631       GigabitEthernet 2/0
6003            101236775       GigabitEthernet 2/1
6004            101236775       GigabitEthernet 2/1
9001            134529054       GigabitEthernet 3/0
9002            134529054       GigabitEthernet 3/0
9003            134791198       GigabitEthernet 3/1
9004            134791198       GigabitEthernet 3/1
Force10#
```

Figure 129 show rmon history brief Command Example

show rmon log

Display the contents of RMON Log Table.

Syntax **show rmon log** [*index*] [**brief**]

Parameters

index	(OPTIONAL) Enter the log index number to display just that entry.
brief	(OPTIONAL) Enter the keyword **brief** to display the RMON Log Table in an easy-to-read format.

Defaults No default behavior

Command Modes EXEC

Command History

Version 6.1.1.0	Introduced

Example 1

```
Force10#show rmon log 2
RMON log entry, alarm table index 2, log index 1
    log time: 14638 (THU AUG 12 22:10:40 2004)
    description: 2
Force10#
```

Figure 130 show rmon log *index* Command Example

Example 2

```
Force10#show rmon log br
eventIndex      description
--------------------------------------------------------------------------
-
2               2
4               4
Force10#
```

Figure 131 show rmon log brief Command Example

Usage Information The log table has a maximum of 500 entries. If the log exceeds that maximum, the oldest log entry is purged to allow room for the new entry.

show rmon statistics

Display the contents of RMON Ethernet Statistics table.

Syntax **show rmon statistics** [*index*] [**brief**]

Parameters

index	(OPTIONAL) Enter the index number to display just that entry.
brief	(OPTIONAL) Enter the keyword **brief** to display the RMON Ethernet Statistics table in an easy-to-read format.

Defaults No default behavior

Command Modes EXEC

Command History

Version 6.1.1.0	Introduced

Example 1

```
Force10#show rmon statistics 6001
RMON statistics entry 6001
    interface: ifIndex.100974631 GigabitEthernet 2/0
    packets dropped: 0
    bytes received: 0
    packets received: 0
    broadcast packets: 0
    multicast packets: 0
    CRC error: 0
    under-size packets: 0
    over-size packets: 0
    fragment errors: 0
    jabber errors: 0
    collision: 0
    64bytes packets: 0
    65-127 bytes packets: 0
    128-255 bytes packets: 0
    256-511 bytes packets: 0
    512-1023 bytes packets: 0
    1024-1518 bytes packets: 0
    owner: 1
    status: OK
    <high-capacity data>
    HC packets received overflow: 0
    HC packets received: 0
    HC bytes received overflow: 0
    HC bytes received: 0
    HC 64bytes packets overflow: 0
    HC 64bytes packets: 0
    HC 65-127 bytes packets overflow: 0
    HC 65-127 bytes packets: 0
    HC 128-255 bytes packets overflow: 0
    HC 128-255 bytes packets: 0
    HC 256-511 bytes packets overflow: 0
    HC 256-511 bytes packets: 0
    HC 512-1023 bytes packets overflow: 0
    HC 512-1023 bytes packets: 0
    HC 1024-1518 bytes packets overflow: 0
    HC 1024-1518 bytes packets: 0
Force10#
```

Figure 132 show rmon statistics *index* Command Example

Example 2

```
Force10#show rmon statistics br
index           ifIndex         interface
------------------------------------------------------------------
6001            100974631       GigabitEthernet 2/0
6002            100974631       GigabitEthernet 2/0
6003            101236775       GigabitEthernet 2/1
6004            101236775       GigabitEthernet 2/1
9001            134529054       GigabitEthernet 3/0
9002            134529054       GigabitEthernet 3/0
9003            134791198       GigabitEthernet 3/1
9004            134791198       GigabitEthernet 3/1
Force10#
```

Figure 133 show rmon statistics brief Command Example

Chapter 13 High Availability Commands

High Availability (HA) features in FTOS supports RPM 1 + 1 redundancy. The Primary RPM performs all routing and control operations while the Secondary RPM is on-line and monitoring the Primary RPM. FTOS provides RPM failover with configuration synchronization to minimize recovery time in the event of an RPM failure.

The HA commands available in FTOS are:

- redundancy auto-failover-limit on page 367
- redundancy disable-auto-reboot on page 368
- redundancy force-failover on page 369
- redundancy primary on page 370
- redundancy reset-counter on page 370
- redundancy sfm standby on page 370
- redundancy synchronize on page 371
- show redundancy on page 372

redundancy auto-failover-limit

Specify an auto-failover limit for RPMs. When an non-recoverable fatal error is detected, an automatic RPM failover occurs. This command does not affect user-initiated (manual) failovers.

Syntax **redundancy auto-failover-limit** [**count** *number* [**period** *minutes*] | **period** *minutes*]]

To disable the auto failover limit control, enter **no redundancy auto-failover-limit**.

Parameters

count *number*	Enter the number of times the RPMs can automatically failover within the period defined in the period parameter. Range: 2 to 10 Default: 3
period *minutes*	Enter a duration in which to allow a number of automatic failovers (limited to the number defined in the count parameter). Range: 5 to 9000 minutes Default: 60 minutes

Defaults Count: 3 Period: 60 minutes

Command Modes CONFIGURATION

Usage Information If auto failover is disabled, enter the **redundancy auto-failover-limit** (without any parameters) to set auto failover to the default parameters (Count 3, Period 60 minutes).Use the show redundancy command to view the redundancy status.

When you change one or both of the optional parameters, FTOS checks that the interval between auto failovers is more than five (5) minutes. If the interval is less, FTOS returns a configuration error message.

redundancy disable-auto-reboot

Prevent the E-Series from auto-rebooting the failed module.

Syntax **redundancy disable-auto-reboot rpm**

To return to the default, enter **no redundancy disable-auto-reboot rpm**.

Parameters

rpm	Enter the keyword **RPM** to disable auto-reboot of the failed RPM.

Defaults Disabled (that is, the failed module is automatically rebooted).

Command Modes CONFIGURATION

Usage Information Enabling this command will keep the failed RPM in the failed state. If there are two RPMs in the system, enabling this command prevents the failed RPM from becoming a working Standby RPM. If there is only one RPM in the system, the failed RPM will not recover—this will effect the system.

redundancy force-failover

Force the secondary RPM to become primary RPM or force an SFM (on an E-Series chassis only) to become the standby SFM. This command can also be used to upgrade the software on one RPM from the other when the other has been loaded with the upgraded software.

Syntax **redundancy force-failover rpm** | **sfm** [*slot-number*]

Parameters

rpm	Enter the keyword **rpm** to force the secondary RPM to become the primary RPM.
sfm *slot-number*	**E-Series Only**—Enter the keyword **sfm** followed by the SFM slot number. Range: 0 to 8.

Defaults Not configured.

Command Modes EXEC privilege

Usage Information This command can be used to provide a hitless or warm upgrade. A hitless upgrade means that a software upgrade does not require a reboot of the line cards. A warm upgrade means that a software upgrade requires a reset of the line cards and SFMs. A warm upgrade is possible for major releases and lower, while a hitless upgrade can only support patch releases.

You load the software upgrade on one RPM and then issue this command with the **rpm** keyword to move the software to the other RPM. The system senses the condition and provides a series of prompts appropriate to that context, as shown in the following example:

Note: On C-Series, this command could affect traffic (even during hot-failover) since the switch fabric present on the RPM is taken down during the failover.

Example

```
Force10#redundancy force-failover rpm
Peer RPM's SW version is different but HA compatible.
Failover can be done by warm or hitless upgrade.
All linecards will be reset during warm upgrade.

Specify hitless upgrade or warm upgrade [confirm hitless/warm]:hitless
Proceed with warm upgrade [confirm yes/no]:
```

Figure 134 redundancy force-failover rpm Command Example

Example

```
Force10#redundancy force-failover sfm 0
%TSM-6-SFM_FAILOVER: Standby switch to SFM 8
Standby switch to SFM 0
Force10#
```

Figure 135 redundancy force-failover sfm (E-Series Only) Command Example

redundancy primary

Set an RPM as the primary RPM.

Syntax **redundancy primary** [**rpm0** | **rpm1**]

To delete a configuration, enter **no redundancy primary**.

Parameters

rpm0	Enter the keyword **rpm0** to set the RPM in slot R0 as the primary RPM.
rpm1	Enter the keyword **rpm1** to set the RPM in slot R1 as the primary RPM.

Defaults The RPM in slot R0 is Primary RPM.

Command Modes CONFIGURATION

redundancy reset-counter

Reset failover counter and timestamp information displayed in the show redundancy command output.

Syntax **redundancy reset-counter**

Defaults Not configured

Command Modes EXEC privilege

redundancy sfm standby

C-Series	✓
E-Series	No

Set the secondary SFM to standby.

Syntax **redundancy sfm standby**

To return the SFM to online, use the **no redundancy sfm standby** command.

Defaults Online

Command Modes CONFIGURATION

Command History

Version 7.5.1.0	Introduced

Usage Information When a secondary RPM with logical SFM is inserted or removed, the system must add or remove the backplane links to the switch fabric trunk. To avoid traffic disruption, use this command when the secondary RPM is inserted. When this command is executed, the logical SFM on the standby RPM is immediately taken offline and the SFM state is set as “standby”.

Note: This command could affect traffic when taking the secondary SFM offline.

Related Commands

show sfm all	Display the SFM status
show switch links	View the switch fabric backplane or internal status..

redundancy synchronize

Manually synchronize data once between the Primary RPM and the Secondary RPM.

Syntax **redundancy synchronize** [**full** | **persistent-data** | **system-data**]

Parameters

full	Enter the keyword **full** to synchronize all data.
persistent-data	Enter the keywords **persistent-data** to synchronize the startup configuration between RPMs.
system-data	Enter the keywords **system-data** to synchronize persistent-data and the running configuration file, event log, SFM and line card states.

Defaults Not configured.

Command Modes EXEC privilege

show redundancy

View the current redundancy configuration.

Syntax **show redundancy**

Command Modes EXEC

EXEC privilege

Example

```
Force10#show redundancy

--  RPM Status  --
-------------------------------------------------
 RPM Slot ID:               1
 RPM Redundancy Role:       Primary
 RPM State:                 Active
 RPM SW Version:            7.5.1.0
 Link to Peer:              Up

--  PEER RPM Status  --
-------------------------------------------------
 RPM State:                 Standby
 RPM SW Version:            7.5.1.0

--  RPM Redundancy Configuration  --
-------------------------------------------------
 Primary RPM:               rpm0
 Auto Data Sync:            Full
 Failover Type:             Hot Failover
 Auto reboot RPM:           Enabled
 Auto failover limit:       3 times in 60 minutes

--  RPM Failover Record  --
-------------------------------------------------
 Failover Count:            1
 Last failover timestamp:   Jul 13 2007 21:25:32
 Last failover Reason:      User request

--  Last Data Block Sync Record:  --
-------------------------------------------------
  Line Card Config:         succeeded  Jul 13 2007 21:28:53
   Start-up Config:         succeeded  Jul 13 2007 21:28:53
  SFM Config State:         succeeded  Jul 13 2007 21:28:53
 Runtime Event Log:         succeeded  Jul 13 2007 21:28:53
    Running Config:         succeeded  Jul 13 2007 21:28:53
Force10#
```

Figure 136 show redundancy Command Example

Table 21 describes the information in Figure 136

Table 21 show redundancy Command Example Fields

Field	Description
RPM Status	Displays the following information: • slot number of the RPM, • whether its the Primary PRM or Standby RPM • which of the following states the RPM is in (Active, Standby, Booting, or Offline) • whether the link to the second RPM is up or down.
PEER RPM Status	Displays the state of the second RPM, if present.

Table 21 show redundancy Command Example Fields (continued)

Field	Description
RPM Redundancy Configuration	Displays the following information: • which RPM is the preferred Primary on next boot (redundancy primary command) • the data sync method configured (redundancy synchronize command). • the failover type (you cannot change this; it is software dependent) **Hot Failover** means the running configuration and routing table are applied on secondary RPM. **Fast Failover** means the running configuration is not applied on the secondary RPM till failover occurs, and the routing table on line cards is cleared during failover. • the status of auto booting the RPM (redundancy disable-auto-reboot command) • the parameter for auto failover limit control (redundancy auto-failover-limit command)
RPM Failover Record	Displays the following information: • RPM failover counter (to reset the counter, use the redundancy reset-counter command) • the time and date of the last RPM failover • the reason for the last RPM failover.
Last Data Sync Record	Displays the data sync information and the timestamp for the data sync: • Start-up Config is the contents of the startup-config file. • Line Card Config is the line card types configured and interfaces on those line cards. • Runtime Event Log is the contents of the Event log. • Running Config is the current running-config. This field only appears when you enter the command from the Primary RPM.

Chapter 14 Time Commands

Use the following commands to configure time values on the system, either using FTOS, or the hardware, or using the Network Time Protocol (NTP).

- calendar set on page 376
- clock read-calendar on page 377
- clock set on page 377
- clock summer-time date on page 378
- clock summer-time recurring on page 379
- clock timezone on page 380
- clock update-calendar on page 381
- debug ntp on page 381
- ntp authenticate on page 382
- ntp authentication-key on page 382
- ntp broadcast client on page 383
- ntp disable on page 383
- ntp multicast client on page 383
- ntp server on page 384
- ntp source on page 385
- ntp trusted-key on page 385
- ntp update-calendar on page 386
- show calendar on page 386
- show clock on page 387
- show ntp associations on page 388
- show ntp status on page 389

calendar set

Set the time and date for the E-Series hardware clock.

Syntax **calendar set** *time month day year*

Parameters

time	Enter the time in hours:minutes:seconds. For the hour variable, use the 24-hour format, for example, 17:15:00 is 5:15 pm.
month	Enter the name of one of the 12 months in English. You can enter the name of a day to change the order of the display to *time day month year*.
day	Enter the number of the day. Range: 1 to 31. You can enter the name of a month to change the order of the display to *time day month year*.
year	Enter a four-digit number as the year. Range: 1993 to 2035.

Command Modes EXEC privilege

Example

```
Force10#calendar set 08:55:00 june 18 2001
Force10#
```

Figure 137 calendar set Command Example

Usage Information You can change the order of the *month* and *day* parameters to enter the time and date as *time day month year*.

In the E-Series, the hardware clock is separate from the software and is called the calendar. This hardware clock runs continuously. After the hardware clock (the calendar) is set, the FTOS automatically updates the software clock after system bootup.You cannot delete the hardware clock (calendar).

To manually update the software with the hardware clock, use the clock read-calendar on page 377 command.

Related Commands

clock read-calendar on page 377	Set the software clock based on the hardware clock.
clock set on page 377	Set the software clock.
clock update-calendar on page 381	Set the hardware clock based on the software clock.
show clock on page 387	View clock settings.

clock read-calendar

Set the E-Series software clock from the information set in hardware clock (calendar).

Syntax **clock read-calendar**

Defaults Not configured.

Command Modes EXEC privilege

Usage Information In the E-Series, the hardware clock is separate from the software and is called the calendar. This hardware clock runs continuously. After the hardware clock (the calendar) is set, the FTOS automatically updates the software clock after system bootup.

You cannot delete this command (that is, there is not a "no" version of this command).

clock set

Set the software clock in the E-Series.

Syntax **clock set** *time month day year*

Parameters

time	Enter the time in hours:minutes:seconds. For the hour variable, use the 24-hour format, example, 17:15:00 is 5:15 pm.
month	Enter the name of one of the 12 months, in English. You can enter the number of a day and change the order of the display to *time day month year*.
day	Enter the number of the day. Range: 1 to 31. You can enter the name of a month to change the order of the display to *time month day year*.
year	Enter a four-digit number as the year. Range: 1993 to 2035.

Defaults Not configured.

Command Modes EXEC privilege

Example

```
Force10#clock set 16:20:00 19 may 2001
Force10#
```

Figure 138 clock set Command Example

Usage Information

You can change the order of the *month* and *day* parameters to enter the time and date as *time day month year*. You cannot delete the software clock.

The software clock runs only when the software is up. The clock restarts, based on the hardware clock, when the E-Series reboots.

Force10 Networks recommends that you use an outside time source, such as NTP, to ensure accurate time on the E-Series system.

Related Commands

ntp update-calendar on page 386	Set the E-Series using the NTP settings.

clock summer-time date

Set a date to switch the E-Series to a daylight savings time zone.

Syntax

clock summer-time *time-zone* **date** *start-month start-day start-year start-time end-month end-day end-year end-time* [*offset*]

To delete a daylight savings time zone configuration, enter **no clock summer-time**.

Parameters

time-zone	Enter the three-letter name for the time zone. This name is displayed in the show clock output.
start-month	Enter the name of one of the 12 months in English. You can enter the name of a day to change the order of the display to *time day month year*.
start-day	Enter the number of the day. Range: 1 to 31. You can enter the name of a month to change the order of the display to *time day month year*.
start-year	Enter a four-digit number as the year. Range: 1993 to 2035.
start-time	Enter the time in hours:minutes:seconds. For the hour variable, use the 24-hour format, example, 17:15:00 is 5:15 pm.
end-day	Enter the number of the day. Range: 1 to 31. You can enter the name of a month to change the order of the display to *time day month year*.
end-month	Enter the name of one of the 12 months in English. You can enter the name of a day to change the order of the display to *time day month year*.

end-time	Enter the time in hours:minutes:seconds. For the hour variable, use the 24-hour format, example, 17:15:00 is 5:15 pm.
end-year	Enter a four-digit number as the year. Range: 1993 to 2035.
offset	(OPTIONAL) Enter the number of minutes to add during the summer-time period. Range: 1 to1440. Default: 60 minutes

Defaults Not configured.

Command Modes CONFIGURATION

clock summer-time recurring

Set software clock to daylight savings time to start and stop on a specific day each year.

Syntax **clock summer-time** *time-zone* **recurring** [*start-week*] *start-day start-month start-time* [*end-week*] *end-day end-month end-time* [*offset*]]

To delete a daylight savings time zone configuration, enter **no clock summer-time**.

Parameters

time-zone	Enter the three-letter name for the time zone. This name is displayed in the show clock on page 387 output (Figure 140). You can enter up to eight characters.
start-week	(OPTIONAL) Enter one of the following as the week that daylight savings begins: • *week-number:* enter a number from 1-4 as the number of the week to start daylight savings time. • **first:** enter the keyword first to start daylight savings time in the first week of the month. • **last:** enter the keyword last to start daylight savings time in the last week of the month.
start-day	Enter the name of weekday that you want daylight saving time to begin. Enter the weekdays using the three letter abbreviations, for example Sun, Sat, Mon etc. Range: Sun to Sat
start-month	Enter the name of one of the 12 months in English.
start-time	Enter the time in hours:minutes:seconds. For the hour variable, use the 24-hour format, example, 17:15:00 is 5:15 pm.

end-week	(OPTIONAL) Enter the one of the following as the week that daylight savings ends: • *week-number:* enter a number from 1-4 as the number of the week to end daylight savings time. • **first:** enter the keyword first to end daylight savings time in the first week of the month. • **last:** enter the keyword last to end daylight savings time in the last week of the month.
end-day	Enter the weekday name that you want daylight saving time to end. Enter the weekdays using the three letter abbreviations, for example Sun, Sat, Mon etc. Range: Sun to Sat
end-month	Enter the name of one of the 12 months in English.
end-time	Enter the time in hours:minutes:seconds. For the hour variable, use the 24-hour format, example, 17:15:00 is 5:15 pm.
offset	(OPTIONAL) Enter the number of minutes to add during the summer-time period. Range: 1 to 1440. Default: 60 minutes.

Defaults Not configured.

Command Modes CONFIGURATION

Command History

Version 7.4.1.0	Updated the *start-day* and *end-day* options to allow for using the three-letter abbreviation of the weekday name.

clock timezone

Configure a timezone for the E-Series.

Syntax **clock timezone** *timezone-name offset*

To delete a timezone configuration, enter **no clock timezone**.

Parameters

timezone-name	Enter the name of the timezone. You cannot use spaces.
offset	Enter one of the following: • a number from 1 to 23 as the number of hours in addition to UTC for the timezone. • a minus sign (-) followed by a number from 1 to 23 as the number of hours

Default Not configured.

Command Modes CONFIGURATION

clock update-calendar

Set the E-Series hardware clock based on the software clock.

Syntax **clock update-calendar**

Defaults Not configured.

Command Modes EXEC privilege

Usage Information Use this command only if you are sure that the hardware clock is inaccurate and the software clock is correct. You cannot delete this command (that is, there is not a "no" form of this command).

Related Commands

calendar set	Set the hardware clock.

debug ntp

View Network Time Protocol (NTP) transactions and protocol messages for troubleshooting.

Syntax **debug ntp** {**adjust** | **all** | **authentication** | **events** | **loopfilter** | **packets** | **select** | **sync**}

To disable debugging of NTP transactions, use the **no debug ntp** {**adjust** | **all** | **authentication** | **events** | **loopfilter** | **packets** | **select** | **sync**} command.

Parameters

adjust	Enter the keyword **adjust** to display information on NTP clock adjustments.
all	Enter the keyword **all** to display information on all NTP transactions.
authentication	Enter the keyword **authentication** to display information on NTP authentication transactions.
events	Enter the keyword **events** to display information on NTP events.
loopfilter	Enter the keyword **loopfilter** to display information on NTP local clock frequency.
packets	Enter the keyword **packets** to display information on NTP packets.
select	Enter the keyword **select** to display information on the NTP clock selection.
sync	Enter the keyword **sync** to display information on the NTP clock synchronization.

Command Modes EXEC privilege

ntp authenticate

Enable authentication of NTP traffic between the E-Series and the NTP time serving hosts.

Syntax **ntp authenticate**

To disable NTP authentication, enter **no ntp authentication**.

Defaults Not enabled.

Command Modes CONFIGURATION

Usage Information You also must configure an authentication key for NTP traffic using the ntp authentication-key command.

Related Commands

ntp authentication-key	Configure authentication key for NTP traffic.
ntp trusted-key	Configure a key to authenticate

ntp authentication-key

Specify a key for authenticating the NTP server.

Syntax **ntp authentication-key** *number* **md5** *key*

To delete an authentication key, use the **no ntp authentication-key** *number* command.

Parameters

number	Specify a number for the authentication key. Range: 1 to 4294967295. This number must be the same as the number parameter configured in the ntp trusted-key command.
md5 *key*	Enter the keyword **md5** followed by a character string to specify that message digest key 5 (md5) algorithm and its key. MD5 is the only key type supported.

Defaults Not configured.

Command Modes CONFIGURATION

Usage Information After configuring the ntp authentication-key command, configure the ntp trusted-key command to complete NTP authentication.

Related Commands

ntp authenticate	Enables NTP authentication.
ntp trusted-key	Configure a trusted key.

ntp broadcast client

Specify the E-Series as an NTP broadcast client.

Syntax **ntp broadcast client**

To disable broadcast, enter **no ntp broadcast client**.

Defaults Disabled.

Command Modes INTERFACE

ntp disable

Prevent an interface from receiving NTP packets.

Syntax **ntp disable**

To re-enable NTP on an interface, enter **no ntp disable**.

Default Disabled (that is, if an NTP host is configured, all interfaces receive NTP packets.)

Command Modes INTERFACE

ntp multicast client

C-Series	No
E-Series	✓

Configure the E-Series to receive NTP information from the network via multicast.

Syntax **ntp multicast client** [*multicast-address*]

To disable multicast reception, use the **no ntp multicast client** [*multicast-address*] command.

Parameters

multicast-address	(OPTIONAL) Enter a multicast address. If you do not enter a multicast address, the address 224.0.1.1 is configured.

Defaults Not configured.

Command Modes INTERFACE

ntp server

Configure a NTP time serving host.

Syntax **ntp server** *ip-address* [**version** *number*] [**key** *keyid*] [**prefer**]

To delete an NTP server configuration, use the **no ntp server** *ip-address* command.

Parameters

ip-address	Enter an IP address, in dotted decimal format, of the NTP time server.
version *number*	(OPTIONAL) Enter the keyword **version** and a number to correspond to the NTP version used on the server. Range: 1 to 3
key *keyid*	(OPTIONAL) Enter the keyword **key** and a number as the NTP peer key. Range: 1 to 4294967295
prefer	(OPTIONAL) Enter the keyword **prefer** to indicate that this peer has priority over other servers.

Defaults Not configured.

Command Modes CONFIGURATION

Usage Information You can configure multiple time serving hosts (up to 250). From these time serving hosts, the FTOS will choose one NTP host with which to synchronize. Use the show ntp associations to determine which server was selected.

Since a large number of polls to NTP hosts can impact network performance, Force10 Networks recommends that you limit the number of hosts configured.

Related Commands

show ntp associations	Displays NTP servers configured and their status.

ntp source

Specify an interface's IP address to be included in the NTP packets.

Syntax **ntp source** *interface*

To delete the configuration, enter **no ntp source**.

Parameters

interface	Enter the following keywords and slot/port or number information: • For an 100/1000 Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For Loopback interfaces, enter the keyword **loopback** followed by a number from zero (0) to 16383. • For a Port Channel interface, enter the keyword **lag** followed by a number: C-Series Range: 1-128 on the C300 E-Series Range: 1 to 32 for EtherScale, 1to 255 for TeraScale • For SONET interface types, enter the keyword **sonet** followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information. • For VLAN interface, enter the keyword **vlan** followed by a number from 1 to 4094.

Defaults Not configured.

Command Modes CONFIGURATION

ntp trusted-key

Set a key to authenticate the system to which NTP will synchronize.

Syntax **ntp trusted-key** *number*

To delete the key, use the **no ntp trusted-key** *number* command.

Parameters

number	Enter a number as the trusted key ID. Range: 1 to 4294967295.

Defaults Not configured.

Command Modes CONFIGURATION

Usage Information

The *number* parameter in the ntp trusted-key command must be the same number as the *number* parameter in the ntp authentication-key command. If you change the ntp authentication-key command, you must also change the ntp trusted-key command.

Related Commands

ntp authentication-key	Set an authentication key for NTP.
ntp authenticate	Enable the NTP authentication parameters you set.

ntp update-calendar

Configure the FTOS to update the calendar (the hardware clock) with the NTP-derived time.

Syntax **ntp update-calendar** [*minutes*]

To return to default setting, enter **no ntp update-calendar**.

Parameters

minutes	(OPTIONAL) Enter the number of minutes between updates from NTP to the hardware clock. Range: 1 to 1440. Default: 60 minutes.

Defaults Not enabled.

Command Modes CONFIGURATION

show calendar

View the current date and time based on the E-Series hardware clock.

Syntax **show calendar**

Command Modes EXEC

EXEC privilege

Example

```
Force10#show calendar
16:33:30 UTC Tue Jun 26 2001
Force10#
```

Figure 139 show calendar Command Example

Related Commands

show clock	View the time and date from the E-Series software clock.

show clock

View the current clock settings.

Syntax **show clock** [**detail**]

Parameters

detail	(OPTIONAL) Enter the keyword **detail** to view the source information of the clock.

Command Modes EXEC

EXEC privilege

Example

```
Force10#show clock
11:05:56.949 UTC Thu Oct 25 2001
Force10#
```

Figure 140 show clock Command Example

Related Commands

show calendar	View the time and date from the E-Series hardware clock.

show ntp associations

View the NTP master and peers.

Syntax **show ntp associations**

Command Modes EXEC

EXEC privilege

Example

```
Force10#show ntp associations
remote         ref clock      st when poll reach   delay   offset    disp
==============================================================================
 10.10.120.5     0.0.0.0         16    -  256    0     0.00    0.000 16000.0
*172.16.1.33     127.127.1.0     11    6   16  377    -0.08  -1499.9  104.16
 172.31.1.33     0.0.0.0         16    -  256    0     0.00    0.000 16000.0
 192.200.0.2     0.0.0.0         16    -  256    0     0.00    0.000 16000.0
* master (synced), # master (unsynced), + selected, - candidate
Force10#
```

Figure 141 show ntp associations Command Example

Table 22 describes the information in the **show ntp associations** example.

Table 22 show ntp associations Command Fields

Field	Description
(none)	One or more of the following symbols could be displayed: • * means synchronized to this peer • # means almost synchronized to this peer • + means the peer was selected for possible synchronization • - means the peer is a candidate for selection • ~ means the peer is statically configured
remote	Displays the remote IP address of the NTP peer.
ref clock	Displays the IP address of the remote peer's reference clock.
st	Displays the peer's stratum, that is, the number of hops away from the external time source. A 16 in this column means the NTP peer cannot reach the time source.
when	Displays the last time the E-Series received an NTP packet.
poll	Displays the polling interval (in seconds).
reach	Displays the reachability to the peer (in octal bitstream).
delay	Displays the time interval or delay for a packet to complete a round-trip to the NTP time source (in milliseconds).
offset	Displays the relative time of the NTP peer's clock to the E-Series clock (in milliseconds).
disp	Displays the dispersion.

Related Commands		
	show ntp status	Display current NTP status.

show ntp status

View the current NTP status.

Syntax **show ntp status**

Command Modes EXEC

EXEC privilege

Example

```
Force10#sh ntp sta
Clock is synchronized, stratum 2, reference is 100.10.10.10
frequency is -32.000 ppm, stability is 15.156 ppm, precision is 4294967290
reference time is BC242FD5.C7C5C000 (10:15:49.780 UTC Mon Jan 10 2000)
clock offset is clock offset msec, root delay is 0.01656 sec
root dispersion is 0.39694 sec, peer dispersion is peer dispersion msec
peer mode is client
Force10#
```

Figure 142 show ntp status Command Example

Table 23 describes the information found in Figure 142.

Table 23 show ntp status Command Example Information

Field	Description
“Clock is ...”	States whether or not the E-Series clock is synchronized, which NTP stratum the system is assigned and the IP address of the NTP peer.
“frequency is ...”	Displays the frequency (in ppm), stability (in ppm) and precision (in Hertz) of the clock in this system.
“reference time is ...”	Displays the reference time stamp.
“clock offset is ...”	Displays the system offset to the synchronized peer and the time delay on the path to the NTP root clock.
“root dispersion is ...”	Displays the root and path dispersion.
“peer mode is ...”	State what NTP mode the E-Series is. This should be client mode.

Related Commands	show ntp associations	View information on NTP master and peer configurations.

Chapter 15 Security Commands

This section contains the FTOS security commands.

- AAA Accounting on page 391
- Authorization and Privilege on page 394
- Authentication and Password on page 396
- RADIUS on page 407
- TACACS+ on page 412
- Port Authentication (802.1x) on page 415
- SSH Server and SCP on page 421
- Trace List on page 434

AAA Accounting

AAA Accounting enables tracking of services that users are accessing and the amount of network resources being consumed by those services.When AAA Accounting is enabled, the network server reports user activity to the TACACS+ security server in the form of accounting records. Each accounting record is comprised of accounting AV pairs and is stored on the access control server.

As with authentication and authorization, you must configure AAA Accounting by defining named list of accounting methods, and then apply that list to various interfaces. The commands are:

- aaa accounting on page 392
- aaa accounting suppress on page 393
- show accounting on page 393

aaa accounting

Enable AAA Accounting and create a record for monitoring the accounting function.

Syntax

aaa accounting {**system** | **exec** | **command** *level*} {*name* | *default*}{**start-stop** | **wait-start** | **stop-only**} {**tacacs+**}

To disable AAA Accounting, use the **no aaa accounting** {**system** | **exec** | **command** *level*} {*name* | *default*}{**start-stop** | **wait-start** | **stop-only**} {**tacacs+**} command.

Parameters

system	Enter the keyword **system** to enable System Accounting.
exec	Enter the keyword **exec** to enable Exec Accounting.
command *level*	Enter the keyword **command** followed by the command privilege level for account monitoring.
name | *default*	Enter one of the following: • *a* user defined name of a list of accounting methods • *default* is a default name of a list of accounting methods
start-stop	Enter the keyword **start-stop** to send a start accounting notice at the beginning of the requested event and a stop accounting notice at the end of the event.
wait-start	Enter the keyword **wait-start** to ensure TACACS+ security server acknowledges the start notice before granting the user's process request.
stop-only	Enter the keyword **stop-only** to instruct the TACACS+ security server to send a stop record accounting notice at the end of the requested user process.
tacacs+	Enter the keyword **tacacs+** to use TACACS+ data for accounting.

Defaults

No default configuration or behavior

Command Modes

CONFIGURATION

Command History

Version 6.3.1.0	Introduced

Example

```
Force10 (config)# aaa accounting default exec start-stop tacacs+
Force10 (config)# aaa accounting command 15 start-stop tacacs+

Force10 (config)#
```

Usage Information

In the example above, TACACS+ accounting is used to track all usage of EXEC command and commands on privilege level 15.

Related Commands

enable password	Change the password for the enable command.
login authentication	Enable AAA login authentication on terminal lines.
password	Create a password.
tacacs-server host	Specify a TACACS+ server host.

aaa accounting suppress

Prevent the generation of accounting records to users with user name value of NULL.

Syntax **aaa accounting suppress null-username**

To permit accounting records to users with user name value of NULL, use the **no aaa accounting suppress null-username** command

Parameters

null-username	Enter the keywords **null-username** to suppress users with user name value of NULL from receiving accounting records.

Defaults Accounting Records are issued to all users

Command Modes CONFIGURATION

Command History

Version 6.3.1.0	Introduced

Usage Information FTOS issues accounting records for all users on the system, including users whose username string, due to protocol translation, is NULL. For example, a user who comes on line with the **aaa authentication login** *method-list* **none** command is applied. Use **aaa accounting suppress** command to prevent accounting records from being generated for sessions that do not have user names associated to them.

show accounting

Displays the active accounting sessions for each online user.

Syntax **show accounting**

Defaults No default configuration or behavior

Command Modes EXEC

Command History

Version 6.3.1.0	Introduced

Example

```
Force10#show accounting
Active accounted actions on tty2, User admin Priv 1
   Task ID 1, EXEC Accounting record, 00:00:39 Elapsed, service=shell
Active accounted actions on tty3, User admin Priv 1
   Task ID 2, EXEC Accounting record, 00:00:26 Elapsed, service=shell
Force10#
```

Figure 143 show accounting command

Usage Information This command steps through all active sessions and then displays the accounting records for the active account functions.

Authorization and Privilege

You can set authorization and privilege levels with the following commands:

- aaa authorization on page 394
- privilege level (CONFIGURATION mode) on page 395
- privilege level (LINE mode) on page 395

aaa authorization

Set parameters that restrict (or permit) a user's network access.

Syntax **aaa authorization** {**commands** | **config-commands** | {**exec** *name* | *default*}} {**if-authenticated** | **local** | **none** | **radius** | **tacacs+**}

Parameters

commands	Enter the key word **commands** to access the EXEC (shell) commands.
config-commands	Enter the key word **config-commands** to access the CONFIGURATION mode commands.
exec	Enter the keyword **exec** followed by either: • *a* user defined name of a list of authorization methods • *default* is a default name of a list of authorization methods
command *level*	Enter the keyword **command** and the command level to designate network access.
if-authenticated | **local** | **none** | **radius** | **tacacs+**	Enter one of the following keywords for authorization. • **if-authenticated** Succeed if user is authenticated • **local** Use local database • **none** No authorization (always succeed) • **radius** Use Radius data for authorization • **tacacs+** Use TACACS+ data for authorization

Defaults Not configured

Command Modes CONFIGURATION

Command History

Version 7.5.1.0	Added **config-command** option
Version 6.1.1.0	Added support for Radius

privilege level (CONFIGURATION mode)

Change the access or privilege level of one or more commands.

Syntax **privilege** *mode* {**level** *level command* | **reset** *command*}

To delete access to a level and command, use the **no privilege** *mode* **level** *level command* command.

Parameters

mode	Enter one of the following keywords as the mode for which you are controlling access: • **configure** for the CONFIGURATION mode • **exec** for the EXEC mode • **interface** for the INTERFACE modes • **line** for the LINE mode • **route-map** for the ROUTE-MAP • **router** for the ROUTER OSPF, ROUTER RIP, ROUTER ISIS and ROUTER BGP modes.
level *level*	Enter the keyword **level** followed by a number for the access level. Range: 0 to 15. Level 1 is the EXEC mode and Level 15 allows access to all CLI modes and commands.
reset	Enter the keyword **reset** to return the security level to the default setting.
command	Enter the command's keywords to assign the command to a certain access level. You can enter one or all of the keywords

Defaults Not configured.

Command Modes CONFIGURATION

Usage Information Use the enable password command to define a password for the level to which you are assigning privilege or access.

privilege level (LINE mode)

Change the access level for users on the terminal lines.

Syntax **privilege level** *level*

To delete access to a terminal line, use the **no privilege level** *level* command.

Parameters		
	level *level*	Enter the keyword **level** followed by a number for the access level. Range: 0 to 15. Level 1 is the EXEC mode and Level 15 allows access to all CLI modes.

Defaults *level* = 15

Command Modes LINE

Authentication and Password

Authentication and Password includes the following commands.

- aaa authentication enable on page 396
- aaa authentication login on page 397
- access-class on page 399
- enable password on page 399
- enable restricted on page 400
- enable secret on page 401
- login authentication on page 402
- password on page 402
- password-attributes on page 403
- privilege level (CONFIGURATION mode) on page 395
- privilege level (LINE mode) on page 395
- service password-encryption on page 404
- show privilege on page 405
- show users on page 405
- timeout login response on page 406
- username on page 406

aaa authentication enable

Configure AAA Authentication methods as default at log in.

Syntax **aaa authentication enable** {**default** | *method-list-name*} *method* [... *method2*]

To return to the default setting, use the **no aaa authentication enable** {**default** | *method-list-name*} *method* [... *method2*] command.

Parameters

default	Enter the keyword **default** followed by the listed authentication methods (that follow this argument) as the default list of methods used at log in. Default: **default enable**
method-list-name	Enter a text string (up to 16 characters long) to name the list of enabled authentication methods activated at log in.
method	Enter one of the following methods: • **enable** - use the password defined by the enable password command in the CONFIGURATION mode. • **line** - use the password defined by the password command in the LINE mode. • **none** - no authentication. • **radius** - use the RADIUS server(s) configured with the radius-server host command. • **tacacs+** - use the TACACS+ server(s) configured with the tacacs-server host command.
... method2	(OPTIONAL) Enter up to two additional methods. In the event of a "no response" from the first method, FTOS applies the next configured method (up to two configured methods)

Defaults **default enable**

Command Modes CONFIGURATION

Command History

Version 6.2.1.1	Introduced

Usage Information Methods configured with the aaa authentication enable command are evaluated in the order they are configured. If users encounter an error with the first method listed, FTOS applies the next method configured *without* prompting for the password. FTOS *does not* prompt for a password before moving onto the next configured method.

Related Commands

enable password	Change the password for the enable command.
login authentication	Enable AAA login authentication on terminal lines.
password	Create a password.
radius-server host	Specify a RADIUS server host.
tacacs-server host	Specify a TACACS+ server host.

aaa authentication login

Configure login authentication methods.

Syntax **aaa authentication login** {*method-list-name* | **default**} *method* [*... method4*]

To return to the default setting, use the **no aaa authentication login** {*method-list-name* | **default**} command.

Parameters

method-list-name	Enter a text string (up to 16 characters long) as the name of a user-configured method list that can be applied to different lines.
default	Enter the keyword **default** to specify that the method list specified is the default method for all terminal lines.
method	Enter one of the following methods: • **enable** - use the password defined by the enable password command in the CONFIGURATION mode. • **line** - use the password defined by the password command in the LINE mode. • **local** - use the user name/password defined by the in the local configuration. • **none** - no authentication. • **radius** - use the RADIUS server(s) configured with the radius-server host command. • **tacacs+** - use the TACACS+ server(s) configured with the tacacs-server host command.
... *method4*	(OPTIONAL) Enter up to four additional methods. In the event of a "no response" from the first method, FTOS applies the next configured method (up to four configured methods).

Default

Not configured (that is, no authentication is performed)

Command Modes

CONFIGURATION

Usage Information

Methods configured with the aaa authentication login command are evaluated in the order they are configured. If users encounter an error with the first method listed, FTOS applies the next method configured. If users fail the first method listed, no other methods are applied. The only exception is the **local** method. If the user's name is not listed in the local database, the next method is applied. If the correct user name/password combination are not entered, the user is not allowed access to the E-Series.

Note: If TACACS+ or RADIUS are configured as the first method on the Method list and a "no response" occurs, FTOS will prompt the user for a password three times before moving onto to the next configured method.

After configuring the aaa authentication login command, configure the login authentication command to enable the authentication scheme on terminal lines.

Connections to the SSH server will work with the following login mechanisms: local, radius and tacacs.

Related Commands

login authentication	Enable AAA login authentication on terminal lines.
password	Create a password.
radius-server host	Specify a RADIUS server host.
tacacs-server host	Specify a TACACS+ server host.

access-class

Restrict incoming connections to a particular IP address in an IP access control list (ACL).

Syntax **access-class** *access-list-name*

To delete a setting, use the **no access-class** command.

Parameters

access-list-name	Enter the name of an established IP Standard ACL.

Defaults Not configured.

Command Modes LINE

enable password

Change the password for the enable command.

Syntax **enable password** [**level** *level*] [*encryption-type*] *password*

To delete a password, use the **no enable password** [*encryption-type*] *password* [**level** *level*] command.

Parameters

level *level*	(OPTIONAL) Enter the keyword **level** followed by a number as the level of access. Range: 1 to 15
encryption-type	(OPTIONAL) Enter the number **7** or **0** as the encryption type. Enter a **7** followed by a text string as the hidden password. The text string must be a password that was already encrypted by a Force10 Networks router. Use this parameter only with a password that you copied from the **show running-config** file of another Force10 Networks router.
password	Enter a text string, up to 32 characters long, as the clear text password.

Defaults No password is configured. *level* = 15

Command Modes CONFIGURATION

Usage Information Use this command to define a password for a level and use the privilege level (CONFIGURATION mode) command to control access to command modes.

Caution: If you specify an encrypted password and then enter a clear text password, you cannot access the EXEC privilege mode. When a password is encrypted, you cannot decipher it.

Passwords must meet the following criteria:

- Start with a letter, not a number.
- Passwords can have a regular expression as the password. To create a password with a regular expression in it, you must use CNTL + v prior to entering regular expression. For example, to create the password `abcd]e`, you type `abcd` CNTL v `]e` and when the password is created, you do not use the CNTL + v key combination and enter `abcd]e`..

Note: The question mark (?) and the tilda (~) are not supported characters.

Related Commands

show running-config	View the current configuration.
privilege level (CONFIGURATION mode)	Control access to command modes within the E-Series.

enable restricted

Allows Force10 Networks technical support to access restricted commands.

Syntax **enable restricted** [*encryption-type*] *password*

To disallow access to restricted commands, enter **no enable restricted**.

Parameters

encryption-type	(OPTIONAL) Enter the number **7** as the encryption type. Enter **7** followed a text string as the hidden password. The text string must be a password that was already encrypted by a Force10 Networks router. Use this parameter only with a password that you copied from the **show running-config** file of another Force10 Networks router.
password	Enter a text string, up to 32 characters long, as the clear text password.

Command Modes Not configured.

Usage Information Only Force10 Networks Technical Support staff use this command.

enable secret

Change the password for the enable command.

Syntax

enable secret [**level** *level*] [*encryption-type*] *password*

To delete a password, use the **no enable secret** [*encryption-type*] *password* [**level** *level*] command.

Parameters

level *level*	(OPTIONAL) Enter the keyword **level** followed by a number as the level of access. Range: 1 to 15
encryption-type	(OPTIONAL) Enter the number **5** or **0** as the encryption type. Enter a **5** followed a text string as the hidden password. The text string must be a password that was already encrypted by a Force10 Networks router. Use this parameter only with a password that you copied from the **show running-config** file of another Force10 Networks router.
password	Enter a text string, up to 32 characters long, as the clear text password.

Defaults

No password is configured. *level* = 15

Command Modes

CONFIGURATION

Usage Information

Use this command to define a password for a level and use the privilege level (CONFIGURATION mode) command to control access to command modes.

Caution: If you specify an encrypted password and then enter a clear text password, you cannot access the EXEC privilege mode. When a password is encrypted, you cannot decipher it.

Passwords must meet the following criteria:

- Start with a letter, not a number.
- Passwords can have a regular expression as the password. To create a password with a regular expression in it, you must use CNTL + v prior to entering regular expression. For example, to create the password `abcd]e`, you type `abcd` CNTL `v ]e` and when the password is created, you do not use the CNTL + v key combination and enter `abcd]e`..

Note: The question mark (?) and the tilda (~) are not supported characters.

Related Commands

show running-config	View the current configuration.
privilege level (CONFIGURATION mode)	Control access to command modes within the E-Series.

login authentication

Enable the AAA login authentication configured on the E-Series terminal lines.

Syntax **login authentication** {*method-list-name* | **default**}

To use the local user database for login authentication, enter **no login authentication**.

Parameters

method-list-name	Enter the *list-name* to specify that method list, created in the aaa authentication login command, is applied to the terminal line.
default	Enter the keyword **default** to specify that the default method list, created in the aaa authentication login command, is applied to the terminal line.

Defaults No authentication is performed on the console lines, and local authentication is performed on the virtual terminal and auxiliary lines.

Command Modes LINE

Usage Information If you configure the aaa authentication login default command, then the login authentication default command automatically is applied to all terminal lines.

Related Commands

aaa authentication login	Select login authentication methods.

password

Specify a password for users on terminal lines.

Syntax **password** [*encryption-type*] *password*

To delete a password, use the **no password** *password* command.

Parameters

encryption-type	(OPTIONAL) Enter either zero (0) or 7 as the encryption type for the *password* entered. The options are: • 0 is the default and means the password is not encrypted and stored as clear text. • 7 means that the password is encrypted and hidden.
password	Enter a text string up to 32 characters long. The first character of the *password* must be a letter. You cannot use spaces in the password.

Defaults No password is configured.

Command Modes LINE

Usage Information FTOS prompts users for passwords when aaa authentication login *method-list-name* and login authentication *method-list-name* commands are configured.

Related Commands

login authentication	Configure an authentication method to log into the E-Series.

When assigning a command to a privilege level, the commands using those keywords are also assigned to that privilege level. For example, if you enter the following command:

```
privilege exec level 5 show interfaces
```

Only a few commands are enabled in privilege level 0.

Related Commands

enable password	Set the password for the enable command.

password-attributes

Enable the password attributes (strong password).

Syntax **password-attributes** [**min-length** *number*] [**max-retry** *number*] [**character-restriction** [**upper** *number*] [**lower** *number*] [**numeric** *number*] [**special-char** *number*]]

To return to the default, use the **no password-attributes** [**min-length** *number*] [**max-retry** *number*] [**character-restriction** [**upper** *number*] [**lower** *number*] [**numeric** *number*] [**special-char** *number*]] command.

Parameters

min-length *number*	(OPTIONAL) Enter the keyword **min-length** followed by the number of characters. Range: 0 - 32 characters
max-retry *number*	(OPTIONAL) Enter the keyword **max-retry** followed by the number of maximum password retries. Range: 0 - 16
character-restriction	(OPTIONAL) Enter the keyword **character-restriction** to indicate a character restriction for the password.
upper *number*	(OPTIONAL) Enter the keyword **upper** followed the upper number. Range: 0 - 31
lower *number*	(OPTIONAL) Enter the keyword **lower** followed the lower number. Range: 0 - 31

numeric *number*	(OPTIONAL) Enter the keyword **numeric** followed the numeric number. Range: 0 - 31
special-char *number*	(OPTIONAL) Enter the keyword **special-char** followed the number of special characters permitted. Range: 0 - 31

Defaults No default values or behavior

Command Modes CONFIGURATION

Command History

Version 7.4.1.0	Introduced

service password-encryption

Encrypt all passwords configured in FTOS.

Syntax **service password-encryption**

To store new passwords as clear text, enter **no service password-encryption**.

Defaults Enabled.

Command Modes CONFIGURATION

Caution: Encrypting passwords with this command does not provide a high level of security.
When the passwords are encrypted, you cannot return them to plain text unless you re-configure them. To remove an encrypted password, use the **no password** *password* command.

Usage Information To keep unauthorized people from viewing passwords in the E-Series configuration file, use the service password-encryption command. This command encrypts the clear-text passwords created for user name passwords, authentication key passwords, the privileged command password, and console and virtual terminal line access passwords.

To view passwords, use show running-config command.

show privilege

View your access level.

Syntax **show privilege**

Command Modes EXEC

EXEC privilege

Example

```
Force10#show privil
Current privilege level is 15
Force10#
```

Figure 144 show privilege Command Output

Related Commands

privilege level (CONFIGURATION mode)	Assign access control to different command modes.

show users

View information on all users logged into the E-Series.

Syntax **show users** [**all**]

Parameters

all	(OPTIONAL) Enter the keyword **all** to view all terminal lines in the E-Series.

Command Modes EXEC privilege

Example

```
Force10#show user
    Line            User                    Host(s)     Location
    0 console 0     admin                   idle
*   3 vty 1         admin                   idle        172.31.1.4
Force10#
```

Figure 145 show users Command Example

Table 24 describes the information in the **show users** command example.

Table 24 show users Command Example Fields

Field	Description
(untitled)	Indicates with a * which terminal line you are using.
Line	Displays the terminal lines currently in use.
User	Displays the user name of all users logged in.
Host(s)	Displays the terminal line status.
Location	Displays the IP address of the user.

Related Commands

username	Enable a user.

timeout login response

Specify how long the software will wait for login input (for example, user name and password) before timing out.

Syntax

timeout login response *seconds*

To return to the default values, enter **no timeout login response**.

Parameters

seconds	Enter a number of seconds the software will wait before logging you out. Range: 1 to 300. Default: 300 seconds.

Defaults

seconds = 300 seconds

Command Modes

LINE

Usage Information

The software measures the period of inactivity defined in this command as the period between consecutive keystrokes. For example, if your password is “password” you can enter “p” and wait 29 seconds to enter the next letter.

username

Establish an authentication system based on user names. If you do not want a specific user to enter a password, use the **nopassword** parameter.

Syntax

username *name* [**access-class** *access-list-name*] [**nopassword | password** [*encryption-type*] *password*] [**privilege** *level*]

To delete an authentication for a user, use the **no username** *name* command.

Parameters

name	Enter a text string for the name of the user up to 25 characters. You can use any character except control characters, such as the RETURN key.
access-class *access-list-name*	(OPTIONAL) Enter the keyword **access-class** followed by the name of a configured access control list (either a IP access control list or MAC access control list).
nopassword	(OPTIONAL) Enter the keyword **nopassword** to specify that the user does not enter a password.
password *password*	(OPTIONAL) Enter the keyword **password** followed by the *encryption-type* or a text string (up to 32 characters long) as the password.
encryption-type	(OPTIONAL) Enter an encryption type for the *password* entered. The options are: • 0 is the default and FTOS stores the password as clear text. • 7 to encrypt the password.
privilege *level*	(OPTIONAL) Enter the keyword **privilege** followed by a number from zero (0) to 15.

Defaults

Not configured.

Command Modes

CONFIGURATION

LINE

Usage Information

To view the defined user names, use the show running-config user command.

Related Commands

show running-config	View the current configuration.

RADIUS

Below are the RADUIS commands supported by FTOS.

- debug radius on page 408
- ip radius source-interface on page 408
- radius-server deadtime on page 409
- radius-server host on page 409
- radius-server key on page 410
- radius-server retransmit on page 411
- radius-server timeout on page 412

debug radius

View RADIUS transactions to assist with troubleshooting.

Syntax **debug radius**

To disable debugging of RADIUS, enter **no debug radius**.

Defaults Disabled.

Command Modes EXEC privilege

ip radius source-interface

Specify an interface's IP address as the source IP address for RADIUS connections.

Syntax **ip radius source-interface** *interface*

To delete a source interface, enter **no ip radius source-interface**.

Parameters

interface	Enter the following keywords and slot/port or number information: • For an 100/1000 Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For a Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For Loopback interfaces, enter the keyword **loopback** followed by a number from zero (0) to 16838. • For the Null interface, enter the keywords **null 0**. • For the Port Channel interface, enter the keyword **port-channel** followed by a number: C-Series Range: 1-128 on the C300 E-Series Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale • For a SONET interface, enter the keyword **sonet** followed by the slot/port information. • For a Ten Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information. • For VLAN interface, enter the keyword **vlan** followed by a number from 1 to 4094.

Defaults Not configured.

Command Mode CONFIGURATION

radius-server deadtime

Configure a time interval during which non-responsive RADIUS servers to authentication requests are skipped.

Syntax **radius-server deadtime** *seconds*

To disable this function or return to the default value, enter **no radius-server deadtime**.

Parameters

seconds	Enter a number of seconds during which non-responsive RADIUS servers are skipped. Range: 0 to 2147483647 seconds. Default: 0 seconds.

Defaults 0 seconds

Command Modes CONFIGURATION

radius-server host

Configure a RADIUS server host.

Syntax **radius-server host** {*hostname* | *ip-address*} [**auth-port** *port-number*] [**retransmit** *retries*] [**timeout** *seconds*] [**key** [*encryption-type*] *key*]

To delete a RADIUS server host or return to the default values, use the **no radius-server host** {*hostname* | *ip-address*} [**auth-port**] [**retransmit**] [**timeout**] command.

Parameters

hostname	Enter the name of the RADIUS server host.
ip-address	Enter the IP address, in dotted decimal format, of the RADIUS server host.
auth-port *port-number*	(OPTIONAL) Enter the keyword **auth-port** followed by a number as the port number. Range: zero (0) to 65535 The default *port-number* is 1812.
retransmit *retries*	(OPTIONAL) Enter the keyword **retransmit** followed by a number as the number of attempts. This parameter overwrites the radius-server retransmit command. Range: zero (0) to 100 Default: 3 attempts

timeout *seconds*	(OPTIONAL) Enter the keyword **timeout** followed by the seconds the time interval the E-Series waits for a reply from the RADIUS server. This parameter overwrites the radius-server timeout command. Range: 0 to 1000 Default: 5 seconds
key [*encryption-type*] *key*	(OPTIONAL) Enter the keyword **key** followed by an optional encryption-type and a string up to 25 characters long as the authentication key. This authentication key is used by the RADIUS host server and the RADIUS daemon operating on this E-Series. For the encryption-type, enter either zero (0) or 7 as the encryption type for the *key* entered. The options are: • 0 is the default and means the password is not encrypted and stored as clear text. • 7 means that the password is encrypted and hidden. Configure this parameter last because leading spaces are ignored.

Defaults Not configured.

Command Modes CONFIGURATION

Usage Information Configure up to six RADIUS server hosts by using this command for each server host configured. FTOS searches for the RADIUS hosts in the order they are configured in the software.

The global default values for timeout, retransmit, and key optional parameters are applied, unless those values are specified in the radius-server host or other commands. If you configure timeout, retransmit, or key values, you must include those keywords when entering the no radius-server host command syntax to return to the global default values.

Related Commands

login authentication	Set the database to be checked when a user logs in.
radius-server key	Set a authentication key for RADIUS communications.
radius-server retransmit	Set the number of times the RADIUS server will attempt to send information.
radius-server timeout	Set the time interval before the RADIUS server times out.

radius-server key

Configure a password for all RADIUS communications between the E-Series and the RADIUS host server.

Syntax **radius-server key** [*encryption-type*] *password*

To delete a password, enter **no radius-server key**.

Parameters

encryption-type	(OPTIIONAL) Enter either zero (0) or 7 as the encryption type for the *password* entered. The options are: • 0 is the default and means the password is not encrypted and stored as clear text. • 7 means that the password is encrypted and hidden.
password	Enter a string that is the password to be exchanged between the E-Series and RADIUS servers. It can be up to 25 characters long.

Defaults Not configured.

Command Modes CONFIGURATION

Usage Information The key configured on the E-Series must match the key configured on the RADIUS server daemon.

If the key parameter in the radius-server host command is configured, the key configured with the radius-server key command is the default key for all RADIUS communications.

Related Commands

radius-server host	Configure a RADIUS host.

radius-server retransmit

Configure the number of times the E-Series attempts to connect with the configured RADIUS host server before declaring the RADIUS host server unreachable.

Syntax **radius-server retransmit** *retries*

To configure zero retransmit attempts, enter **no radius-server retransmit**. To return to the default setting, enter **radius-server retransmit 3**.

Parameters

retries	Enter a number of attempts the E-Series software tries to locate a RADIUS server. Range: zero (0) to 100. Default: 3 retries.

Defaults 3 retries

Command Modes CONFIGURATION

Related Commands

radius-server host	Configure a RADIUS host.

radius-server timeout

Configure the amount of time the RADIUS client (the E-Series) waits for a RADIUS host server to reply to a request.

Syntax **radius-server timeout** *seconds*

To return to the default value, enter **no radius-server timeout**.

Parameters

seconds	Enter the number of seconds between an unsuccessful attempt and the FTOS times out. Range: zero (0) to 1000 seconds. Default: 5 seconds.

Defaults 5 seconds

Command Modes CONFIGURATION

Related Commands

radius-server host	Configure a RADIUS host.

TACACS+

FTOS supports TACACS+ as an alternate method for login authentication.

- debug tacacs+ on page 412
- ip tacacs source-interface on page 413
- tacacs-server host on page 413
- tacacs-server key on page 414

debug tacacs+

View TACACS+ transactions to assist with troubleshooting.

Syntax **debug tacacs+**

To disable debugging of TACACS+, enter **no debug tacacs+**.

Defaults Disabled.

Command Modes EXEC privilege

ip tacacs source-interface

Specify an interface's IP address as the source IP address for TACACS+ connections.

Syntax **ip tacacs source-interface** *interface*

To delete a source interface, enter **no ip tacacs source-interface**.

Parameters

interface	Enter the following keywords and slot/port or number information: • For an 100/1000 Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For a Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For Loopback interfaces, enter the keyword **loopback** followed by a number from zero (0) to 16838. • For the Null interface, enter the keywords **null 0**. • For the Port Channel interface, enter the keyword **port-channel** followed by a number: C-Series Range: 1-128 on the C300 E-Series Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale • For a SONET interface, enter the keyword **sonet** followed by the slot/port information. • For a Ten Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information. • For VLAN interface, enter the keyword **vlan** followed by a number from 1 to 4094.

Defaults Not configured.

Command Mode CONFIGURATION

tacacs-server host

Specify a TACACS+ host.

Syntax **tacacs-server host** {*hostname* | *ip-address*} [**port** *number*] [**timeout** *seconds*] [**key** *key*]

To remove a TACACS+ server host, use the **no tacacs-server host** {*hostname* | *ip-address*} command.

Parameters

hostname	Enter the name of the TACACS+ server host.
ip-address	Enter the IP address, in dotted decimal format, of the TACACS+ server host.

port *number*	(OPTIONAL) Enter the keyword **port** followed by a number as the port to be used by the TACACS+ server. Range: zero (0) to 65535 Default: 49
timeout *seconds*	(OPTIONAL) Enter the keyword **timeout** followed by the number of seconds the E-Series waits for a reply from the TACACS+ server. Range: 0 to 1000 Default: 10 seconds
key *key*	(OPTIONAL) Enter the keyword **key** followed by a string up to 127 characters long as the authentication key. This authentication key must match the key specified in the tacacs-server key for the TACACS+ daemon. Configure this parameter last because leading spaces are ignored.

Defaults Not configured.

Command Modes CONFIGURATION

Usage Information To list multiple TACACS+ servers to be used by the aaa authentication login command, configure this command multiple times.

If you are not configuring the E-Series as a TACACS+ server, you do not need to configure the port, timeout and key optional parameters. If you do not configure a key, the key assigned in the tacacs-server key command is used.

Related Commands

aaa authentication login	Specify the login authentication method.
tacacs-server key	Configure a TACACS+ key for the TACACS server.

tacacs-server key

Configure a key for communication between a TACACS+ server and client.

Syntax **tacacs-server key** *key*

To delete a key, use the **no tacacs-server key** *key*

Parameters

key	Enter a text string, up to 127 characters long, as the clear text password. Leading spaces are ignored.

Defaults Not configured.

Command Modes CONFIGURATION

Usage Information The key configured with this command must match the key configured on the TACACS+ daemon.

Port Authentication (802.1x)

An authentication server must authenticate a client connected to an 802.1x switch port. Until the authentication, only EAPOL (Extensible Authentication Protocol over LAN) traffic is allowed through the port to which a client is connected. Once authentication is successful, normal traffic passes through the port.

FTOS supports RADIUS and Active Directory environments using 802.1x Port Authentication.

Important Points to Remember

FTOS limits network access for certain users by using VLAN assignments. 802.1x with VLAN assignment has these characteristics when configured on the switch and the RADIUS server.

- 802.1x is not supported on the LAG or the channel members of a LAG.
- If no VLAN is supplied by the RADIUS server or if 802.1x authorization is disabled, the port is configured in its access VLAN after successful authentication.
- If 802.1x authorization is enabled but the VLAN information from the RADIUS server is not valid, the port returns to the unauthorized state and remains in the configured access VLAN. This prevents ports from appearing unexpectedly in an inappropriate VLAN due to a configuration error. Configuration errors create an entry in Syslog.
- If 802.1x authorization is enabled and all information from the RADIUS server is valid, the port is placed in the specified VLAN after authentication.
- If port security is enabled on an 802.1x port with VLAN assignment, the port is placed in the RADIUS server assigned VLAN.
- If 802.1x is disabled on the port, it is returned to the configured access VLAN.
- When the port is in the force authorized, force unauthorized, unauthorized, or shutdown state, it is placed in the configured access VLAN.
- If an 802.1x port is authenticated and put in the RADIUS server assigned VLAN, any change to the port access VLAN configuration will not take effect.
- The 802.1x with VLAN assignment feature is not supported on trunk ports, dynamic ports, or with dynamic-access port assignment through a VLAN membership.

The 802.1x Port Authentication commands included are:

- dot1x authentication (Configuration) on page 416
- dot1x authentication (Interface) on page 416
- dot1x auth-server on page 417
- dot1x max-eap-req on page 417

- dot1x port-contol on page 418
- dot1x quiet-period on page 418
- dot1x reauthentication on page 419
- dot1x reauth-max on page 419
- dot1x server-timeout on page 420
- dot1x supplicant-timeout on page 420
- dot1x tx-period on page 421

dot1x authentication (Configuration)

Enable dot1x globally; dot1x must be enabled both globally and at the interface level.

Syntax **dot1x authentication**

To disable dot1x on an globally, use the **no dot1x authentication** command.

Defaults Disabled

Command Modes CONFIGURATION

Command History

Version 7.4.1.0	Introduced

Related Commands

dot1x authentication (Interface)	Enable dot1x on an interface

dot1x authentication (Interface)

Enable dot1x on an interface; dot1x must be enabled both globally and at the interface level.

Syntax **dot1x authentication**

To disable dot1x on an interface, use the **no dot1x authentication** command.

Defaults Disabled

Command Modes INTERFACE

Command History

Version 7.4.1.0	Introduced

Related Commands		
	dot1x authentication (Configuration)	Enable dot1x globally

dot1x auth-server

Configure the type of authentication server.

Syntax **dot1x auth-server radius**

Parameters None.

Defaults None.

Command Modes CONFIGURATION

Command History		
	Version 4.2.1.0	Introduced

dot1x max-eap-req

Configure the maximum number of times an EAP (Extensive Authentication Protocol) request is transmitted before the session times out.

Syntax **dot1x max-eap-req** *number*

To return to the default, use the **no dot1x max-eap-req** command.

Parameters		
	number	Enter the number of times an EAP request is transmitted before a session time-out. Range: 1 to 10 Default: 2

Defaults 2

Command Modes INTERFACE

Command History		
	Version 4.2.1.0	Introduced

Related Commands		
	interface range	Configure a range of interfaces

dot1x port-contol

Enable port-control on an interface.

Syntax **dot1x port-control** {**force-authorized** | **auto** | **force-unauthorized**}

Parameters

force-authorized	Enter the keyword **force-authorized** to forcibly authorize a port.
auto	Enter the keyword **auto** to authorize a port based on the 802.1x operation result.
force-unauthorized	Enter the keyword **force-unauthorized** to forcibly de-authorize a port.

Defaults None.

Command Modes INTERFACE

Command History

Version 4.2.1.0	Introduced

Usage Information The authenticator performs authentication only when port-control is set to **auto**.

dot1x quiet-period

Set the number of seconds that the authenticator remains quiet after a failed authentication with a client.

Syntax **dot1x quiet-period** *seconds*

To disable quiet time, use the **no dot1x quiet-time** command.

Parameters

seconds	Enter the number of seconds. Range: 1 to 65535 Default: 30

Defaults 30 seconds

Command Modes INTERFACE

Command History

Version 4.2.1.0	Introduced

dot1x reauthentication

Enable periodic re-authentication of the client.

Syntax **dot1x reauthentication** [**interval** *seconds*]

To disable periodic re-authentication, use the **no dot1x reauthentication** command.

Parameters

interval *seconds*	(Optional) Enter the keyword **interval** followed by the interval time, in seconds, after which re-authentication will be initiated. Range: 1 to 31536000 (1 year) Default: 3600 (1 hour)

Defaults 3600 seconds (1 hour)

Command Modes INTERFACE

Command History

Version 4.2.1.0	Introduced

Related Commands

interface range	Configure a range of interfaces

dot1x reauth-max

Configure the maximum number of times a port can re-authenticate before the port becomes unauthorized.

Syntax **dot1x reauth-max** *number*

To return to the default, use the **no dot1x reauth-max** command.

Parameters		
	number	Enter the permitted number of reauthentications. Range: 1 - 10 Default: 2

Defaults 2

Command Modes INTERFACE

Command History		
	Version 4.2.1.0	Introduced

dot1x server-timeout

Configure the amount of time after which exchanges with the server time out.

Syntax **dot1x server-timeout** *seconds*

To return to the default, use the **no dot1x server-timeout** command.

Parameters		
	seconds	Enter a time-out value in seconds. Range: 1 to 300 , where 300 is implementation dependant. Default: 30

Defaults 30 seconds

Command Modes INTERFACE

Command History		
	Version 4.2.1.0	Introduced

dot1x supplicant-timeout

Configure the amount of time after which exchanges with the supplicant time out.

Syntax **dot1x supplicant-timeout** *seconds*

To return to the default, use the **no dot1x supplicant-timeout** command.

Parameters		
	seconds	Enter a time-out value in seconds. Range: 1 to 300 , where 300 is implementation dependant. Default: 30

Defaults 30 seconds

Command Modes INTERFACE

Command History		
	Version 4.2.1.0	Introduced

dot1x tx-period

Configure the intervals at which EAPOL PDUs are trasmitted by the Authenticator PAE.

Syntax **dot1x tx-period** *seconds*

To return to the default, use the **no dot1x tx-period** command.

Parameters		
	seconds	Enter the interval time, in seconds, that EAPOL PDUs are transmitted. Range: 1 to 31536000 (1 year) Default: 30

Defaults 30 seconds

Command Modes INTERFACE

Command History		
	Version 4.2.1.0	Introduced

SSH Server and SCP

FTOS supports SSH Protocol versions 1.5 and 2.0. Secure Shell (SSH) is a protocol for secure remote login over an insecure network. SSH sessions are encrypted and use authentication.

- crypto key generate on page 422
- debug ip ssh on page 423

- ip scp topdir on page 424
- ip ssh authentication-retries on page 424
- ip ssh connection-rate-limit on page 425
- ip ssh hostbased-authentication on page 425
- ip ssh key-size on page 426
- ip ssh password-authentication on page 426
- ip ssh pub-key-file on page 427
- ip ssh rhostsfile on page 427
- ip ssh rsa-authentication (Config) on page 428
- ip ssh rsa-authentication (EXEC) on page 429
- ip ssh server on page 429
- show crypto on page 430
- show ip ssh on page 431
- show ip ssh client-pub-keys on page 432
- show ip ssh rsa-authentication on page 432
- ssh on page 433

crypto key generate

Generate keys for the SSH server.

Syntax **crypto key generate** {**rsa** | **rsa1**}

Parameters

rsa	Enter the keyword **rsa** followed by the key size to generate a SSHv2 RSA host keys. Range: 1024 to 2048 Default: 1024
rsa1	Enter the keyword **rsa1** followed by the key size to generate a SSHv1 RSA host keys. Range: 1024 to 2048 Default: 1024

Defaults Key size 1024

Command Modes CONFIGURATION

Example

```
Force10#conf
Force10(conf)#crypto key generate rsa1
Enter key size <1024-2048>. Default<1024>: 1024

Host key already exists. Do you want to replace. [y/n]  :y
FForce10(conf)#
```

Figure 146 crypto key generate rsa1 command example

Usage Information

The host keys are required for key-exchange by the SSH server. If the keys are not found when the server is enabled (**ip ssh server enable**), the keys are automatically generated.

This command requires user interaction (see Figure 146) and will generate a prompt prior to overwriting any existing host keys.

Note: Only a user with superuser permissions should generate host-keys.

Related Commands

show crypto	Display SSH host public keys

debug ip ssh

Enables collecting SSH debug information.

Syntax **debug ip ssh** {**client** | **server**}

To disable debugging, use the **no debug ip ssh** {**client** | **server**} command.

Parameters

client	Enter the keyword **client** to enable collecting debug information on the client.
server	Enter the keyword **server** to enable collecting debug information on the server.

Defaults Disabled on both client and server

Command Modes EXEC

Usage Information Debug information includes details for key-exchange, authentication, and established session for each connection.

ip scp topdir

Identify a location for files used in secure copy transfer.

Syntax **ip scp topdir** *directory*

To return to the default setting, enter **no ip scp topdir**.

Parameters

directory	Enter a directory name.

Defaults The internal flash (**flash:**) is the default directory.

Command Modes CONFIGURATION

Usage Information To configure the E-Series as a SCP server, use the ip ssh server command.

Usage Information

ip ssh server	Enable SSH and SCP server on the E-Series.

ip ssh authentication-retries

Configure the maximum number of attempts that should be used to authenticate a user.

Syntax **ip ssh authentication-retries** *1-10*

Parameters

1-10	Enter the number of maximum retries to authenticate a user. Range: 1 to 10 Default: 3

Defaults 3

Command Modes CONFIGURATION

Usage Information This command specifies the maximum number of attempts to authenticate a user on a SSH connection with the remote host for password authentication. SSH will disconnect when the number of password failures exceeds authentication-retries.

ip ssh connection-rate-limit

Configure the maximum number of incoming SSH connections per minute.

Syntax **ip ssh connection-rate-limit** *1-10*

Parameters

1-10	Enter the number of maximum number of incoming SSH connections allowed per minute. Range: 1 to 10 per minute Default: 10 per minute

Defaults 10 per minute

Command Modes CONFIGURATION

ip ssh hostbased-authentication

Enable hostbased-authentication for the SSHv2 server.

Syntax **ip ssh hostbased-authentication enable**

To disable hostbased-authentication for SSHv2 server, use the **no ip ssh hostbased-authentication enable** command.

Parameters

enable	Enter the keyword **enable** to enable hostbased-authentication for SSHv2 server.

Defaults Disable by default

Command Modes CONFIGURATION

Usage Information If this command is enabled, clients can login without a password prompt. This provides two levels of authentication:

- rhost-authentication is done with the file specified in the **ip ssh rhostfile** command
- checking client host-keys is done with the file specified in the **ip ssh pub-key-file** command

If **no ip ssh rsa-authentication enable** is executed, host-based authentication is disabled.

Note: Administrators must specify the two files (rhosts and pub-key-file) to configure host-based authentication.

Related Commands		
	ip ssh pub-key-file	Public keys of trusted hosts from a file.
	ip ssh rhostsfile	Trusted hosts and users for rhost authentication.

ip ssh key-size

Configure the size of the server-generated RSA SSHv1 key.

Syntax **ip ssh key-size** *512-869*

Parameters		
	512-869	Enter the key-size number for the server-generated RSA SSHv1 key. Range: 512 to 869 Default: 768

Defaults Key size 768

Command Modes CONFIGURATION

Usage Information The server-generated key is used for SSHv1 key-exchange.

ip ssh password-authentication

Enable password authentication for the SSH server.

Syntax **ip ssh password-authentication enable**

To disable password-authentication, use the **no ip ssh password-authentication enable**.

Parameters		
	enable	Enter the keyword **enable** to enable password-authentication for the SSH server.

Defaults Enabled by default

Command Modes CONFIGURATION

Usage Information With password authentication enabled, users can authenticate using local, RADIUS, or TACACS+ password fallback order as configured.

ip ssh pub-key-file

Specify the file to be used for host-based authentication.

Syntax **ip ssh pub-key-file** {*WORD*}

Parameters

WORD	Enter the file name for the host-based authentication.

Defaults No default behavior or values

Command Modes CONFIGURATION

Example

```
Force10#conf
Force10(conf)# ip ssh pub-key-file flash://knownhosts
Force10(conf)#
```

Usage Information This command specifies the file to be used for the host-based authentication. The file creates/overwrites the file flash://ADMIN_DIR/ssh/knownhosts and deletes the user specified file. Even though this is a global configuration command, it will not appear in the running configuration since this command needs to be run just once.

The file contains the OpenSSH compatible public keys of the host for which host-based authentication is allowed. An example known host file format:

poclab4,123.12.1.123 ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAox/
QQp8xYhzOxn07yh4VGPAoUfgKoieTHO9G4sNV+ui+DWEc3cgYAcU5Lai1MU2ODrzhCwyDNp05tK
BU3tReG1o8AxLi6+S4hyEMqHzkzBFNVqHzpQc+Rs4p2urzV0F4pRKnaXdHf3Lk4D460HZRhhVrxqe
NxPDpEnWIMPJi0ds= ashwani@poclab4

Note: For **rhostfile** and **pub-key-file**, the administrator must FTP the file to the chassis.

Related Commands

show ip ssh client-pub-keys	Display the client-public keys used for the host-based authentication.

ip ssh rhostsfile

Specify the rhost file to be used for host-based authorization.

Syntax **ip ssh rhostsfile** {*WORD*}

Parameters		
	WORD	Enter the rhost file name for the host-based authentication.

Defaults No default behavior or values

Command Modes CONFIGURATION

Example

```
Force10#conf
Force10(conf)# ip ssh rhostsfile flash://shosts
Force10(conf)#
```

Usage Information This command specifies the rhost file to be used for host-based authentication. This file creates/overwrites the file flash:/ADMIN_DIR/ssh/shosts and deletes the user specified file. Even though this is a global configuration command, it will not appear in the running configuration since this command needs to be run just once.

This file contains hostnames and usernames, for which hosts and users, rhost-authentication can be allowed.

Note: For **rhostfile** and **pub-key-file**, the administrator must FTP the file to the chassis.

ip ssh rsa-authentication (Config)

Enable RSA authentication for the SSHv2 server.

Syntax **ip ssh rsa-authentication enable**

To disable RSA authentication, use the **no ip ssh rsa-authentication enable** command.

Parameters		
	enable	Enter the keyword **enable** to enable RSA authentication for the SSHv2 server.

Defaults RSA authentication is disabled by default

Command Modes CONFIGURATION

Usage Information Enabling RSA authentication allows the user to login without being prompted for a password. In addition, the OpenSSH compatible SSHv2 RSA public key must be added to the list of authorized keys (**ip ssh rsa-authentication my-authorized-keys** *device://filename* command).

Related Commands		
	ip ssh rsa-authentication (EXEC)	Add keys for RSA authentication.

ip ssh rsa-authentication (EXEC)

Add keys for the RSA authentication.

Syntax **ip ssh rsa-authentication** {**my-authorized-keys** *WORD*}

To delete the authorized keys, use the **no ip ssh rsa-authentication** {**my-authorized-keys**} command.

Parameters		
	my-authorized-keys *WORD*	Enter the keyword **my-authorized-keys** followed by the file name of the RSA authorized-keys.

Defaults No default behavior or values

Command Modes EXEC

Usage Information If you want to login without being prompted for a password, login through RSA authentication. You need to add the SSHv2 RSA public keys to the list of authorized-keys. This command will add the specified RSA keys to the file flash://ADMIN_DIR/authorized-keys-*username* (where *username* is the user associated with this terminal).

Note: The no form of this command will delete the file flash://ADMIN_DIR/authorized-keys-*username*

Related Commands		
	show ip ssh rsa-authentication	Display RSA authorized keys.
	ip ssh rsa-authentication (Config)	Enable RSA authentication.

ip ssh server

Configure an SSH server.

Syntax **ip ssh server** {**enable** | **port** *port-number* } [**version** {**1** | **2**}]

To disable SSH server functions, enter **no ip ssh server enable** command.

Parameters

enable	Enter the key word **enable** to start the SSH server.
port *port-number*	(OPTIONAL) Enter the keyword **port** followed by the port number of the listening port of the SSH server. Range: 1 to 65535 Default: 22
[**version** {**1** | **2**}]	(OPTIONAL) Enter the keyword **version** followed by the SSH version 1 or 2 to specify only SSHv1 or SSHv2.

Defaults Default listening port is 22

Command Modes CONFIGURATION

Command History

Version 7.5.1.0	Expanded to include specifying SSHv1 or SSHv2

Usage Information This command enables the SSH server and begins listening on a port. If a port is not specified, listening is on SSH default port 22.

Example

```
Force10# conf
Force10(conf)# ip ssh server port 45
Force10(conf)# ip ssh server enable
Force10#
```

Related Commands

show ip ssh	Display the ssh information

show crypto

Display the public part of the SSH host-keys.

Syntax **show crypto** {**Key**} {**mypubkey**} {**rsa** | **rsa1**}

Parameters

Key	Enter the keyword **key** to display the host public key.
mypubkey	Enter the keyword mypubkey to display the host public key.
rsa	Enter the keyword **rsa** to display the host SSHv2 RSA public key.
rsa1	Enter the keyword **rsa1** to display the host SSHv1 RSA public key.

Defaults No default behavior or values

Command Modes EXEC

Example

```
Force10#show crypto key mypubkey rsa
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAtzkZME/
e8V8smnXR22EJGQhCMkEOkuisa+OILVoMYU1ZKGfj0W5BPCSvF/
x5ifqYFFwUzJNOcsJK7vjSsnmMhChF2YSvXlvTJ6h971FJAQlOsgd0ycpocsF+DNLKfJnx7SAjhakFQMwG
g/g78ZkDT3Ydr8KKjfSI4Bg/WS8B740=

Force10#show crypto key mypubkey rsa1
1024 35
131060015480873398953257515397249657850072206444294963674080935683088961020317226 6
798895675496676526500637962218977992760927852363883922305508181916600992813261640 8
664345774602219229518903992966334579117374224743155375050167692966027379060149443 4
050000015179864425629613385774919236081771341059533760063913083
Force10#
```

Figure 147 show crypto command examples

Usage Information

This command is useful if the remote SSH client implements Strict Host Key Checking. You can copy the host key to your list of known hosts.

Related Commands

crypto key generate	Generate SSH keys.

show ip ssh

Display information about established SSH sessions.

Syntax **show ip ssh**

Command Modes EXEC

EXEC privilege

Example

```
Force10#show ip ssh
SSH server                : enabled.
SSH server version        : v1 and v2.
Password Authentication   : enabled.
Hostbased Authentication  : disabled.
RSA          Authentication  : disabled.
   Vty          Encryption      Remote IP
   0            3DES            172.16.1.162
   1            3DES            172.16.1.162
   2            3DES            172.16.1.162Force10#
Force10
```

Figure 148 show ip ssh Command Example

Related Commands

show ip ssh client-pub-keys	Display the client-public keys.

show ip ssh client-pub-keys

Display the client public keys used in host-based authentication.

Syntax **show ip ssh client-pub-keys**

Defaults No default behavior or values

Command Modes EXEC

Example

```
Force10#show ip ssh client-pub-keys

poclab4,123.12.1.123 ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAox/
QQp8xYhzOxn07yh4VGPAoUfgKoieTHO9G4sNV+ui+DWEc3cgYAcU5Lai1MU2ODrzhCwyDNp05tKBU3tReG1
o8AxLi6+S4hyEMqHzkzBFNVqHzpQc+Rs4p2urzV0F4pRKnaXdHf3Lk4D460HZRhhVrxqeNxPDpEnWIMPJi0
ds= ashwani@poclab4

Force10#
```

Figure 149 show ip ssh client-pub-keys command

Usage Information This command displays the contents of the file flash://ADMIN_DIRssh/knownhosts

Related Commands

ip ssh pub-key-file	Configure the file name for the host-based authentication

show ip ssh rsa-authentication

Display the authorized-keys for the RSA authentication.

Syntax **show ip ssh rsa-authentication** {**my-authorized-keys**}

Parameters

my-authorized-keys	Display the RSA authorized keys.

Defaults No default behavior or values

Command Modes EXEC

Example

```
Force10#show ip ssh rsa-authentication my-authorized-keys
ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAyB17l4gFp4r2DRHIvMc1VZd0Sg5GQxRV1y1X1JOMeO6Nd0WuYyzrQMM
4qJAoBwtneOXfLBcHF3V2hcMIqaZN+CRCnw/
zCMlnCf0+qVTd1oofsea5r09kS0xTp0CNfHXZ3NuGCq9Ov33m9+U9tMwhS8vy8AVxdH4x4km3c3t5Jvc=
freedom@poclab4

Force10#
```

Figure 150 show ip ssh rsa-authentication command

Usage Information

This command displays the contents of the file flash:/ADMIN_DIR/ssh/authorized-keys.*username*.

Related Commands

ip ssh rsa-authentication (Config)	Configure the RSA authorized keys.

ssh

Open an SSH connection specifying the hostname, username, port number and version of the SSH client.

Syntax

ssh {*hostname* | *ipv4 address* | *ipv6 address*} [**-l** *username* | **-p** *port-number* | **-v** {**1** | **2**}]

Parameters

hostname	(OPTIONAL) Enter the IP address or the hostname of the remote device.
ipv4 address	(OPTIONAL) Enter the IP address in dotted decimal format A.B.C.D.
ipv6-address prefix-length	(OPTIONAL) Enter the IPv6 address in the **x:x:x:x::x** format followed by the prefix length in the **/x** format. Range: /0 to /128 **Note:** The **::** notation specifies successive hexadecimal fields of zeros
-l *username*	(OPTIONAL) Enter the keyword **-l** followed by the user name used in this SSH session. Default: The user name of the user associated with the terminal.
-p *port-number*	(OPTIONAL) Enter the keyword **-p** followed by the port number. Range: 1 to 65536 Default: 22
-v {**1** | **2**}	(OPTIONAL) Enter the keyword **-v** followed by the SSH version 1 or 2. Default: The version from the protocol negotiation

Defaults

As above.

Command Modes

EXEC privilege

Command History

Version 7.5.1.0	Added IPv6 support

Example

```
Force10#ssh 123.12.1.123 -l ashwani -p 5005 -v 2
```

Trace List

IP trace lists create an Access Control List to trace all traffic into the E-Series. This feature is useful for tracing Denial of Service (DOS) attacks.

- clear counters ip trace-group on page 434
- deny on page 435
- deny tcp on page 436
- deny udp on page 437
- ip trace-group on page 438
- ip trace-list on page 439
- permit on page 439
- permit tcp on page 440
- permit udp on page 442
- seq on page 443
- show config on page 444
- show ip accounting trace-lists on page 445

clear counters ip trace-group

C-Series	No
E-Series	✓

Erase all counters maintained for trace lists.

Syntax **clear counters ip trace-group** [*trace-list-name*]

Parameters

trace-list-name	(OPTIONAL) Enter the name of a configured trace list.

Command Modes EXEC privilege

deny

Configure a filter that drops IP packets meeting the filter criteria.

Syntax

deny {**ip |** *ip-protocol-number*} {*source mask* | **any** | **host** *ip-address*} {*destination mask* | **any** | **host** *ip-address*} [**count** [**byte**]] | **log**] [**order** *number*]

To remove this filter, you have two choices:

- use the **no seq** *sequence-number* command syntax if you know the filter's sequence number or
- use the **no deny** {**ip |** *ip-protocol-number*} {*source mask* | **any** | **host** *ip-address*} {*destination mask* | **any** | **host** *ip-address*} command.

Parameters

ip	Enter the keyword **ip** to configure a generic IP access list. The keyword **ip** specifies that the access list will deny all IP protocols.
ip-protocol-number	Enter a number from 0 to 255 to deny based on the protocol identified in the IP protocol header.
source	Enter the IP address of the network or host from which the packets were sent.
mask	(OPTIONAL) Enter a network mask in /prefix format (/x).
any	Enter the keyword **any** to specify that all routes are subject to the filter.
host *ip-address*	Enter the keyword **host** followed by the IP address to specify a host IP address.
destination	Enter the IP address of the network or host to which the packets are sent.
count	(OPTIONAL) Enter the keyword **count** to count packets processed by the filter.
bytes	(OPTIONAL) Enter the keyword **bytes** to count only bytes processed by the filter.
log	(OPTIONAL) Enter the keyword **log** to have the information kept in a Trace-list log file.
order *number*	(OPTIONAL) Enter the keyword **order** followed by a number from 0 to 7 as the order number.

Defaults

Not configured.

Command Modes

TRACE LIST

Related Commands

deny tcp	Assign a trace list filter to deny TCP packets.
deny udp	Assign a trace list filter to deny UDP packets.
ip trace-group	Create a trace list.

deny tcp

Configure a filter that drops TCP packets meeting the filter criteria.

Syntax

deny tcp {*source mask* | **any** | **host** *ip-address*} [*operator port* [*port*]] {*destination mask* | **any** | **host** *ip-address*} [*operator port* [*port*]] [**count** [**byte**]] | **log**] [**order** *number*]

To remove this filter, you have two choices:

- use the **no seq** *sequence-number* command syntax if you know the filter's sequence number or
- use the **no deny tcp** {*source mask* | **any** | **host** *ip-address*} {*destination mask* | **any** | **host** *ip-address*} command.

Parameters

source	Enter the IP address of the network or host from which the packets were sent.
mask	(OPTIONAL) Enter a network mask in /prefix format (/x).
any	Enter the keyword **any** to specify that all routes are subject to the filter.
host *ip-address*	Enter the keyword **host** followed by the IP address to specify a host IP address.
operator	(OPTIONAL) Enter one of the following logical operand: • **eq** = equal to • **neq** = not equal to • **gt** = greater than • **lt** = less than • **range** = inclusive range of ports (you must specify two ports for the *port* command parameter.)
port port	Enter the application layer port number. Enter two port numbers if using the range logical operand. Range: 0 to 65535. The following list includes some common TCP port numbers: • 23 = Telnet • 20 and 21 = FTP • 25 = SMTP • 169 = SNMP
destination	Enter the IP address of the network or host to which the packets are sent.
count	(OPTIONAL) Enter the keyword **count** to count packets processed by the filter.
byte	(OPTIONAL) Enter the keyword **byte** to count only bytes processed by the filter.
log	(OPTIONAL) Enter the keyword **log** to have the information kept in a Trace-list log file.
order *number*	(OPTIONAL) Enter the keyword **order** followed by a number from 0 to 7 as the order number.

Defaults

Not configured.

Command Modes TRACE LIST

Related Commands

deny	Assign a trace list filter to deny IP traffic.
deny udp	Assign a trace list filter to deny UDP traffic.

deny udp

Configure a filter to drop UDP packets meeting the filter criteria.

Syntax **deny udp** {*source mask* | **any** | **host** *ip-address*} [*operator port* [*port*]] {*destination mask* | **any** | **host** *ip-address*} [*operator port* [*port*]] [**count** [**byte**]] | **log**] [**order** *number*]

To remove this filter, you have two choices:

- use the **no seq** *sequence-number* command syntax if you know the filter's sequence number or
- use the **no deny udp** {*source mask* | **any** | **host** *ip-address*} {*destination mask* | **any** | **host** *ip-address*} command.

Parameters

source	Enter the IP address of the network or host from which the packets were sent.
mask	(OPTIONAL) Enter a network mask in /prefix format (/x).
any	Enter the keyword **any** to specify that all routes are subject to the filter.
host *ip-address*	Enter the keyword **host** followed by the IP address to specify a host IP address.
operator	(OPTIONAL) Enter one of the following logical operand: • **eq** = equal to • **neq** = not equal to • **gt** = greater than • **lt** = less than • **range** = inclusive range of ports
port *port*	(OPTIONAL) Enter the application layer port number. Enter two port numbers if using the **range** logical operand. Range: 0 to 65535
destination	Enter the IP address of the network or host to which the packets are sent.
mask	(OPTIONAL) Enter a network mask in /prefix format (/x).
count	(OPTIONAL) Enter the keyword **count** to count packets processed by the filter.
byte	(OPTIONAL) Enter the keyword **byte** to count only bytes

log	(OPTIONAL) Enter the keyword **log** to have the information kept in a Trace-list log file.
order *number*	(OPTIONAL) Enter the keyword **order** followed by a number from 0 to 7 as the order number.

Defaults Not configured.

Command Modes TRACE LIST

Related Commands

deny	Assign a trace list filter to deny IP traffic.
deny tcp	Assign a trace list filter to deny TCP traffic.

ip trace-group

C-Series	No
E-Series	✓

Assign a trace list globally to process all incoming packets to the E-Series.

Syntax **ip trace-group** *trace-list-name*

To delete an trace list configuration, use the **no ip trace-group** *trace-list-name* command.

Parameters

trace-list-name	Enter the name of a configured trace list.

Defaults Not enabled.

Command Modes CONFIGURATION

Usage Information You can assign one Trace list to the chassis.

If there are unresolved next-hops and a Trace-list is enabled, there is a possibility that the traffic hitting the CPU will not be rate-limited.

Related Commands

ip trace-list	Configure a trace list ACL.

ip trace-list

C-Series	No
E-Series	✓

Configure a trace list, based on IP addresses or protocols, to filter all traffic on the E-Series.

Syntax **ip trace-list** *trace-list-name*

To delete a trace list, use the **no ip trace-list** *trace-list-name* command.

Parameters

trace-list-name	Enter a string up to 16 characters long as the access list name.

Defaults Not configured

Example

```
Force10(conf)#ip trace-list suzanne
Force10(config-trace-acl)#
```

Figure 151 ip trace-list Command Example

Command Modes CONFIGURATION

Usage Information After you create a trace list, you must apply it to the E-Series using the ip trace-group command in the CONFIGURATION mode.

Related Commands

ip trace-group	View the current configuration.

permit

Configure a filter to pass IP packets meeting the filter criteria.

Syntax **permit** {**ip** | *ip-protocol-number*} {*source mask* | **any** | **host** *ip-address*} {*destination mask* | **any** | **host** *ip-address*} [**count** [**byte**]| **log**]

To remove this filter, you have two choices:

- use the **no seq** *sequence-number* command syntax if you know the filter's sequence number or

- use the **no deny** {**ip** | *ip-protocol-number*} {*source mask* | **any** | **host** *ip-address*} {*destination mask* | **any** | **host** *ip-address*} command.

Parameters

ip	Enter the keyword **ip** to configure a generic IP access list. The keyword **ip** specifies that the access list will permit all IP protocols.
ip-protocol-number	Enter a number from 0 to 255 to permit based on the protocol identified in the IP protocol header.
source	Enter the IP address of the network or host from which the packets were sent.
mask	(OPTIONAL) Enter a network mask in /prefix format (/x).
any	Enter the keyword **any** to specify that all routes are subject to the filter.
host *ip-address*	Enter the keyword **host** followed by the IP address to specify a host IP address.
destination	Enter the IP address of the network or host to which the packets are sent.
count	(OPTIONAL) Enter the keyword **count** to count packets processed by the filter.
byte	(OPTIONAL) Enter the keyword **byte** to count only bytes processed by the filter.
log	(OPTIONAL) Enter the keyword **log** to have the information kept in a Trace-list log file.

Defaults Not configured.

Command Modes TRACE LIST

Related Commands

ip trace-list	Create a trace list.
permit tcp	Assign a trace list filter to forward TCP packets.
permit udp	Assign a trace list filter to forward UDP packets.

permit tcp

Configure a filter to pass TCP packets meeting the filter criteria.

Syntax **permit tcp** {*source mask* | **any** | **host** *ip-address*} [*operator port* [*port*]] {*destination mask* | **any** | **host** *ip-address*} [*operator port* [*port*]] [**count** [**byte**]] | **log**] [**order** *number*]

To remove this filter, you have two choices:

- use the **no seq** *sequence-number* command syntax if you know the filter's sequence number or

- use the **no permit tcp** {*source mask* | **any** | **host** *ip-address*} {*destination mask* | **any** | **host** *ip-address*} command.

Parameters

source	Enter the IP address of the network or host from which the packets were sent.
mask	(OPTIONAL) Enter a network mask in /prefix format (/x).
any	Enter the keyword **any** to specify that all routes are subject to the filter.
host *ip-address*	Enter the keyword **host** followed by the IP address to specify a host IP address.
operator	(OPTIONAL) Enter one of the following logical operand: **eq** = equal to **neq** = not equal to **gt** = greater than **lt** = less than **range** = inclusive range of ports (you must specify two port for the *port* parameter.)
port port	Enter the application layer port number. Enter two port numbers if using the range logical operand. Range: 0 to 65535. The following list includes some common TCP port numbers: 23 = Telnet 20 and 21 = FTP 25 = SMTP 169 = SNMP
destination	Enter the IP address of the network or host to which the packets are sent.
count	(OPTIONAL) Enter the keyword **count** to count packets processed by the filter.
byte	(OPTIONAL) Enter the keyword byte to count only bytes processed by the filter.
log	(OPTIONAL) Enter the keyword **log** to have the information kept in a Trace-list log file.
order *number*	(OPTIONAL) Enter the keyword **order** followed by a number from 0 to 7 as the order number.

Defaults

Not configured.

Command Modes

TRACE LIST

Related Commands

ip trace-list	Create a trace list.
permit	Assign a trace list filter to forward IP packets.
permit udp	Assign a trace list filter to forward UDP packets.

permit udp

Configure a filter to pass UDP packets meeting the filter criteria.

Syntax

permit udp {*source mask* | **any** | **host** *ip-address*} [*operator port* [*port*]] {*destination mask* | **any** | **host** *ip-address*} [*operator port* [*port*]] [**count** [**byte**]] | **log**] [**order** *number*]

To remove this filter, you have two choices:

- use the **no seq** *sequence-number* command syntax if you know the filter's sequence number or
- use the **no permit udp** {*source mask* | **any** | **host** *ip-address*} {*destination mask* | **any** | **host** *ip-address*} command.

Parameters

source	Enter the IP address of the network or host from which the packets were sent.
mask	(OPTIONAL) Enter a network mask in /prefix format (/x).
any	Enter the keyword **any** to specify that all routes are subject to the filter.
host *ip-address*	Enter the keyword **host** followed by the IP address to specify a host IP address.
operator	(OPTIONAL) Enter one of the following logical operand: • **eq** = equal to • **neq** = not equal to • **gt** = greater than • **lt** = less than • **range** = inclusive range of ports (you must specify two ports for the *port* parameter.)
port port	(OPTIONAL) Enter the application layer port number. Enter two port numbers if using the **range** logical operand. Range: 0 to 65535
destination	Enter the IP address of the network or host to which the packets are sent.
count	(OPTIONAL) Enter the keyword **count** to count packets processed by the filter.
byte	(OPTIONAL) Enter the keyword **byte** to count only bytes processed by the filter.
log	(OPTIONAL) Enter the keyword **log** to have the information kept in a Trace-list log file.
order *number*	(OPTIONAL) Enter the keyword **order** followed by a number from 0 to 7 as the order number.

Defaults

Not configured.

Command Modes

TRACE LIST

Related Commands

ip trace-list	Configure a trace list.

permit	Assign a trace list filter to forward IP packets.
permit tcp	Assign a trace list filter to forward TCP packets.

seq

Assign a sequence number to a deny or permit filter in a trace list while creating the filter.

Syntax

seq *sequence-number* {**deny** | **permit**} {*ip-protocol-number* | **ip | tcp | udp**} {*source mask* | **any** | **host** *ip-address*} {*destination mask* | **any** | **host** *ip-address*} [*operator port* [*port*]] [**precedence** *precedence*] [**tos** *tos-value*] [**count** [**byte**] | **log**]

To delete a filter, use the **no seq** *sequence-number* command.

Parameters

sequence-number	Enter a number from 0 to 65535.
deny	Enter the keyword **deny** to configure a filter to drop packets meeting this condition.
permit	Enter the keyword **permit** to configure a filter to forward packets meeting this criteria.
ip-protocol-number	Enter a number from 0 to 255 to filter based on the protocol identified in the IP protocol header.
ip	Enter the keyword **ip** to configure a generic IP access list. The keyword **ip** specifies that the access list will permit all IP protocols.
tcp	Enter the keyword **tcp** to configure a TCP access list filter.
udp	Enter the keyword **udp** to configure a UDP access list filter.
source	Enter the IP address of the network or host from which the packets were sent.
mask	(OPTIONAL) Enter a network mask in /prefix format (/x).
any	Enter the keyword **any** to specify that all routes are subject to the filter.
host *ip-address*	Enter the keyword **host** followed by the IP address to specify a host IP address.
operator	(OPTIONAL) Enter one of the following logical operands: • **eq** = equal to • **neq** = not equal to • **gt** = greater than • **lt** = less than • **range** = inclusive range of ports (you must specify two ports for the *port* parameter.)

port port	(OPTIONAL) Enter the application layer port number. Enter two port numbers if using the **range** logical operand. Range: 0 to 65535 The following list includes some common TCP port numbers: • 23 = Telnet • 20 and 21 = FTP • 25 = SMTP • 169 = SNMP
destination	Enter the IP address of the network or host to which the packets are sent.
precedence *precedence*	Enter the keyword **precedence** followed by a number from 0 to 7 as the precedence value.
tos *tos-value*	Enter the keyword **tos** followed by a number from 0 to 15 as the TOS value.
count	(OPTIONAL) Enter the keyword **count** to count packets processed by the filter.
byte	(OPTIONAL) Enter the keyword **byte** to count only bytes processed by the filter.
log	(OPTIONAL) Enter the keyword **log** to have the information kept in a Trace-list log file.

Defaults Not configured.

Command Modes TRACE LIST

Command History

Version 7.4.1.0	Deprecated **established** keyword—not supported on TeraScale line cards.

Related Commands

deny	Configure a filter to drop packets.
permit	Configure a filter to forward packets.

show config

View the current IP trace list configuration.

Syntax **show config**

Command Modes TRACE LIST

Example

```
Force10(config-trace-acl)#show config
!
ip trace-list suzanne
 seq 5 deny tcp any any
Force10(config-trace-acl)#
```

Figure 152 show config Command Example in TRACE LIST Mode

show ip accounting trace-lists

View the trace lists created on the E-Series and the sequence of filters.

Syntax **show ip accounting trace-lists** [*trace-list-name* [**linecard** *number*]]

Parameters

trace-list-name	(OPTIONAL) Enter the name of the trace list to be displayed.
linecard *number*	(OPTIONAL) Enter the keyword **linecard** followed by the line card number to view the Trace list information on that line card. C-Series Range: 0-7on the C300 E-Series Range: 0 to 13 on a E1200, 0 to 6 on a E600, and 0 to 5 on a E300.

Command Modes EXEC

EXEC privilege

Example

```
Force10#show ip accounting trace-list suzanne
Trace List suzanne
 seq 5 deny ip any any count (0x00 packets)
 seq 10 permit tcp 10.1.1.0 /24 any count bytes (0x00 bytes)
Force10#
```

Figure 153 show ip accounting trace-lists Command Example

Chapter 16 Storm Control

The FTOS Storm Control feature allows users to limit or suppress traffic during a traffic storm (Broadcast/Unknown Unicast Rate Limiting).

The Storm Control commands are:

- show storm-control broadcast on page 448
- show storm-control unknown-unicast on page 449
- storm-control broadcast (Configuration) on page 450
- storm-control unknown-unicast (Configuration) on page 451
- storm-control broadcast (Interface) on page 452
- storm-control unknown-unicast (Interface) on page 453

Important Points to Remember

C-Series

- In C-Series, storm-control is packets per second (E-Series is in percentage of line rate).
- Only ingress storm-control is supported on the C-Series.
- The interface commands can only be applied on physical interfaces (VLANs and LAG interfaces are not supported).
- An Interface-level command only support storm-control configuration on the Ingress.
- An Interface-level command will override any Configuration-level Ingress command for that physical interface, if both are configured.
- Do not apply per-VLAN QoS on an interface that has storm-control enabled (either on an Interface or globally)
- When storm control is applied on an interface, the percentage of storm control applied is calculated based on the advertised rate of the line card. Not based on the speed setting for the line card.

E-Series

- The interface commands can only be applied on physical interfaces (VLANs and LAG interfaces are not supported).
- An Interface-level command only support storm-control configuration on the Ingress.

- An Interface-level command will override any Configuration-level Ingress command for that physical interface, if both are configured.
- The configuration-level storm-control commands can be applied at the Ingress or Egress and are supported on all physical interfaces.
- When storm control is applied on an interface, the percentage of storm control applied is calculated based on the advertised rate of the line card. Not based on the speed setting for the line card.
- Do not apply per-VLAN QoS on an interface that has storm-control enabled (either on an Interface or globally)
- When broadcast storm-control is enabled on an interface or globally on the Ingress and DSCP marking for a DSCP value 1 is configured for the data traffic, the traffic will go to queue 1 instead of queue 0.
- Similarly, if unicast storm-control is enabled on an interface or globally on the Ingress, and DSCP marking for a DSCP value 2 is configured for the data traffic, the traffic will go to queue 2 instead of queue 0.

Note: Bi-directional traffic (unknown unicast and broadcast) along with egress storm control causes the configured traffic rates to be split between the involved ports. The percentage of traffic that each port receives after the split is not predictable. These ports can be in the same/different port-pipes, or the same/different line cards.

show storm-control broadcast

Display the storm-control broadcast configuration.

Syntax **show storm-control broadcast** [*interface*]

Parameters

interface	OPTIONAL) Enter one of the following interfaces to display the interface specific storm-control configuration. • For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information. • For a SONET interface, enter the keyword **sonet** followed by the slot/port information. • Fast Ethernet is not supported.

Defaults No default behavior or values

Command Modes EXEC

Command History

Version 7.5.1.0	Introduced

Example

```
Force10#show storm-control broadcast gigabitethernet 11/11

 Broadcast storm control configuration

Interface       Direction       Percentage       Wred Profile
-----------------------------------------------------------------
Gi 11/11         Ingress               5.6

Gi 11/11         Egress                5.6                -
Force10#
```

Figure 154 show storm-control broadcast command Example (E-Series)

Example

```
Force10#show storm-control broadcast gigabitethernet 3/24

 Broadcast storm control configuration

Interface       Direction       Packets/Second
-----------------------------------------------
Gi 3/24          Ingress               1000

Force10#
```

Figure 155 show storm-control broadcast command Example (C-Series)

show storm-control unknown-unicast

Display the storm-control unknown-unicast configuration

Syntax **show storm-control** {*interface*}

Parameters

interface	(OPTIONAL) Enter one of the following interfaces to display the interface specific storm-control configuration. • For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information. • For a SONET interface, enter the keyword **sonet** followed by the slot/port information. • Fast Ethernet is not supported.

Defaults No default behavior or values

Command Modes EXEC

Command History

Version 7.5.10	Introduced

Example E-Series

```
Force10#show storm-control unknown-unicast gigabitethernet 11/1

 Unknown-unicast storm control configuration

Interface       Direction       Percentage       Wred Profile
-----------------------------------------------------------------
Gi 11/1          Ingress               5.9        -

Gi 11/1          Egress                5.7        w8

Force10#
```

Figure 156 show storm-control unknown-unicast command Example (E-Series)

Example C-Series

```
Force10#Force10#show storm-control unknown-unicast gigabitethernet 3/0

 Unknown-unicast storm control configuration

Interface       Direction       Packets/Second
-----------------------------------------------
Gi 3/0           Ingress               1000

Force10#
```

Figure 157 show storm-control unknown-unicast command Example (C-Series)

storm-control broadcast (Configuration)

Configure the percentage of broadcast traffic allowed in or out of the network.

Syntax **storm-control broadcast** [*percentage* {*decimal value*} **in | out**] | [**wred-profile** *name*]] [*packets per second* **in**]

To disable broadcast rate-limiting, use the **storm-control broadcast** [*percentage* {*decimal value*} **in | out**] | [**wred-profile** *name*]] [*packets per second* **in**] command.

Parameters

percentage {*decimal value*} **in | out**	**E-Series Only**: Enter the percentage of broadcast traffic allowed in or out of the network. Optionally, you can designate a decimal value percentage, for example, 55.5%. Percentage: 0 to 100 0 % blocks all related traffic 100% allows all traffic into the interface Decimal Range: .1 to .9

wred-profile *name*	**E-Series Only**: (Optionally) Enter the keyword **wred-profile** followed by the profile name to designate a wred-profile.
packets per second **in**	**C-Series Only**: Enter the packets per second of broadcast traffic allowed into the network. Range: 0 to 33554431

Defaults No default behavior or values

Command Modes CONFIGURATION

Command History

Version 7.5.1.0	C-Series: Introduced
Version 7.4.1.0	E-Series Only: Added percentage decimal value option
Version 6.5.1.0	E-Series Only: Introduced

Usage Information Broadcast Storm-Control is valid on Layer 2/Layer 3 interfaces only. Layer 2 broadcast traffic is treated as unknown-unicast traffic.

storm-control unknown-unicast (Configuration)

Configure the percentage of unknown-unicast traffic allowed in or out of the network.

Syntax **storm-control unknown-unicast** [*percentage* {*decimal value*} **in | out**] | [**wred-profile** *name*]] [*packets per second* **in**]

To disable unknown-unicast traffic, use the **no storm-control unknown-unicast** [*percentage* {*decimal value*} **in | out**] | [**wred-profile** *name*]] [*packets per second* **in**] command.

Parameters

percentage {*decimal value*} **in	out**	Enter the percentage of broadcast traffic allowed in or out of the network. Optionally, you can designate a decimal value percentage, for example, 55.5%. Percentage: 0 to 100 0 % blocks all related traffic 100% allows all traffic into the interface Decimal Range: .1 to .9
wred-profile *name*	**E-Series Only**: (Optionally) Enter the keyword **wred-profile** followed by the profile name to designate a wred-profile.
packets per second **in**	**C-Series Only**: Enter the packets per second of broadcast traffic allowed into the network. Range: 0 to 33554431

Defaults No default behavior or values

Command Modes CONFIGURATION

Command History

Version 7.5.1.0	C-Series: Introduced
Version 7.4.1.0	E-Series Only: Added percentage decimal value option
Version 6.5.1.0	E-Series Only: Introduced

Usage Information Unknown Unicast Strom-Control is valid for Layer 2 and Layer 2/Layer 3 interfaces.

storm-control broadcast (Interface)

Configure the percentage of broadcast traffic allowed on an interface (Ingress only).

Syntax **storm-control broadcast** [*percentage* {*decimal value*} **in**] |[**wred-profile** *name*]] [*packets per second* **in**]

To disable broadcast storm-control on the interface, use the **no storm-control broadcast** [*percentage* {*decimal value*} **in**] |[**wred-profile** *name*]] [*packets per second* **in**] command.

Parameters

percentage {*decimal value*} **in**	Enter the percentage of broadcast traffic allowed in to the network. Optionally, you can designate a decimal value percentage, for example, 55.5%. Percentage: 0 to 100 0 % blocks all related traffic 100% allows all traffic into the interface Decimal Range: .1 to .9
wred-profile *name*	**E-Series Only**: (Optionally) Enter the keyword **wred-profile** followed by the profile name to designate a wred-profile.
packets per second **in**	**C-Series Only**: Enter the packets per second of broadcast traffic allowed into the network. Range: 0 to 33554431

Defaults No default behavior or values

Command Modes INTERFACE

Command History

Version 7.5.1.0	C-Series: Introduced
Version 7.4.1.0	E-Series Only: Added percentage decimal value option
Version 6.5.1.0	E-Series Only: Introduced

storm-control unknown-unicast (Interface)

Configure percentage of unknown-unicast traffic allowed on an interface (Ingress only).

Syntax

storm-control unknown-unicast [*percentage* {*decimal value*} **in**] | [**wred-profile** *name*]] [*packets per second* **in**]

To disable unknown-unicast storm-control on the interface, use the **no storm-control unknown-unicast** [*percentage* {*decimal value*} **in**] | [**wred-profile** *name*]] [*packets per second* **in**] command.

Parameters

percentage {*decimal value*} **in**	Enter the percentage of broadcast traffic allowed in to the network. Optionally, you can designate a decimal value percentage, for example, 55.5%. Percentage: 0 to 100 0 % blocks all related traffic 100% allows all traffic into the interface Decimal Range: .1 to .9
wred-profile *name*	**E-Series Only**: (Optionally) Enter the keyword **wred-profile** followed by the profile name to designate a wred-profile.
packets per second **in**	**C-Series Only**: Enter the packets per second of broadcast traffic allowed into the network. Range: 0 to 33554431

Defaults

No default behavior or values

Command Modes

INTERFACE

Command History

Version 7.5.1.0	C-Series: Introduced
Version 7.4.1.0	E-Series Only: Added percentage decimal value option
Version 6.5.1.0	E-Series Only: Introduced

Chapter 17 Interface Commands

The chapter contains commands to configure Interfaces and includes the following sections

- Basic Interface Commands on page 455
- Port Channel-Specific Commands on page 500
- Port Mirroring (Deprecated) on page 507
- Time Domain Reflectometer (TDR) on page 507
- UDP Broadcast on page 510

Basic Interface Commands

The following commands are in the INTERFACE mode for physical, Loopback, and Null interfaces. Use the following commands to configure interfaces:

- clear counters on page 456
- clear dampening on page 458
- dampening on page 458
- description on page 460
- duplex (Management) on page 460
- duplex (10/100 Interfaces) on page 461
- flowcontrol on page 461
- interface on page 464
- interface loopback on page 464
- interface ManagementEthernet on page 465
- interface null on page 466
- interface port-channel on page 467
- interface range on page 468
- interface range macro (define) on page 470
- interface range macro name on page 472
- interface rate-interval on page 472
- interface vlan on page 473

- ipg (Gigabit Ethernet interfaces) on page 474
- ipg (10 Gigabit Ethernet interfaces) on page 474
- keepalive on page 475
- lfs enable (EtherScale) on page 475
- monitor on page 476
- mtu on page 478
- negotiation auto on page 480
- portmode hybrid on page 482
- show config on page 483
- show config (Bulk Configuration) on page 484
- show interfaces on page 484
- show interfaces configured on page 490
- show interfaces dampening on page 491
- show interfaces description on page 492
- show interfaces linecard on page 493
- show interfaces status on page 493
- show interfaces switchport on page 494
- show range on page 496
- shutdown on page 496
- speed (10/100/1000 Interfaces) on page 497
- speed (Management interface) on page 498
- switchport on page 498
- WAN Port on page 499

clear counters

Clear the counters used in the show interfaces commands for all VRRP groups, VLANs, and physical interfaces or selected ones.

Syntax **clear counters** [*interface*] [**vrrp** [*vrid*] | **learning-limit**]

Parameters

interface	(OPTIONAL) Enter the following keywords and slot/port or number information: • For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For a Loopback interface, enter the keyword **loopback** followed by a number from 0 to 16383. • For a Port Channel interface, enter the keyword **port-channel** followed by a number: C-Series Range: 1-128 on the C300 E-Series Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale • For the management interface on the RPM, enter the keyword **ManagementEthernet** followed by slot/port information. The slot range is 0-1, and the port range is 0. • For a SONET interface, enter the keyword **sonet** followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information. • For a VLAN, enter the keyword **vlan** followed by a number from 1 to 4094.
vrrp *vrid*	(OPTIONAL) Enter the keyword **vrrp** to clear statistics for all VRRP groups configured. Enter a number from 1 to 255 as the *vrid*.
learning-limit	(OPTIONAL) Enter the keyword **learning-limit** to clear unknown source address (SA) drop counters when MAC learning limit is configured on the interface.

Defaults

Without an interface specified, the command clears all interface counters.

Command Modes

EXEC privilege

Command History

Version 6.5.1.0	Updated definition of the learning-limit option for clarity.

Example

```
Force10#clear counters
Clear counters on all interfaces [confirm]
```

Figure 158 clear counters Command Example

Related Commands

show interfaces	Displays information on the interfaces.

clear dampening

Clear the dampening counters on all the interfaces or just the specified interface.

Syntax **clear dampening** [*interface*]

Parameters

interface	(Optional) Enter one of the following keywords and slot/port or number information: • For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For a Port Channel interface, enter the keyword **port-channel** followed by a number: C-Series Range: 1-128 on the C300 E-Series Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale • For a SONET interface, enter the keyword **sonet** followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information.

Defaults Without a specific interface specified, the command clears all interface dampening counters

Command Modes EXEC Privilege

Command History

Version 7.4.1.0	Introduced

Example

```
Force10#clear dampening gigabitethernet 1/2
Clear dampening counters on Gi 1/2 [confirm] y
Force10#
```

Related Commands

show interfaces dampening	View interface dampening information
dampening	Configure dampening on an interface

dampening

Configure dampening on an interface.

Syntax **dampening [[[[***half-life***]** [*reuse-threshold*]] [*suppress-threshold*]] [*max-suppress-time*]]

To disable dampening, use the **no dampening [[[[***half-life***]** [*reuse-threshold*]] [*suppress-threshold*]] [*max-suppress-time*]]command.

Parameters

half-life	Enter the number of seconds after which the Penalty is decreased. The Penalty is decreased by half after the half-life period expires. Range: 1 to 30 seconds Default: 5 seconds
reuse-threshold	Enter a number as the reuse threshold; the Penalty value below which the interface state is changed to “up”. Range: 1 to 20000 Default: 750
suppress-threshold	Enter a number as the suppress threshold; the Penalty value above which the interface state is changed to “error disabled”. Range: 1 to 20000 Default: 2500
max-suppress-time	Enter the maximum number for which a route can be suppressed. The default is four times the half-life value. Range: 1 to 20000 Default: 20 seconds

Defaults

Disabled

Command Modes

INTERFACE (conf-if-)

Command History

Version 7.4.1.0	Introduced

Example

```
Force10(conf-if-gi-3/2)#dampening 20 800 4500 120
Force10(conf-if-gi-3/2)#
```

Usage Information

With each flap, FTOS penalizes the interface by assigning a penalty (1024) that decays exponentially depending on the half-life. Once the accumulated penalty exceeds the supress threshold value, the interface is moved to error-disabled state. This interface state is deemed as “down” by all static/dynamic Layer 2 and Layer 3 protocols. The penalty is exponentially decayed based on the half-life timer. Once the penalty decays below the reuse threshold, the interface is enabled. The configured parameters should follow:

- *suppress-threshold* should be greater than *reuse-threshold*
- *max-suppress-time* should be at least 4 times *half-life*

Note: Dampening can not be applied on an interface that is monitoring traffic for other interface(s).

Related Commands

show interfaces dampening	View interface dampening information.

description

Assign a descriptive text string to the interface.

Syntax **description** *desc text*

To delete a description, enter **no description**.

Parameters

desc text	Enter a text string up to 78 characters long.

Defaults No description is defined.

Command Modes INTERFACE

Usage Information Entering a text string after the description command overwrites any previous text string configured as the description. The shutdown and description commands are the only commands that you can configure on an interface that is a member of a Port Channel. Use the show interfaces description command to view descriptions configured for each interface.

Related Commands

show interfaces description	View description field of interfaces.

duplex (Management)

Set the mode of the Management interface.

Syntax **duplex** {**half** | **full**}

To return to the default setting, enter **no duplex**.

Parameters

half	Enter the keyword **half** to set the Management interface to transmit only in one direction.
full	Enter the keyword **full** to set the Management interface to transmit in both directions.

Defaults Not configured

Command Modes INTERFACE

Command History

Version 6.4.1.0	Documentation modified—added Management to distinquish from duplex (10/100 Interfaces)

Usage Information This command applies only to the Management interface on the RPMs.

Related Commands		
	speed (Management interface)	Set the speed on the Management interface.

duplex (10/100 Interfaces)

Configure duplex mode on any physical interfaces with the speed set to 10/100.

Syntax **duplex** {**half** | **full**}

To return to the default setting, enter **no duplex**.

Parameters		
	half	Enter the keyword **half** to set the physical interface to transmit only in one direction.
	full	Enter the keyword **full** to set the physical interface to transmit in both directions.

Defaults Not configured

Command Modes INTERFACE

Command History		
	Version 6.4.1.0	Introduced

Usage Information This command applies to any physical interface with speed set to 10/100.

Related Commands		
	speed (10/100/1000 Interfaces)	Set the speed on the Base-T Ethernet interface.
	negotiation auto	Enable or disable auto negotiation on an interface.

flowcontrol

Control how the system responds to, and generates 802.3x pause frames on 1 and 10 Gig line cards.

Syntax **flowcontrol rx** {**off** | **on**} **tx** {**off** | **on**}

To return to the default **(rx on tx on**), use the **no flowcontrol rx** {**off** | **on**} **tx** {**off** | **on**} command.

Parameters

rx on	Enter the keywords **rx on** to process the received flow control frames on this port. This is the default value for the receive side.
rx off	Enter the keywords **rx off** to ignore the received flow control frames on this port.
tx on	Enter the keywords **tx on** to send control frames from this port to the connected device when a higher rate of traffic is received. This is the default value on the send side.
tx off	Enter the keywords **tx off** so that flow control frames are not sent from this port to the connected device when a higher rate of traffic is received.

Defaults

rx on tx on

Command Modes

INTERFACE

Command History

Version 6.5.1.9 and 7.4.1.0	Introduced

Usage Information

The globally assigned 48-bit Multicast address 01-80-C2-00-00-01 is used to send and receive pause frames. To allow full duplex flow control, stations implementing the pause operation instruct the MAC to enable reception of frames with destination address equal to this multicast address.

Important Points to Remember

- Asymmetric flow control (**rx on tx off** or **rx off tx on**) setting for the interface port less than 100 Mb/s speed is not permitted. The following error is returned:

  Can't configure Asymmetric flowcontrol when speed <1G, config ignored

- The only configuration applicable to half duplex ports is **rx off tx off**. The following error is returned:

  Can't configure flowcontrol when half duplex is configure, config ignored

  Half duplex can not be configured when Flow control configuration is on (default is **rx on tx on**). The following error is returned:

  Can't configure half duplex when flowcontrol is on, config ignored

Note: The flow control must be off (**rx off tx off**) before configuring the half duplex.

- Speeds less than 1 Gig can not be configured when the asymmetric flow control configuration is on. The following error is returned:

  Can't configure speed <1G when Asymmetric flowcontrol is on, config ignored

  FTOS only supports **rx on tx on** and **rx off tx off** for speeds less than 1 Gig (Symmetric).

Example

```
Force10(conf-if-gi-0/1)#show config
!
interface GigabitEthernet 0/1
no ip address
switchport
no negotiation auto
flowcontrol rx off tx on
no shutdown
...
```

Figure 159 show running config (partial)

Table 25 displays how FTOS negotiate the flow control values between two Force10 chassis connected back-to-back using 1 Gig Copper Ports.

Table 25 Negotiated Flow Control Values

Configured				Negotiated			
LocRxConf	**LocTxConf**	**RemoteRxConf**	**RemoteTxConf**	**LocNegRx**	**LocNegTx**	**RemNegRx**	**RemNegTx**
off	off	off	off	**off**	**off**	**off**	**off**
		off	on	**off**	**off**	**off**	**off**
		on	off	**off**	**off**	**off**	**off**
		on	on	**off**	**off**	**off**	**off**
off	on	off	off	**off**	**off**	**off**	**off**
		off	on	**off**	**off**	**off**	**off**
		on	off	**off**	**on**	**on**	**off**
		on	on	**off**	**off**	**off**	**off**
on	off	off	off	**off**	**off**	**off**	**off**
		off	on	**on**	**off**	**off**	**on**
		on	off	**on**	**on**	**on**	**on**
		on	on	**on**	**on**	**on**	**on**
on	on	off	off	**off**	**off**	**off**	**off**
		off	on	**off**	**off**	**off**	**off**
		on	off	**on**	**on**	**on**	**on**
		on	on	**on**	**on**	**on**	**on**

Related Commands

show running-config	Display the flow configuration parameters (non-default values only)
show interfaces	Displays the negotiated flow control parameters

interface

Configure a physical interface on the E-Series.

Syntax **interface** *interface*

Parameters

interface	Enter the following keywords and slot/port or number information: • For 100/1000 Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For SONET interfaces, enter the keyword **sonet** followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information.

Defaults Not configured.

Command Modes CONFIGURATION

Example

```
Force10(conf)#interface gig 0/0
Force10(conf-if-gi-0/0)#exit#
```

Figure 160 interface Command Example

Usage Information You cannot delete a physical interface.

By default, physical interfaces are disabled (shutdown) and are in Layer 3 mode. To place an interface in mode, ensure that the interface's configuration does not contain an IP address and enter the switchport command.

Related Commands

interface loopback	Configure a Loopback interface.
interface null	Configure a Null interface.
interface port-channel	Configure a Port Channel.
interface sonet	Configure a SONET interface.
interface vlan	Configure a VLAN.

interface loopback

Configure a Loopback interface.

Syntax **interface loopback** *number*

To remove a loopback interface, use the **no interface loopback** *number* command.

Parameters

number	Enter a number as the interface number. Range: 0 to 16383.

Defaults Not configured.

Command Modes CONFIGURATION

Example

```
Force10(conf)#interface loopback 1655
Force10(conf-if-lo-1655)#
```

Figure 161 interface loopback Command Example

Related Commands

interface	Configure a physical interface.
interface null	Configure a Null interface.
interface port-channel	Configure a Port Channel.
interface vlan	Configure a VLAN.

interface ManagementEthernet

Configure the Management port on the E-Series RPM (either the Primary or Standby RPM).

Syntax **interface ManagementEthernet** *interface*

Parameters

interface	Enter the keyword **ManagementEthernet** followed by slot number (0-1) and port number zero (0).

Defaults Not configured.

Command Modes CONFIGURATION

Example

```
Force10(conf)#interface managementethernet 0/0
Force10(conf-if-ma-0/0)#
```

Figure 162 interface ManagementEthernet Command Example

Usage Information

You cannot delete a Management port.

Management port is enabled by default (no shutdown). Use the ip address to assign an IP address to the Management port.

If two RPMs are installed in your system, use the show redundancy to view which RPM is the Primary RPM.

interface null

Configure a Null interface on the E-Series.

Syntax **interface null** *number*

Parameters

number	Enter zero (0) as the Null interface number.

Defaults Not configured; *number* = 0

Command Modes CONFIGURATION

Example

```
Force10(conf)#interface null 0
Force10(conf-if-nu-0)#
```

Figure 163 interface null Command Example

Usage Information

You cannot delete the Null interface. The only configuration command possible in a Null interface is ip unreachables.

Related Commands

interface	Configure a physical interface.
interface loopback	Configure a Loopback interface.
interface port-channel	Configure a Port Channel.
interface vlan	Configure a VLAN.
ip unreachables	Enable generation of ICMP unreachable messages.

interface port-channel

Create a Port Channel interface, which is a link aggregation group containing up to 16 physical interfaces. FTOS supports up to 255 Port Channels for TeraScale, 32 for EtherScale.

Syntax **interface port-channel** *channel-number*

To delete a Port Channel, use the **no interface port-channel** *channel-number* command.

Parameters

channel-number	Enter a number as the interface number. Range: 1 to 255 for TeraScale, 1 to 32 for EtherScale.

Defaults Not configured.

Command Modes CONFIGURATION

Example

```
Force10(conf)#int port-channel 2
Force10(conf-if-po-2)#
```

Figure 164 interface port-channel Command Example

Usage Information

Port Channel interfaces are logical interfaces and can be either in Layer 2 mode (by using the switchport command) or Layer 3 mode (by configuring an IP address). You can add a Port Channel in Layer 2 mode to a VLAN.

The shutdown, description, and name commands are the only commands that you can configure on an interface while it is a member of a Port Channel. To add a physical interface to a Port Channel, the interface can only have the shutdown, description, and name commands configured. The Port Channel's configuration is applied to the interfaces within the Port Channel.

A Port Channel can contain both 100/1000 interfaces and GE interfaces. Based on the first interface configured in the Port Channel and enabled, FTOS determines if the Port Channel uses 100 Mb/s or 1000 Mb/s as the common speed. Refer to channel-member for more information.

If the line card is in a Jumbo mode chassis, then the mtu and ip mtu commands can also be configured. The Link MTU and IP MTU values configured on the channel members must be greater than the Link MTU and IP MTU values configured on the Port Channel interface.

Note: In a Jumbo-enabled system, all members of a Port Channel must be configured with the same link MTU values and the same IP MTU values.

Related Commands

interface	Configure a physical interface.
interface loopback	Configure a Loopback interface.
interface null	Configure a null interface.
interface vlan	Configure a VLAN.

interface range

This command permits configuration of a range of interface to which subsequent commands are applied (bulk configuration). Using the **interface range** command, identical commands can be entered for a range of interface.

Syntax **interface range interface , interface ,** ...

Parameters

interface , interface , ...	Enter the keyword **interface range** and one of the interfaces slot/port, port-channel or VLAN numbers. Select the range of interfaces for bulk configuration. You can enter up to six comma separated ranges—spaces are **not** required between the commas. Comma-separated ranges can include VLANs, port-channels and physical interfaces. Slot/Port information must contain a space before and after the dash. For example, **interface range gigabitethernet 0/1 - 5** is valid; **interface range gigabitethernet 0/1-5** is not valid. • For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For a Port Channel interface, enter the keyword **port-channel** followed by a number: C-Series Range: 1-128 on the C300 E-Series Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale • For a SONET interface, enter the keyword **sonet** followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information. • For a VLAN, enter the keyword **vlan** followed by a number from 1 to 4094

Defaults This command has no default behavior or values.

Command Modes CONFIGURATION

Usage Information When creating an interface range, interfaces appear in the order they are entered; they are not sorted. The command verifies that interfaces are present (physical) or configured (logical). Important things to remember:

- Bulk configuration is created if at least one interface is valid
- Automatically excludes non-existing interfaces from the bulk configuration and generates a warning message (Figure 165).
- The interface range prompt includes interface types with slot/port information for valid interfaces. The prompt allows for a maximum of 32 characters. If the bulk configuration exceeds 32 characters, it is represented by an ellipsis (...).
- If the interface range prompt has multiple port ranges, the smaller port range is excluded from the prompt (Figure 166).
- If overlapping port ranges are specified, the port range is extended to the smallest start port and the biggest end port (Figure 167).

Example

```
Force10(conf)#intface range so 2/0 - 1 , te 10/0 , gi 3/0  , fa 0/0
% Warning: Non-existing ports (not configured) are ignored by
interface-range
```

Figure 165 Bulk Configuration Warning Message

Example

```
Force10(conf)#intface range gi 2/0 - 23 , gi 2/1 - 10
Force10(conf-if-range-gi-2/0-23#
```

Figure 166 Interface Range prompt with Multiple Ports

Example

```
Force10(conf)#intface range gi 2/1 - 11 , gi 2/1 - 23
Force10(conf-if-range-gi-2/1-23#
```

Figure 167 Interface Range prompt Overlapping Port Ranges

Only VLAN and port-channel interfaces created using the interface vlan and interface port-channel commands can be used in the **interface range** command.

Use the show running-config command to view the VLAN and port-channel interfaces. VLAN or port-channel interfaces that are not displayed in the show running-config command can not be used with the bulk configuration feature of the **interface range** command. Note that you cannot create virtual interfaces (VLAN, Port-channel) using the **interface range** command.

Note: If a range has VLAN, physical, port-channel, and SONET interfaces, only commands related to physical interfaces can be bulk configured. To configure commands specific to VLAN, port-channel or SONET, only those respective interfaces should be configured in a particular range.

Figure 168 is an example of a single range bulk configuration.

Example

```
Force10(config)# interface range gigabitethernet 5/1 - 23
Force10(config-if-range)# no shutdown
Force10(config-if-range)#
```

Figure 168 Single range Bulk Configuration

Figure 169 shows how to use commas to add different interface types to the range enabling all Gigabit Ethernet interfaces in the range 5/1 to 5/23 and both Ten Gigabit Ethernet interfaces 1/1 and 1/2.

Example

```
Force10(config-if)# interface range gigabitethernet 5/1 - 23, tengigabitethernet 1/1 - 2
Force10(config-if-range)# no shutdown
Force10(config-if-range)#
```

Figure 169 Multiple range Bulk Configuration Gigabit Ethernet and Ten Gigabit Ethernet

Figure 170 shows how to use commas to add SONET, VLAN, and port-channel interfaces to the range.

Example

```
Force10(config-if)# interface range gigabitethernet 5/1 - 23, tengigabitethernet 1/1 - 2,
Sonet 6/1 - 10 , Vlan 2 - 100 , Port 1 - 25
Force10(config-if-range)# no shutdown
Force10(config-if-range)#
```

Figure 170 Multiple range Bulk Configuration with SONET, VLAN, and port-channel

Related Commands

interface port-channel	Configure a Port Channel group.
interface vlan	Configure a VLAN interface.
show config (Bulk Configuration)	Show the bulk configuration interfaces.
show range	Show the bulk configuration ranges.
interface range macro (define)	Define a macro for an interface-range.

interface range macro (define)

Defines a macro for an interface-range and then saves the macro in the running configuration file.

Syntax **define interface range macro** *name* **interface , interface ,** ...

Parameters

name	Enter up to 32 characters for the macro name.
interface , interface , ...	Enter the **interface keyword (see below) and** one of the interfaces slot/port, port-channel or VLAN numbers. Select the range of interfaces for bulk configuration. You can enter up to six comma separated ranges—spaces are **not** required between the commas. Comma-separated ranges can include VLANs, port-channels and physical interfaces. Slot/Port information must contain a space before and after the dash. For example, **interface range gigabitethernet 0/1 - 5** is valid; **interface range gigabitethernet 0/1-5** is not valid. • For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For a Port Channel interface, enter the keyword **port-channel** followed by a number: C-Series Range: 1-128 on the C300 E-Series Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale • For a SONET interface, enter the keyword **sonet** followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information. • For a VLAN, enter the keyword **vlan** followed by a number from 1 to 4094

Defaults

This command has no default behavior or value

Command Modes

CONFIGURATION

Command History

Version 6.2.1.1	Introduced

Example

```
Force10(config)# define interface-range test tengigabitethernet 0/0 - 3 ,
gigabitethernet 5/0 - 47 , gigabitethernet 13/0 - 89

Force10# show running-config | grep define
define interface-range test tengigabitethernet 0/0 - 3 , gigabitethernet 5/0 - 47 ,
gigabitethernet 13/0 - 89
Force10(config)#interface range macro test
Force10(config-if-range-te-0/0-3,gi-5/0-47,gi-13/0-89)#
```

Figure 171 define interface-range macro *test* command

Usage Information

Figure 171 is an example of how to define an interface-range macro named *test*. Execute the **show running-config** command to display the macro definition as shown in Figure 171.

Related Commands

interface range	Configure a range of command (bulk configuration)
interface range macro name	Run an interface range macro.

interface range macro *name*

Run the interface-range macro to automatically configure the pre-defined range of interfaces.

Syntax **interface range macro name**

Parameters

name	Enter the macro name as a keyword.

Defaults This command has no default behavior or value

Command Modes CONFIGURATION

Command History

Version 6.2.1.1	Introduced

Example

```
Force10(config)#interface range macro test
Force10(config-if-range-te-0/0-3,gi-5/0-47,gi-13/0-89)#
Force10
```

Figure 172 run interface-range macro *test*

Usage Information Figure 172 runs the macro named *test* that was defined in Figure 171.

Related Commands

interface range	Configure a range of command (bulk configuration)
interface range macro (define)	Define a macro for an interface range (bulk configuration)

interface rate-interval

Configure the rate interval with any value between 30 and 300 seconds.

Syntax **interface rate-interval** *seconds*

Parameters

seconds	Enter the number of seconds to configure the rate interval. Range: 30 to 299 seconds Default: 299 seconds **Note:** Since polling occurs every 15 seconds, the number of seconds designated will round to the nearest multiple of 15 seconds. For example, if 44 seconds is designated it will round to 30; 45 to 59 seconds will round to 45 and so forth.

Defaults No default behavior

Command Modes CONFIGURATION INTERFACE (conf-if)

Command History

Version 6.1.1.0	Introduced

Related Commands

show interfaces	View information on physical and virtual interfaces.

interface vlan

Configure a VLAN on the E-Series. You can configure up to 4094 VLANs on an E-Series.

Syntax **interface vlan** *vlan-id*

To delete a VLAN, use the **no interface vlan** *vlan-id* command.

Parameters

vlan-id	Enter a number as the VLAN Identifier. Range: 1 to 4094.

Defaults Not configured, except for the Default VLAN, which is configured as VLAN 1.

Command Modes CONFIGURATION

Example

```
Force10(conf)#int vlan 3
Force10(conf-if-vl-3)#
```

Figure 173 interface vlan Command Example

Usage Information For more information on VLANs and the commands to configure them, refer to Virtual LANs on page 330.

FTP, TFTP, and SNMP operations are not supported on a VLAN. ACLs (IP and MAC) are not supported in VLANs.

Related Commands

interface	Configure a physical interface.
interface loopback	Configure a loopback interface.
interface null	Configure a null interface.
interface port-channel	Configure a Port Channel group.

ipg (Gigabit Ethernet interfaces)

C-Series	No
E-Series	✓

Set the Inter-packet gap (IPG) to 8 bytes for traffic on a Gigabit Ethernet interface.

Syntax **ipg 8**

To return to the default setting, enter **no ipg**.

Parameters

8	Enter the keyword **8** to set the IPG to 8 bytes.

Defaults **12 bytes**

Command Modes INTERFACE

Usage Information For 1-Gigabit Ethernet interfaces only.

Note: This command is an EtherScale only command.

ipg (10 Gigabit Ethernet interfaces)

C-Series	No
E-Series	✓

Set the Inter-packet Gap for traffic on 10 Gigabit Ethernet interface.

Syntax **ipg** {**ieee-802.3ae** | **shrink**}

To return to the default of averaging the IPG, enter **no ipg** {**shrink** | **ieee-802.3ae**}

Parameters

ieee-802.3ae	Enter the keyword **ieee-802.3ae** to set the IPG to 12 (12-15) bytes (packet size dependent)
shrink	Enter the keyword **shrink** to set the IPG to 8 (8-11) bytes (packet size dependent).

Defaults averaging the IPG

Command Modes INTERFACE

Usage Information For 10 Gigabit Ethernet interfaces only.

IPG equals 96 bits times from end of the previous packet to start of the pre-amble of the next packet.

Note: This command is an EtherScale only command.

keepalive

Send keepalive packets periodically to keep an interface alive when it is not transmitting data.

Syntax **keepalive** [*seconds*]

To stop sending keepalive packets, enter **no keepalive**.

Parameters

seconds	(OPTIONAL) For SONET interfaces with PPP encapsulation enabled, enter the number of seconds between keepalive packets. Range: 0 to 23767 Default: 10 seconds

Defaults Enabled.

Command Modes INTERFACE

lfs enable (EtherScale)

Enable Link Fault Signaling (LFS) on EtherScale 10 Gigabit Ethernet interfaces only.

Syntax **lfs enable**

To disable LFS, enter **no lfs enable**.

Defaults Enabled.

Command Modes INTERFACE (10 Gigabit Ethernet interfaces only)

Usage Information If there is a failure on the link, FTOS brings down the interface. The interface will stay down until the link failure signal stops.

Note: On TeraScale line cards, LFS is always enabled by default.

monitor

Monitor counters on a single interface or all interfaces on a line card. The screen is refreshed every 5 seconds and the CLI prompt disappears.

Syntax **monitor interface** [*interface*]

To disable monitoring and return to the CLI prompt, press the q key.

Parameters

interface	(OPTIONAL) Enter the following keywords and slot/port or number information: • For an 100/1000 Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For the management port, enter the keyword **managementethernet** followed by the slot (0-1) and the port (0). • For SONET interface types, enter the keyword **sonet** followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information.

Command Modes EXEC

EXEC privilege

Usage Information The delta column displays changes since the last screen refresh.

Example

```
systest-3   Monitor time: 00:00:06   Refresh Intvl.: 2s   Time: 03:26:26

Interface: Gi 0/3, Enabled, Link is Up, Linespeed is 1000 Mbit

 Traffic statistics:              Current           Rate                 Delta
        Input bytes:              9069828         43 Bps                    86
       Output bytes:            606915800         43 Bps                    86
     Input packets:                54001          0 pps                     1
    Output packets:              9401589          0 pps                     1
       64B packets:                   67          0 pps                     0
   Over 64B packets:                49166          0 pps                     1
  Over 127B packets:                  350          0 pps                     0
  Over 255B packets:                 1351          0 pps                     0
  Over 511B packets:                  286          0 pps                     0
 Over 1023B packets:                 2781          0 pps                     0
Error statistics:
    Input underruns:                    0          0 pps                     0
       Input giants:                    0          0 pps                     0
    Input throttles:                    0          0 pps                     0
          Input CRC:                    0          0 pps                     0
  Input IP checksum:                    0          0 pps                     0
      Input overrun:                    0          0 pps                     0
   Output underruns:                    0          0 pps                     0
   Output throttles:                    0          0 pps                     0

      m - Change mode                          c - Clear screen
      l - Page up                              a - Page down
      T - Increase refresh interval            t - Decrease refresh interval
      q - Quit
```

Figure 174 monitor Command Example of a Single Interface

```
 systest-3   Monitor time: 00:01:31   Refresh Intvl.: 2s   Time: 03:54:14

Interface   Link           In Packets         [delta]          Out Packets
[delta]
   Gi 0/0   Down                  0               0                    0             0
   Gi 0/1   Down                  0               0                    0             0
   Gi 0/2     Up                61512              52                66160            42
   Gi 0/3     Up                63086              20              9405888            24
   Gi 0/4     Up          14697471418         2661481          13392989657
2661385
   Gi 0/5     Up                 3759               3            161959604        832816
   Gi 0/6     Up                 4070               3              8680346             5
   Gi 0/7     Up                61934              34            138734357            72
   Gi 0/8     Up                61427               1                59960             1
   Gi 0/9     Up                62039              53            104239232             3
  Gi 0/10     Up          17740044091             372           7373849244            79
  Gi 0/11     Up          18182889225              44           7184747584           138
  Gi 0/12     Up          18182682056               0                 3682             1
  Gi 0/13     Up          18182681434              43           6592378911           144
  Gi 0/14     Up                61349              55              86281941            15
  Gi 0/15     Up                59808              58                 62060            27
  Gi 0/16     Up                59889               1                 61616             1
  Gi 0/17     Up                    0               0              14950126         81293
  Gi 0/18     Up                    0               0                     0             0
  Gi 0/19   Down                    0               0                     0             0
  Gi 0/20     Up                62734              54                62766            18
  Gi 0/21     Up                60198               9               200899             9
  Gi 0/22     Up          17304741100         3157554          10102508511
1114221
  Gi 0/23     Up          17304769659         3139507           7133354895
523329

       m - Change mode                          c - Clear screen
       b - Display bytes                        r - Display pkts/bytes per sec
       l - Page up                              a - Page down
```

Figure 175 monitor Command Example of All Interfaces on a Line Card

Table 26 defines the menu options available.

Table 26 monitor Command Menu Options

Key	Description
systest-3	Displays the host name assigned to the system.
monitor time	Displays the amount of time since the monitor command was entered.
time	Displays the amount of time the chassis is up (since last reboot).
m	Change the view from a single interface to all interfaces on the line card or visa-versa.
c	Refresh the view.
b	Change the counters displayed from Packets on the interface to Bytes.
r	Change the [delta] column from change in the number of packets/bytes in the last interval to rate per second.
l	Change the view to next interface on the line card, or if in the line card mode, the next line card in the chassis.
a	Change the view to the previous interface on the line card, or if the line card mode, the previous line card in the chassis.
T	Increase the screen refresh rate.
t	Decrease the screen refresh rate.
q	Return to the CLI prompt.

mtu

Set the maximum Link MTU (frame size) for an Ethernet interface.

Syntax **mtu** *value*

To return to the default MTU value, enter **no mtu**.

Parameters

value	Enter a maximum frame size in bytes. Range: 594 to 9252 Default: 1554

Defaults 1554

Command Modes INTERFACE

Usage Information When you enter no mtu command, FTOS reduces the ip mtu value to 1536 bytes. To return the IP MTU value to the default, enter **no ip mtu**.

You must compensate for Layer 2 header when configuring IP MTU and link MTU on an Ethernet interface. If the packet includes a Layer 2 header, the difference between the link MTU and IP MTU (ip mtu command) must be enough bytes to include for the Layer 2 header.

Link MTU and IP MTU considerations for Port Channels and VLANs are as follows.

Port Channels:

- All members must have the same link MTU value and the same IP MTU value.
- The Port Channel link MTU and IP MTU must be less than or equal to the link MTU and IP MTU values configured on the channel members.

Example: if the members have a link MTU of 2100 and an IP MTU 2000, the Port Channel's MTU values cannot be higher than 2100 for link MTU or 2000 bytes for IP MTU.

VLANs:

- All members of a VLAN must have same IP MTU value.
- Members can have different Link MTU values. Tagged members must have a link MTU 4 bytes higher than untagged members to account for the packet tag.
- The VLAN link MTU and IP MTU must be less than or equal to the link MTU and IP MTU values configured on the VLAN members.

Example: The VLAN contains tagged members with Link MTU of 1522 and IP MTU of 1500 and untagged members with Link MTU of 1518 and IP MTU of 1500. The VLAN's Link MTU cannot be higher than 1518 bytes and its IP MTU cannot be higher than 1500 bytes.

Table 27 lists the various Layer 2 overheads found in FTOS and the number of bytes.

Table 27 Difference between Link MTU and IP MTU

Layer 2 Overhead	Link MTU and IP MTU Delta
Ethernet (untagged)	18 bytes
VLAN Tag	22 bytes
Untagged Packet with VLAN-Stack Header	22 bytes
Tagged Packet with VLAN-Stack Header	26 bytes

Related Commands

ip mtu	Set the IP MTU for an Ethernet interface.

negotiation auto

Enable auto negotiation on an interface.

Syntax **negotiation auto**

To disable auto negotiation, enter **no negotiation auto**.

Defaults Enabled.

Command Modes INTERFACE

Usage Information On EtherScale 100/1000 Base-T Ethernet line cards and on TeraScale 10/100/1000 Base-T Ethernet line cards only, **negotiation auto** provides a mode option for configuring an individual port to forced-master/forced slave once auto negotiation is enabled (see Figure 176).

Note: mode option is not available on non-10/100/1000 Base-T Ethernet line cards.

```
Force10(conf)# int gi 0/0
Force10(conf-if)#neg auto
Force10(conf-if-autoneg)# ?

end                     Exit from configuration mode
exit                    Exit from autoneg configuration mode
mode                    Specify autoneg mode
no                      Negate a command or set its defaults
show                    Show autoneg configuration information
Force10(conf-if-autoneg)#mode ?
forced-master           Force port to master mode
forced-slave            Force port to slave mode
Force10(conf-if-autoneg)#
```

Figure 176 negotiation auto master/slave example

If the mode option is not used, the default setting is slave. If you do not configure forced-master/forced slave on a port, the port negotiates to either a master or a slave state. Port status is one of the following:

- Forced-master
- Force-slave
- Master
- Slave
- Auto-neg Error—typically indicates that both ends of the node are configured with forced-master or forced-slave.

Caution: Ensure that one end of your node is configured as forced-master and one is configured as forced-slave. If both are configured the same (that is forced-master or forced-slave), the show interfaces command will flap between an auto-neg-error and forced-master/slave states.

You can view master/slave settings via the **show interfaces** command (Figure 177).

```
Force10#show interfaces configured
GigabitEthernet 13/18 is up, line protocol is up
Hardware is Force10Eth, address is 00:01:e8:05:f7:fc
    Current address is 00:01:e8:05:f7:fc
Interface index is 474791997
Internet address is 1.1.1.1/24
MTU 1554 bytes, IP MTU 1500 bytes
LineSpeed 1000 Mbit, Mode full duplex, Master
ARP type: ARPA, ARP Timeout 04:00:00
Last clearing of "show interfaces" counters 00:12:42
Queueing strategy: fifo
Input Statistics:
...
```

Figure 177 View auto negotiation master/slave setting (partial)

Both sides of the link must have auto negotiation enabled or disabled for the link to come up.

Table 28 details the possible speed and auto negotiation combinations for a line between two 10/100/1000 Base-T Ethernet interfaces.

Table 28 Auto Negotiation and Link Speed Combinations

Port 0	Port 1	Link Status between Port 1 and Port 2
auto negotiation enabled* speed 1000 or auto	auto negotiation enabled* speed 1000 or auto	Up at 1000 Mb/s
auto negotiation enabled speed 100	auto negotiation enabled speed 100	Up at 100 Mb/s
auto negotiation disabled speed 100	auto negotiation disabled speed 100	Up at 100 Mb/s
auto negotiation disabled speed 100	auto negotiation enabled speed 100	Down
auto negotiation enabled* speed 1000 or auto	auto negotiation disabled speed 100	Down

* You cannot disable auto negotiation when the speed is set to 1000 or auto.

Related Commands

speed (10/100/1000 Interfaces)	Set the link speed to 10, 100, 1000 or auto negotiate the speed.

portmode hybrid

C-Series	✓
E-Series	No

Set a C-Series port to accept *both* tagged and untagged frames (hybrid) on the same port (physical ports only).

Syntax **portmode hybrid**

To return a port to accept *either* tagged or untagged frames (non-hybrid), use the **no portmode hybrid** command.

Defaults non-hybrid

Command Modes INTERFACE (conf-if-*interface-slot/port*)

Command History

Version 7.5.1.0	Introduced on C-Series Only

Example

```
Force10(conf)#interface gi 7/0
Force10(conf-if-gi-7/0)#portmode hybrid
Force10(conf-if-gi-7/0)#interface vlan 10
Force10(conf-if-vl-10)#untagged gi 7/0
Force10(conf-if-vl-10)#interface vlan 20
Force10(conf-if-vl-20)#tagged gi 7/0
Force10(conf-if-vl-20)#
```

Figure 178 portmode hybrid configuration example

Usage Information Figure 178 sets a port as hybrid, makes the port a tagged member of VLAN 20, and an untagged member of VLAN 10 which becomes the native VLAN of the port. The port will now accept:

- untagged frames and classify them as VLAN 10 frames
- VLAN 20 tagged frames

Figure 179 is an example show output with “Hybrid” as the newly added value for 802.1QTagged. The options for this field are:

- True—port is tagged
- False—port is untagged
- Hybrid—port accepts both tagged and untagged frames

```
Force10(conf-if-vl-20)#do show interfaces switchport
Name: GigabitEthernet 7/0
802.1QTagged: Hybrid
Vlan membership:
Vlan   10, Vlan   20
Native VlanId:    10
Force10(conf-if-vl-20)#
```

Figure 179 View the Tagged Hybrid Interface

Figure 180 is an example unconfiguration of the hybrid port using the **no portmode hybrid** command.

Note: You must removed all other configurations on the port before you can remove the hybrid configuration from the port.

```
Force10(conf-if-vl-20)#interface vlan 10
Force10(conf-if-vl-10)#no untagged gi 7/0
Force10(conf-if-vl-10)#interface vlan 20
Force10(conf-if-vl-20)#no tagged gi 7/0
Force10(conf-if-vl-20)#interface gi 7/0
Force10(conf-if-gi-7/0)#no portmode hybrid
Force10(conf-if-vl-20)#
```

Figure 180 Unconfigure the hybrid port

Related Commands

switchport	Place the interface in a Layer 2 mode

show config

View the interface configuration.

Syntax **show config**

Command Modes INTERFACE

Example

```
Force10(conf-if)#show conf
!
interface GigabitEthernet 1/7
 no ip address
 switchport
 no shutdown
Force10(conf-if)#
```

Figure 181 show config Command Example for the INTERFACE mode

show config (Bulk Configuration)

View the bulk configured interfaces (interface range).

Syntax **show config**

Command Modes CONFIGURATION INTERFACE (conf-if-range)

Command History

Version 6.1.1.0	Introduced

Example

```
Force10(conf-if-range-so-2/0-1,fa-0/0)#show conf
!
interface SONET 2/0
 shutdown
!
interface SONET 2/1
 shutdown
!
interface FastEthernet 0/0
 no ip address
 shutdown
Force10(conf-if-range-so-2/0-1,fa-0/0)#
```

Figure 182 show config (Bulk Configuration) Command Example

show interfaces

Displays information on the configured physical interfaces, virtual interfaces, and pluggable media (on 10-Gigabit interface only).

Syntax **show interfaces** *interface*

Parameters

interface	Enter one of the following keywords and slot/port or number information: • For a Fast Ethernet interface, enter the keyword **FastEthernet** followed by the slot/port information. • For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For Loopback interfaces, enter the keyword **loopback** followed by a number from 0 to 16383. • For the management interface on the RPM, enter the keyword **ManagementEthernet** followed by the slot/port information. The slot range is 0-1 and the port range is 0. • For the Null interface, enter the keywords **null 0**. • For a Port Channel interface, enter the keyword **port-channel** followed by a number: C-Series Range: 1-128 on the C300 E-Series Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale • For SONET interfaces, enter the keyword **sonet** followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information. • For VLAN interfaces, enter the keyword **vlan** followed by a number from 1 to 4094.

Command Modes

EXEC

EXEC privilege

Command History

Version 6.4.1.0	Changed organization of display output
Version 6.3.1.0	Added Pluggable Media Type field in output (TeraScale only)

Example 1

```
Force10#show interfaces tengigabitethernet 2/0
TenGigabitEthernet 2/0 is up, line protocol is up
Hardware is Force10Eth, address is 00:01:e8:05:f7:3a
Interface index is 100990998
Internet address is 213.121.22.45/28
MTU 1554 bytes, IP MTU 1500 bytes
LineSpeed 10000 Mbit
ARP type: ARPA, ARP Timeout 04:00:00
Last clearing of "show interfaces" counters 02:31:45
Queueing strategy: fifo
Input Statistics:
     0 packets, 0 bytes
     Input 0 IP Packets, 0 Vlans 0 MPLS
     0 64-byte pkts, 0 over 64-byte pkts, 0 over 127-byte pkts
     0 over 255-byte pkts, 0 over 511-byte pkts, 0 over 1023-byte pkts
     0 symbol errors, 0 runts, 0 giants, 0 throttles
     0 CRC, 0 IP Checksum, 0 overrun, 0 discarded
Output Statistics:
     1 packets, 64 bytes, 0 underruns
     0 Multicasts, 2 Broadcasts, 0 Unicasts
     0 IP Packets, 0 Vlans, 0 MPLS
     0 throttles, 0 discarded
Rate info (interval 299 seconds):
     Input 00.00 Mbits/sec,          0 packets/sec, 0.00% of line-rate
     Output 00.00 Mbits/sec,          0 packets/sec, 0.00% of line-rate
Time since last interface status change: 00:00:27
```

Figure 183 show interfaces Command Example (EtherScale)

Table 29 defines the information displayed in Figure 183.

Table 29 Lines in show interfaces Command Example (EtherScale)

Line	Description
GigabitEthernet 1/2...	Displays the interface's type, slot/port and administrative and line protocol status.
Hardware is...	Displays the interface's hardware information and its assigned MAC address.
Interface index...	Displays the interface index number used by SNMP to identify the interface.
Internet address...	States whether an IP address is assigned to the interface. If one is, that address is displayed.
MTU 1554...	Displays link and IP MTU information. If the chassis is in Jumbo mode, this number can range from 576 to 9252.
LineSpeed	Displays the interface's line speed.
ARP type:...	Displays the ARP type and the ARP timeout value for the interface.
Last clearing...	Displays the time when the **show interfaces** counters where cleared.
Queuing strategy...	States the packet queuing strategy. FIFO means first in first out.
Input Statistics:	Displays all the input statistics including: • the number of packets and bytes into the interface • the number of packets with IP headers, VLAN tagged headers and MPLS headers Note: The sum of the number of packets may not be as expected since a VLAN tagged IP packet counts as both a VLAN packet and an IP packet. • the packet size and the number of those packets inbound to the interface • the number of symbol errors, runts, giants, and throttles packets: symbol errors = number packets containing bad data. That is, the port MAC detected a physical coding error in the packet. runts = number of packets that are less than 64B giants = packets that are greater than the MTU size throttles = packets containing PAUSE frames • the number of CRC, IP Checksum, overrun, and discarded packets: CRC = packets with CRC/FCS errors IP Checksum = packets with IP Checksum errors overrun = number of packets discarded due to FIFO overrun conditions discarded = the sum of input symbol errors, runts, giants, CRC, IP Checksum, and overrun packets discarded without any processing

Table 29 Lines in show interfaces Command Example (EtherScale)

Line	Description
Output Statistics:	Displays output statistics sent out of the interface including: • the number of packets, bytes and underruns out of the interface packets = total number of packets bytes = total number of bytes underruns = number of packets with FIFO underrun conditions • the number of Multicast, Broadcast and Unicast packets: Multicasts = number of MAC multicast packets Broadcasts = number of MAC broadcast packets Unicasts = number of MAC unicast packets • the number of IP, VLAN and MPLs packets: IP Packets = number of IP packets Vlans = number of VLAN tagged packets MPLS = number of MPLS packets (found on a LSR interface) • the number of throttles and discards packets: throttles = packets containing PAUSE frames discarded = number of packets discarded without any processing
Rate information...	Displays an estimate of the input and output traffic rate over a designated interval (30 to 299 seconds). Traffic rate is displayed in bits, packets per second, and percent of line rate.
Time since...	Displays the elapse time since the last interface status change (hh:mm:ss format).

Example 2

```
Force10#show interfaces tengigabitethernet 0/0

TenGigabitEthernet 0/0 is up, line protocol is up
Hardware is Force10Eth, address is 00:01:e8:3a:2c:3e
    Current address is 00:01:e8:3a:2c:3e
Pluggable media present, Media type is unknown
    Wavelength is 1310.00nm
Interface index is 33882185
Internet address is not set
MTU 9252 bytes, IP MTU 9234 bytes
LineSpeed 10000 Mbit
Flowcontrol rx on tx on
ARP type: ARPA, ARP Timeout 04:00:00
Last clearing of "show interface" counters 00:15:14
Queueing strategy: fifo
Input Statistics:
     4410013700 packets, 282240876800 bytes
     0 Vlans
     4410013700 64-byte pkts, 0 over 64-byte pkts, 0 over 127-byte pkts
     0 over 255-byte pkts, 0 over 511-byte pkts, 0 over 1023-byte pkts
     0 Multicasts, 0 Broadcasts
     0 runts, 0 giants, 0 throttles
     0 CRC, 0 overrun, 0 discarded
Output Statistics:
     857732 packets, 54894848 bytes, 0 underruns
     857732 64-byte pkts, 0 over 64-byte pkts, 0 over 127-byte pkts
     0 over 255-byte pkts, 0 over 511-byte pkts, 0 over 1023-byte pkts
     24 Multicasts, 0 Broadcasts, 857708 Unicasts
     0 Vlans,0 throttles, 0 discarded, 0 collisions, 4409143619 wredDrops
Rate info (interval 30 seconds):
     Input 00.00 Mbits/sec,          0 packets/sec, 0.00% of line-rate
     Output 00.00 Mbits/sec,          0 packets/sec, 0.00% of line-rate
Time since last interface status change: 00:12:14
Force10#
```

Figure 184 show interfaces Command Example (TeraScale)

Table 30 defines the information displayed in Figure 184.

Table 30 Lines in show interfaces Command Example (TeraScale)

Line	Description
TenGigabitEthernet 1/0...	Displays the interface's type, slot/port and administrative and line protocol status.
Hardware is...	Displays the interface's hardware information, its assigned MAC address, and current address.
Pluggable media present...	Displays the present pluggable media wavelength, type, and rate. The error scenarios are: • Wavelength, Non-qualified — F10 ID is not present, but wavelength information is available from XFP serial data • Wavelength, F10 unknown—F10 ID is present, but not able to determine the optics type • Unknown, Non-qualified— if wavelength is reading error, and F10 ID is not present
Interface index...	Displays the interface index number used by SNMP to identify the interface.
Internet address...	States whether an IP address is assigned to the interface. If one is, that address is displayed.
MTU 1554...	Displays link and IP MTU information.
LineSpeed	Displays the interface's line speed, duplex mode, and Slave

Table 30 Lines in show interfaces Command Example (TeraScale)

Line	Description
ARP type:...	Displays the ARP type and the ARP timeout value for the interface.
Last clearing...	Displays the time when the **show interfaces** counters where cleared.
Queuing strategy...	States the packet queuing strategy. FIFO means first in first out.
Input Statistics:	Displays all the input statistics including: • the number of packets and bytes into the interface • the number of packets with VLAN tagged headers • the packet size and the number of those packets inbound to the interface • the number of Multicast and Broadcast packets: Multicasts = number of MAC multicast packets Broadcasts = number of MAC broadcast packets • the number of runts, giants, and throttles packets: runts = number of packets that are less than 64B giants = packets that are greater than the MTU size throttles = packets containing PAUSE frames • the number of CRC, overrun, and discarded packets: CRC = packets with CRC/FCS errors overrun = number of packets discarded due to FIFO overrun conditions discarded = the sum of runts, giants, CRC, and overrun packets discarded without any processing
Output Statistics:	Displays output statistics sent out the interface including: • the number of packets, bytes and underruns out of the interface • the packet size and the number of those packets outbound to the interface • the number of Multicast, Broadcast and Unicast packets: Multicasts = number of MAC multicast packets Broadcasts = number of MAC broadcast packets Unicasts = number of MAC unicast packets • the number of VLANs, throttles, discards, and collisions: Vlans = number of VLAN tagged packets throttles = packets containing PAUSE frames discarded = number of packets discarded without any processing collisions = number of packet collisions wred=count both packets discarded in the MAC and in the hardware-based queues
Rate information...	Displays an estimate of the input and output traffic rate over a designated interval (30 to 299 seconds) Traffic rate is displayed in bits, packets per second, and percent of line rate.
Time since...	Displays the elapse time since the last interface status change (hh:mm:ss format).

Related Commands

show interfaces switchport	View Layer 2 information about the interfaces.
show ip interface	View Layer 3 information about the interfaces.

show interfaces configured

View an interface with non-default configurations.

Syntax **show interfaces configured**

Command Modes EXEC

EXEC privilege

Command History

Version 6.4.1.0	Changed organization of display output

Example

```
Force10#show interfaces configured
GigabitEthernet 13/18 is up, line protocol is up
Hardware is Force10Eth, address is 00:01:e8:05:f7:fc
    Current address is 00:01:e8:05:f7:fc
Interface index is 474791997
Internet address is 1.1.1.1/24
MTU 1554 bytes, IP MTU 1500 bytes
LineSpeed 1000 Mbit, Mode full duplex, Master
ARP type: ARPA, ARP Timeout 04:00:00
Last clearing of "show interfaces" counters 00:12:42
Queueing strategy: fifo
Input Statistics:
     10 packets, 10000 bytes
     0 Vlans
     0 64-byte pkts, 0 over 64-byte pkts, 0 over 127-byte pkts
     0 over 255-byte pkts, 10 over 511-byte pkts, 0 over 1023-byte pkts
     0 Multicasts, 0 Broadcasts
     0 runts, 0 giants, 0 throttles
     0 CRC, 0 overrun, 0 discarded
Output Statistics:
     1 packets, 64 bytes, 0 underruns
     1 64-byte pkts, 0 over 64-byte pkts, 0 over 127-byte pkts
     0 over 255-byte pkts, 0 over 511-byte pkts, 0 over 1023-byte pkts
     0 Multicasts, 1 Broadcasts, 0 Unicasts
     0 Vlans, 0 throttles, 0 discarded, 0 collisions
Rate info (interval 299 seconds):
     Input 00.00 Mbits/sec,          0 packets/sec, 0.00% of line-rate
     Output 00.00 Mbits/sec,          0 packets/sec, 0.00% of line-rate
Time since last interface status change: 00:04:59
Force10#
```

Related Commands

show interfaces	View interface configuration

show interfaces dampening

View interface dampening information.

Syntax **show interface dampening** [[*interface*] [**summary**] [**detail**]]

Parameters

interface	(Optional) Enter one of the following keywords and slot/port or number information: • For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For a Port Channel interface, enter the keyword **port-channel** followed by a number: C-Series Range: 1-128 on the C300 E-Series Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale • For a SONET interface, enter the keyword **sonet** followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information. .
summary	(OPTIONAL) Enter the keyword **summary** to view the current summary of dampening information including the number of interfaces configured and the number of interfaces suppressed, if any.
detail	(OPTIONAL) Enter the keyword **detail** view detailed information of interface dampening.

Defaults No default values or behavior

Command Modes EXEC

Command History

Version 7.4.1.0	Introduced

Example

```
Force10#show interface dampening
Interface     Supp     Flaps     Penalty     Half-Life    Reuse     Suppress    Max-Sup
              State
Gi 3/2        Up       0         0           20           800       4500        120
Gi 3/10       Up       0         0           5            750       2500        20
Force10#
```

Related Commands

dampening	Configure dampening on an interface

show interfaces description

View the descriptions configured on the interface.

Syntax **show interfaces** [*interface*] **description**

Parameters

interface	Enter one of the following keywords and slot/port or number information: • For a Fast Ethernet interface, enter the keyword **FastEthernet** followed by the slot/port information. • For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For Loopback interfaces, enter the keyword **loopback** followed by a number from 0 to 16383. • For the management interface on the RPM, enter the keyword **ManagementEthernet** followed by the slot/port information. The slot range is 0-1 and the port range is 0. • For the Null interface, enter the keywords **null 0**. • For a Port Channel interface, enter the keyword **port-channel** followed by a number: C-Series Range: 1-128 on the C300 E-Series Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale • For SONET interfaces, enter the keyword **sonet** followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information. • For VLAN interfaces, enter the keyword **vlan** followed by a number from 1 to 4094.

Command Modes EXEC

EXEC privilege

Example

```
Force10>
Interface               OK? Status     Protocol    Description
GigabitEthernet 4/17    NO  admin down down        ***connected-to-host***
GigabitEthernet 4/18    NO  admin down down        ***connected-to-Tom***
GigabitEthernet 4/19    NO  admin down down        ***connected-to-marketing***
GigabitEthernet 4/20    NO  admin down down        ***connected-to-Bill***
GigabitEthernet 4/21    NO  up         down       ***connected-to-Radius-Server***
GigabitEthernet 4/22    NO  admin down down        ***connected-to-Web-Server***
GigabitEthernet 4/23    NO  admin down down        ***connected-to-PC-client***
TenGigabitEthernet 6/0  NO  admin down down
GigabitEthernet 8/0     YES up         up
GigabitEthernet 8/1     YES up         up
GigabitEthernet 8/2     YES up         up
GigabitEthernet 8/3     YES up         up
GigabitEthernet 8/4     YES up         up
GigabitEthernet 8/5     YES up         up
GigabitEthernet 8/6     YES up         up
GigabitEthernet 8/7     YES up         up
GigabitEthernet 8/8     YES up         up
GigabitEthernet 8/9     YES up         up
GigabitEthernet 8/10    YES up         up
GigabitEthernet 8/11    YES up         up
Force10>
```

Figure 185 show interfaces description Command Example

Table 31 defines the fields in Figure 185.

Table 31 show interfaces description Command Example Fields

Field	Description
Interface	Displays type of interface and associated slot and port number.
OK?	Indicates if the hardware is functioning properly.
Status	States whether the interface is enabled (up) or disabled (administratively down).
Protocol	States whether IP is enabled (up) or disabled (down) on the interface.
Description	Displays the description (if any) manually configured for the interface.

show interfaces linecard

View information on all interfaces on a specific line card.

Syntax **show interfaces linecard** *slot-number*

Parameters

slot-number	Enter a number for the line card slot. C-Series Range: 0-7 on the C300 E-Series Range: 0 to 13 for the E1200, 0 to 6 for the E600, 0 to 5 for the E300

Command Modes EXEC

EXEC privilege

Related Commands

show interfaces	View interface configuration

show interfaces status

View a summary of interface information or specify a line card slot and interface to view status information on that specific interface only.

Syntax **show interfaces** [*interface* | **linecard** *slot-number*] **status**

Parameters

interface	(OPTIONAL) Enter one of the following keywords and slot/port or number information: • For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information.
linecard *slot-number*	(OPTIONAL) Enter the keyword **linecard** followed by the slot number. C-Series Range: 0 to 7 on the C300 E-Series Range: 0 to 13 for the E1200, 0 to 6 for the E600, 0 to 5 for the E300

Defaults No default behavior or values

Command Modes EXEC

Command History

Version 7.5.1.0	Introduced

Example

```
Force10#show interfaces status
Port     Description  Status Speed     Duplex Vlan
Gi 0/0                Up     1000 Mbit Auto   --
Gi 0/1                Down   Auto      Auto   1
Gi 0/2                Down   Auto      Auto   1
Gi 0/3                Down   Auto      Auto   --
Gi 0/4   Force10Port  Up     1000 Mbit Auto   30-130
Gi 0/5                Down   Auto      Auto   --
Gi 0/6                Down   Auto      Auto   --
Gi 0/7                Up     1000 Mbit Auto   1502,1504,1506-1508,1602
Gi 0/8                Down   Auto      Auto   --
Gi 0/9                Down   Auto      Auto   --
Gi 0/10               Down   Auto      Auto   --
Gi 0/11               Down   Auto      Auto   --
Gi 0/12               Down   Auto      Auto   --
Gi 0/13               Down   Auto      Auto   --
Gi 0/14               Down   Auto      Auto   --
Gi 0/15               Down   Auto      Auto   --
Force10#
```

Figure 186 show interfaces status Command Example

show interfaces switchport

View only virtual and physical interfaces in Layer 2 mode. This command displays the Layer 2 mode interfaces' IEEE 802.1Q tag status and VLAN membership.

Syntax **show interfaces switchport** [*interface*] [**linecard** *slot-number*]

Parameters

interface	Enter one of the following keywords and slot/port or number information: • For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For a Port Channel interface, enter the keyword **port-channel** followed by a number: C-Series Range: 1-128 on the C300 E-Series Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale • For SONET interfaces, enter the keyword **sonet** followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information.
linecard *slot-number*	(OPTIONAL) Enter the keyword **linecard** followed by the slot number. C-Series Range: 0-7 on the C300 E-Series Range: 0 to 13 for the E1200, 0 to 6 for the E600, 0 to 5 for the E300

Command Modes

EXEC

EXEC privilege

Example

```
Force10#show interfaces switchport
Name: GigabitEthernet 13/0
802.1QTagged: True
Vlan membership:
Vlan    2


Name: GigabitEthernet 13/1
802.1QTagged: True
Vlan membership:
Vlan    2


Name: GigabitEthernet 13/2
802.1QTagged: True
Vlan membership:
Vlan    2


Name: GigabitEthernet 13/3
802.1QTagged: True
Vlan membership:
Vlan    2


--More--
```

Figure 187 show interfaces switchport Command Example

Table 32 defines the output that appears in Figure 187.

Table 32 Items in show interfaces switchport Command Example

Items	Description
Name:	Displays the interface's type, slot and port number.
802.1QTagged:	Displays whether if the VLAN tagged (`true`) or untagged (`false`).
Vlan membership:	Lists the VLANs to which the interface is a member.

Related Commands

show ip interface	Displays Layer 3 information about the interfaces.

show range

Displays all interfaces configured using the interface range command.

Syntax **show range**

Command Modes CONFIGURATION INTERFACE (config-if-range)

Command History

Version 6.1.1.0	Introduced

Example

```
Force10(conf-if-range-so-2/0-1,fa-0/0)#show range
interface sonet 2/0 - 1
interface fastethernet 0/0
Force10(conf-if-range-so-2/0-1,fa-0/0)#
```

Figure 188 show range Command Example

shutdown

Disable an interface.

Syntax **shutdown**

To activate an interface, enter **no shutdown**.

Defaults Enabled (that is, the interface is disabled)

Command Modes INTERFACE

Usage Information The shutdown command marks a physical interface as unavailable for traffic. To discover if an interface is disabled, use the show ip interface brief command. Disabled interfaces are listed as down.

Disabling a VLAN or a Port Channel causes different behavior. When a VLAN is disabled the Layer 3 functions within that VLAN are disabled. Layer 2 traffic continues to flow. Entering the shutdown command on a Port Channel disables all traffic on the Port Channel and the individual interfaces within the Port Channel. To enable a Port Channel, you must enter no shutdown on the Port Channel interface and at least one interface within that Port Channel.

The shutdown and description commands are the only commands that you can configure on an interface that is a member of a Port Channel.

Related Commands

show ip interface	Displays the interface routing status. Add the keyword **brief** to view a table of interfaces and their status.

speed (10/100/1000 Interfaces)

Set the speed for 10/100/1000 Base-T Ethernet interfaces. Both sides of a link must be set to the same speed (10/100/1000) or to auto or the link may not come up.

Syntax **speed** {**10** | **100** | **1000** | **auto**}

To return to the default setting, use the **no speed** {**10** | **100** | **1000**} command.

Parameters

10	Enter the keyword **10** to set the interface's speed to 10 Mb/s.
100	Enter the keyword **100** to set the interface's speed to 10/100 Mb/s.
1000	Enter the keyword **1000** to set the interface's speed to 1000 Mb/s. (Auto negotiation is enabled. See negotiation auto for more information)
auto	Enter the keyword **auto** to set the interface to auto negotiate its speed. (Auto negotiation is enabled. See negotiation auto for more information)

Defaults **auto**

Command Modes INTERFACE

Usage Information This command is found on the 10/100/1000 Base-T Ethernet interfaces.

When you configure a speed for the 10/100/1000 interface, you should confirm negotiation auto command setting. Both sides of the link should have auto negotiation either enabled or disabled. For speed settings of 1000 or auto, the software sets the link to auto negotiation, and you cannot change that setting.

Related Commands

negotiation auto	Enable or disable auto negotiation on an interface.

speed (Management interface)

Set the speed for the Management interface.

Syntax **speed** {**10** | **100** | **auto**}

To return to the default setting, use the **no speed** {**10** | **100**} command.

Parameters

10	Enter the keyword **10** to set the interface's speed to 10 Mb/s.
100	Enter the keyword **100** to set the interface's speed to 100 Mb/s.
auto	Enter the keyword **auto** to set the interface to auto negotiate its speed.

Defaults **auto**

Command Modes INTERFACE

Usage Information This command is found on the Management interface only.

switchport

Place the interface to Layer 2 mode.

Syntax **switchport**

To disable switchport and place the interface in Layer 3 mode, enter **no switchport**.

Defaults Disabled (that is, interfaces are in Layer 3 mode)

Command Modes INTERFACE

Usage Information

If an IP address or VRRP group is assigned to the interface, you cannot use the switchport command for that interface. To use the switchport command on an interface, only the **no ip address** and **no shutdown** statements must be listed in the **show config** for that command.

When you enable the switchport command, the interface is automatically added to the Default VLAN.

WAN Port

C-Series	**No**
E-Series	✔

Enable the WAN mode on a TenGigabitEthernet interface.

Syntax **wanport**

To disable the WAN Port, enter **no wanport**.

Defaults Not configured.

Command Modes CONFIGURATION

Usage Information The port must be in a shutdown state to change from LAN mode to WAN mode and vice-versa as shown in Figure 189.

Example

```
interface TenGigabitEthernet 13/0
 no ip address
 no shutdown
Force10(conf-if-te-13/0)#
Force10(conf-if-te-13/0)#wanport
% Error: Port should be in shutdown mode, config ignored Te 13/0.
Force10(conf-if-te-13/0)#
Force10(conf-if-te-13/0)#shutdown
Force10(conf-if-te-13/0)#
Force10(conf-if-te-13/0)#wanport
Force10(conf-if-te-13/0)#
```

Figure 189 wanport command with shutdown command

Related Commands

ais-shut	Send LAIS on shutdown
alarm-report	Enable reporting of a selected alarm
clock source	Configure a clock source
down-when-looped	Send a message when a loopback condition is detected
flag	Set flags to ensure interoperability

framing	Set framing type
keepalive	Enable keepalive
loopback	Troubleshoot a SONET loopback

Port Channel-Specific Commands

A Link Aggregation Group (LAG) is a group of links that appear to a MAC client as if they were a single link according to IEEE 802.3ad. In FTOS, a LAG is referred to as a Port Channel interface.

Note: The FTOS implementation of LAG or Port Channel requires that you configure LAG on both switches manually. For information on FTOS Link Aggregation Control Protocol (LACP) refer to Chapter 19, “LACP,” on page 521.

For more information on configuring and using Port Channels, refer to the *FTOS Configuration Guide*. The commands listed here are specific to Port Channel interfaces.

- channel-member on page 500
- minimum-links on page 501
- show interfaces port-channel on page 502
- show port-channel-flow on page 505

channel-member

Add an interface to the Port Channel, while in the INTERFACE PORTCHANNEL mode.

Syntax **channel-member** *interface*

To delete an interface from a Port Channel, use the **no channel-member** *interface* command.

Parameters

interface	Enter the following keywords and slot/port or number information: • For a 100/1000 Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For a Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For a SONET interface, enter the keyword **sonet** followed by the slot/port information. • For a Ten Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information.

Defaults Not configured.

Command Modes INTERFACE PORTCHANNEL

Usage Information You cannot add an interface to a Port Channel if the interface contains an IP address in its configuration. Only the shutdown, description, mtu, and ip mtu commands can be configured on an interface if it is to be added to a Port Channel. The mtu and ip mtu commands are only available when the chassis is in Jumbo mode.

Link MTU and IP MTU considerations for Port Channels are:

- All members must have the same link MTU value and the same IP MTU value.
- The Port Channel link MTU and IP MTU must be less than or equal to the link MTU and IP MTU values configured on the channel members.

Example: if the members have a link MTU of 2100 and an IP MTU 2000, the Port Channel's MTU values cannot be higher than 2100 for link MTU or 2000 bytes for IP MTU.

When an interface is removed from a Port Channel with the no channel-member command syntax, the interface reverts to its configuration prior to joining the Port Channel.

An interface can belong to only one Port Channel.

You can add up to 16 interfaces to a Port Channel. The interfaces can be located on different line cards but must be the same physical type and speed (for example, all 1-Gigabit Ethernet interfaces). However, you can combine 100/1000 interfaces and GE interfaces in the same Port Channel.

If the Port Channel contains a mix of interfaces with 100 Mb/s speed and 1000 Mb/s speed, the software disables those interfaces whose speed does not match the speed of the first interface configured and enabled in the Port Channel. If that first interface goes down, the Port Channel does not change its designated speed; you must disable and re-enable the Port Channel or change the order of the channel members configuration to change the designated speed. Refer to the *FTOS Configuration Guide* for more information on Port Channels.

minimum-links

Configure the minimum number of links in a LAG (Port Channel) that must be in "oper up" status for the LAG to be also in "oper up" status.

Syntax **minimum-links** *number*

Parameters

number	Enter the number of links in a LAG that must be in "oper up" status. Range: 1 to 16 Default: 1

Defaults 1

Command Modes INTERFACE

Usage Information If you use this command to configure the minimum number of links in a LAG that must be in "oper up" status, then the LAG must have at least that number of "oper up" links before it can be declared as up.

For example, if the required minimum is four, and only three are up, then the LAG will be considered down.

show interfaces port-channel

View information on configured Port Channel groups.

Syntax **show interfaces port-channel** [*channel-number*] [**brief**]

Parameters

channel-number	(OPTIONAL) Enter the number of the Port Channel to view information on that Port Channel: C-Series Range: 1-128 on the C300 E-Series Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale
brief	(OPTIONAL) Enter the keyword **brief** to view only the Port Channel number, the state of the Port Channel, and the number of interfaces in the Port Channel. Refer to Figure 191.

Command Modes EXEC

EXEC privilege

Example

```
Force10#show interfaces port-channel 20
Port-channel 20 is up, line protocol is up
Hardware address is 00:01:e8:01:46:fa
Internet address is 1.1.120.1/24
MTU 1554 bytes, IP MTU 1500 bytes
LineSpeed 2000 Mbit
Members in this channel:  Gi 0/5 Gi 0/18
ARP type: ARPA, ARP timeout 04:00:00
Last clearing of "show interfaces" counters 00:00:00
Queueing strategy: fifo
     44507301 packets input, 3563070343 bytes
     Input 44506754 IP Packets, 0 Vlans 0 MPLS
     41 64-byte pkts, 44502871 over 64-byte pkts, 249 over 127-byte pkts
     407 over 255-byte pkts, 3127 over 511-byte pkts, 606 over 1023-byte pkts
     Received 0 input symbol errors, 0 runts, 0 giants, 0 throttles
     0 CRC, 0 IP Checksum, 0 overrun, 0 discarded
     1218120 packets output, 100745130 bytes, 0 underruns
     Output 5428 Multicasts, 4 Broadcasts, 1212688 Unicasts
     1216142 IP Packets, 0 Vlans, 0 MPLS
     0 throttles, 0 discarded
Rate info (interval 299 sec):
     Input 01.50Mbits/sec,       2433 packets/sec
     Output 00.02Mbits/sec,          4 packets/sec
Time since last interface status change: 00:22:34

Force10#
```

Figure 190 show interfaces port-channel Command Example

Table 33 defines the output displayed in Figure 190.

Table 33 show interfaces port-channel Command Example Fields

Field	Description
Port-Channel 1...	Displays the interface's type, slot/port, and physical and line protocol status.
Hardware is...	Displays the interface's hardware information and its assigned MAC address.
Internet address...	States whether an IP address is assigned to the interface. If one is, that address is displayed.
MTU 1554...	Displays link and IP MTU.
LineSpeed	Displays the interface's line speed. For a Port Channel interface, it is the line speed of the interfaces in the Port Channel.
Members in this ...	Displays the interfaces belonging to this Port Channel.
ARP type:...	Displays the ARP type and the ARP timeout value for the interface.
Last clearing...	Displays the time when the **show interfaces** counters were cleared.
Queueing strategy..	States the packet queuing strategy. FIFO means first in first out.
packets input ...	Displays the number of packets and bytes into the interface.
Input 0 IP packets...	Displays the number of packets with IP headers, VLAN tagged headers and MPLS headers. The number of packets may not add correctly because a VLAN tagged IP packet counts as both a VLAN packet and an IP packet.
0 64-byte...	Displays the size of packets and the number of those packets entering that interface. This information is displayed over two lines.
Received 0...	Displays the type and number of errors or other specific packets received. This information is displayed over three lines.

Table 33 show interfaces port-channel Command Example Fields (continued)

Field	Description
Output 0...	Displays the type and number of packets sent out the interface. This information is displayed over three lines.
Rate information...	Displays the traffic rate information into and out of the interface. Traffic rate is displayed in bits and packets per second.
Time since...	Displays the time since the last change in the configuration of this interface.

```
Force10#sh int por 1 br

LAG Mode  Status       Uptime     Ports
1   L2    up           00:00:08   Gi 3/0      (Up) *
                                  Gi 3/1      (Down)
                                  Gi 3/2      (Up)
Force10#
```

Figure 191 show interfaces port-channel brief Command Example

Table 34 defines the output information in Figure 191.

Table 34 show interfaces port-channel brief Command Example Fields

Field	Description
LAG	Lists the Port Channel number.
Mode	Lists the mode: • L3 - for Layer 3 • L2 - for Layer 2
Status	Displays the status of the Port Channel. • down - if the Port Channel is disabled (shutdown) • up - if the Port Channel is enabled (no shutdown)
Uptime	Displays the age of the Port Channel in hours:minutes:seconds.
Ports	Lists the interfaces assigned to this Port Channel.
(untitled)	Displays the status of the physical interfaces (`up` or `down`). In Layer 2 Port Channels, an * (asterisk) indicates which interface is the primary port of the Port Channel. The primary port sends out interface PDU. In Layer 3 Port Channels, the primary port is not indicated.

show port-channel-flow

View an egress port in a given port-channel flow.

Syntax **show port-channel-flow outgoing-port-channel** *number* **incoming-interface** *interface* {**source-ip** *address* **destination-ip** *address*} | {**protocol** *number* | **icmp** | **tcp** |**udp**} | {**source-port** *number* **destination-port** *number*} | {**source-mac** *address* **destination-mac** *address*}

Parameters

outgoing-port-channel *number*	Enter the keyword **outgoing-port-channel** followed by the number of the Port Channel to view flow information. • For a Port Channel interface, enter the keyword **port-channel** followed by a number: C-Series Range: 1-128 on the C300 E-Series Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale
incoming-interface *interface*	Enter the keyword **incoming-interface** followed by the interface type and slot/port or number information: • For a Fast Ethernet interface, enter the keyword **FastEthernet** followed by the slot/port information. • For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For a SONET interface, enter the keyword **sonet** followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information.
source-ip *address*	Enter the keyword **source-ip** followed by the IP source address in IP address format.
destination-ip *address*	Enter the keyword **destination-ip** followed by the IP destination address in IP address format.
protocol *number* | **icmp** | **tcp** | **udp**	Enter the keyword **protocol** followed by the protocol number or one of the applicable keywords **ICMP**, **TCP** or **UDP**.
source-port *number*	Enter the keyword **source-port** followed by the source port number. Range: 1-65536 Default: None
destination-port *number*	Enter the keyword **destination-port** followed by the destination port number. Range: 1-65536 Default: None
source-mac *address*	Enter the keyword **source-mac** followed by the MAC source address in the nn:nn:nn:nn:nn:nn format.
destination-mac *address*	Enter the keyword **destination-mac** followed by the MAC destination address in the nn:nn:nn:nn:nn:nn format.

Command Modes EXEC

Usage Information

Since this command calculates based on a Layer 2 hash algorithm, use this command to display flows for switched Layer 2 packets, *not* for routed packets (use the **show ip flow** command to view routed packets).

The **show port-channel-flow** command returns the egress port identification in a given port-channel, if a valid flow is entered. Mismatched flow error will occur if MAC-based hashing is configured for a Layer 2 interface and the user is trying to view a Layer 3 flow.

The output will display three entries:

- Egress port for unfragmented packets.
- In the event of fragmented packets, egress port of the first fragment.
- In the event of fragmented packets, egress port of the subsequent fragments.

Example 1

show port-channel-flow outgoing-port-channel *number* **incoming-interface** *interface* **source-mac** *address* **destination-mac** *address*

- Load-balance is configured for MAC
- A non-IP payload is going out of Layer 2 LAG interface that is a member of VLAN with an IP address.

The output is shown in Figure 192.

```
Force10#show port-channel-flow outgoing-port-channel 1 incoming-interface gi 3/0
source-mac 00:00:50:00:00:00 destination-mac 00:00:a0:00:00:00

    Egress Port for port-channel 1, for the given flow, is Te 13/01
```

Figure 192 show port-channel-flow Command for MAC

Example 2

show port-channel-flow outgoing-port-channel *number* **incoming-interface** *interface* **source-ip** *address* **destination-ip** *address* {**protocol** *number* [**icmp**/**tcp**/**udp**]} {**source-port** *number* **destination-port** *number*}

- Load-balance is configured for IP 5-tuple/3-tuple
- An IP payload is going out of Layer 2 LAG interface that is a member of VLAN with an IP address:

The output is shown in Figure 193.

```
Force10#show port-channel-flow outgoing-port-channel 2 incoming-interface gi 3/0
source-ip 2.2.2.0 destination-ip 3.2.3.1 protocol tcp source-port 5
destination-port 6

    Egress Port for port-channel 2, for the given flow:
    Unfragmented packet: Gi 1/6
    Fragmented packets (first fragment): Gi 1/12
    Fragmented packets (remaining fragments): Gi 1/12
```

Figure 193 show port-channel-flow Command for TCP

Related Commands		
	load-balance (E-Series)	Balance traffic over Port Channel members.

Port Mirroring (Deprecated)

FTOS Port Mirroring feature is replaced with the expanded Port Monitoring feature (Chapter 18, “Port Monitoring,” on page 515) beginning with FTOS version 7.4.1.0.

- mirroring source port (deprecated) (Deprecated)
- show run mirroring (deprecated) (Deprecated)

mirroring source port (deprecated)

Command History		
	Version 7.4.1.0	Deprecated
	Version 6.2.1.1	Introduced

show run mirroring (deprecated)

Command History		
	Version 7.4.1.0	Deprecated
	Version 6.2.1.1	Introduced

Time Domain Reflectometer (TDR)

Platform Specific Feature: Time Domain Reflectometer is supported on the E-Series only.

TDR is useful for troubleshooting an interface that is not establishing a link; either it is flapping or not coming up at all. TDR detects open or short conditions of copper cables on 100/1000 Base-T modules.

- tdr-cable-test on page 508
- show tdr on page 509

Important Points to Remember

- The interface and port must be enabled (configured) before running TDR (interface). An error message is generated if you have not enabled the interface.
- The interface on the Far-End device must be shut down before running TDR.
- Since TDR is an intrusive test on an interface that is not establishing a link, do not run TDR on an interface that is passing traffic.
- When testing between two devices, do not run the test on both ends of the cable.

tdr-cable-test

C-Series	**No**
E-Series	✓

Test the condition of copper cables on 100/1000 Base-T modules.

Syntax **tdr-cable-test** *interface*

Parameters

interface	Enter the keyword **GigabitEthernet** followed by the slot/port information for the 100/1000 Ethernet interface.

Defaults No default behavior or setting

Command Modes EXEC

Command History

Version 6.1.1.0	Introduced

Usage Information The interface must be enabled to run the test or an error messages is generated:

```
Force10#tdr-cable-test gigabitethernet 5/2
%Error: Interface is disabled GI 5/2
```

Related Commands

show tdr	Display the results of the TDR test.

show tdr

C-Series	No
E-Series	✓

Display the TDR test results.

Syntax **show tdr** *interface*

Parameters

interface	Enter the keyword **GigabitEthernet** followed by the slot/port information for the 100/1000 Ethernet interface.

Defaults No default behavior or settings

Command Modes EXEC

Command History

Version 6.1.1.0	Introduced

Example

```
Force10#show tdr gigabitethernet 10/47
Time since last test: 00:00:02
  Pair A, Length: OK Status: Terminated
  Pair B, Length: 92 (+/- 1) meters, Status: Short
  Pair C, Length: 93 (+/- 1) meters, Status: Open
  Pair D, Length: 0 (+/- 1) meters, Status: Impedance Mismatch
```

Figure 194 show tdr gigabitethernet Command Example

Table 35 list the TDR test results displayed in Figure 194.

Table 35 TDR Test Status

Status	Definition
OK Status: Terminated	TDR test is complete, no fault is detected on the cable, and the test is terminated
Length: 92 (+/- 1) meters, Status: Shorted	A short is detected on the cable. The location, in this example 92 meters, of the short is accurate to plus or minus one meter.
Length: 93 (+/- 1) meters, Status: Open	An opening is detected on the cable. The location, in this example 93 meters, of the open is accurate to plus or minus one meter.
Status: Impedance Mismatch	There is an impedance mismatch in the cables.

Usage Information If the TDR test has not been run, an error messages is generated:

```
%Error: Please run the TDR test first
```

Related Commands		
	tdr-cable-test	Run the TDR test.

UDP Broadcast

C-Series	NO
E-Series	✓

Platform Specific Feature: This feature is supported on the E-Series only.

The User Datagram Protocol (UDP) broadcast feature is a software-based method to forward low throughput (not to exceed 200 pps) IP/UDP broadcast traffic arriving on a physical or VLAN interface.

The commands for UDP Broadcast are:

- debug ip udp-helper on page 510
- ip udp-broadcast-address on page 511
- ip udp-helper udp-port on page 512
- show ip udp-helper on page 512

Important Points to Remember

- This feature is applied to TeraScale Layer 3 physical or VLAN interfaces.
- Routing Information Protocol (RIP) is not supported with UDP Broadcast feature.
- If this feature is configured on an interface using ip udp-helper udp-port, then the command ip directed-broadcast becomes ineffective on that interface.
- The existing command show interface has been modified to display the configured broadcast address.

debug ip udp-helper

C-Series	No
E-Series	✓

Enable UDP debug and display the debug information on a console.

Syntax **debug ip udp-helper**

To disable debug information, use the **no debug ip udp-helper** command.

Defaults Debug disabled

Command Modes EXEC

EXEC Privilege

Example

```
Force10#debug ip udp-helper
UDP helper debugging is on

01:20:22: Pkt rcvd on Gi 5/0 with IP DA (0xffffffff) will be sent on Gi 5/1 Gi 5/2
Vlan 3

01:44:54: Pkt rcvd on Gi 7/0 is handed over for DHCP processing.
```

Figure 195 Debug Output Example

Related Commands

ip udp-broadcast-address	Configure a UDP IP address for broadcast
ip udp-helper udp-port	Enable the UDP broadcast feature on an interface.
show ip udp-helper	Display the configured UDP helper(s) on all interfaces.

ip udp-broadcast-address

C-Series	No
E-Series	✓

Configure an IP UDP address for broadcast.

Syntax **ip udp-broadcast-address** *address*

To delete the configuration, use the **no ip udp-broadcast-address** *address* command.

Parameters

address	Enter an IP broadcast address in dotted decimal format (A.B.C.D).

Defaults Not Configured

Command Modes INTERFACE (config-if)

Usage Information When a UDP broadcast packet is flooded out of an interface, and the outgoing interface is configured using this command, the outgoing packet's IP destination address is replaced with the configured broadcast address.

Related Commands

debug ip udp-helper	Enable debug and display the debug information on a console.
show ip udp-helper	Display the configured UDP helper(s) on all interfaces.

ip udp-helper udp-port

C-Series	No
E-Series	✓

Enable the UDP broadcast feature on an interface either for all UDP ports or a specified list of UDP ports.

Syntax

ip udp-helper udp-port [*udp-port-list*]

To disable the UDP broadcast on a port, use the **no ip udp-helper udp-port** [*udp-port-list*] command.

Parameters

udp-port-list	(OPTIONAL) Enter up to 16 comma separated UDP port numbers. **Note:** If this option is not used, all UDP Ports are considered by default.

Defaults

No default behavior or values

Command Modes

INTERFACE (config-if)

Usage Information

If the **ip helper-address** command and **ip udp-helper udp-port** command are configured, the behavior is that the UDP broadcast traffic with port numbers 67/68 will be unicast relayed to the DHCP server per the **ip helper-address** configuration. This will occur regardless if **ip udp-helper udp-port** command contains port numbers 67/68 or not.

If only the **ip udp-helper udp-port** command is configured, all the UDP broadcast traffic is flooded, including ports 67/68 traffic if those ports are part of the *udp-port-list*.

Related Commands

ip helper-address	Configure the destination broadcast or host address for DHCP server.
debug ip udp-helper	Enable debug and display the debug information on a console.
show ip udp-helper	Display the configured UDP helper(s) on all interfaces.

show ip udp-helper

C-Series	No
E-Series	✓

Display the configured UDP helper(s) on all interfaces.

Syntax

show ip udp-helper

Defaults

No default configuration or values

Command Modes

EXEC

Example

```
Force10#show ip udp-helper
-------------------------------------------------
Port     UDP port list
-------------------------------------------------
Gi 10/0  656, 658
Gi 10/1  All
```

Figure 196 show ip udp-helper command Example

Related Commands

debug ip udp-helper	Enable debug and display the debug information on a console.
ip udp-broadcast-address	Configure a UDP IP address for broadcast.
ip udp-helper udp-port	Enable the UDP broadcast feature on an interface either for all UDP ports or a specified list of UDP ports.

Chapter 18 Port Monitoring

Port Monitoring allows you to monitor network traffic by forwarding a copy of each incoming or outgoing packet from one port to another port.

- flow-based enable on page 515
- monitor session on page 516
- show config on page 517
- show monitor session on page 517
- show running-config monitor session on page 518
- source on page 519

Important Points to Remember

- On the E-Series, Port Monitoring is supported on TeraScale platforms only.
- A SONET port can only be configured as a monitored port.
- The Monitored and Monitoring ports must be on the same switch.
- Port Monitoring supports only one Monitored port from a single port pipe.
- Monitored ports from different sessions can set destination as the same Monitoring port.
- FTOS supports as many monitor sessions on a system as the number of port-pipes.
- Port Monitoring is supported on physical ports only. Logical interfaces, such as Port-Channel and VLANs are not supported.

Note: The Monitoring port should not be a part of any other configuration.

flow-based enable

Enable flow-based monitoring.

Syntax **flow-based enable**

To disable flow-based monitoring, use the **no flow-based enable** command.

Defaults Disabled, that is flow-based monitoring is not applied

Command Modes MONITOR SESSION (conf-mon-sess-*session-ID*)

Command History

Version 7.4.1.0	Introduced

Usage Information To monitoring traffic with particular flows ingressing/egressing the interface, appropriate ACLs can be applied in both ingress and egress direction.

Related Commands

monitor session	Enter the Monitor Session.

monitor session

Create a session for monitoring traffic.

Syntax **monitor session** *session-ID*

To delete a session, use the **no monitor session** *session-ID* command.

To delete all monitor sessions, use the **no monitor session** command.

Parameters

session-ID	Enter a session identification number. Range: 0 to 65535

Defaults No default values or behaviors

Command Modes MONITOR SESSION (conf-mon-sess-*session-ID*)

Command History

Version 7.4.1.0	Introduced

Example

```
Force10(conf)# monitor session 60
Force10(conf-mon-sess-60)
```

Usage Information All monitor sessions contain an implicit “mode interface,” that is, if no mode is designated, the mode is set to interface as shown in the example above.

Only one monitor session per port-pipe is allowed, therefore at most, only 28 monitor sessions can be enabled at any time.

The monitoring command is saved in the running configuration at the Monitor Session mode level and can be restored after a chassis reload.

Related Commands

show monitor session	Display the monitor session
show running-config monitor session	Display the running configuration of a monitor session

show config

Display the current monitor session configuration.

Syntax **show config**

Defaults No default values or behavior

Command Modes MONITOR SESSION (conf-mon-sess-*session-ID*)

Command History

Version 7.4.1.0	Introduced

Example

```
Force10(conf-mon-sess-11)#show config
!
monitor session 11
 source GigabitEthernet 10/0 destination GigabitEthernet 10/47 direction rx
Force10#
```

show monitor session

Display the monitor information of a particular session or all sessions.

Syntax **show monitor session** {*session-ID*}

To display the monitor information for all sessions, use the **show monitor session** command.

Parameters

session-ID	(OPTIONAL) Enter a session identification number. Range: 0 to 65535

Defaults No default values or behavior

Command Modes EXEC

EXEC privilege

Command History

Version 7.4.1.0	Introduced

Example

```
Force10#show monitor session 11

SessionID       Source       Destination     Direction      Mode
-----------     --------     -------------   ------------   -------
   11           Gi 10/0      Gi 10/47        rx             interface

Force10#
```

Related Commands

monitor session	Create a session for monitoring.

show running-config monitor session

Display the running configuration of all monitor sessions or a specific session.

Syntax **show running-config monitor session** {*session-ID*}

To display the running configuration for all monitor sessions, use just the **show running-config monitor session** command.

Parameters

session-ID	(OPTIONAL) Enter a session identification number. Range: 0 to 65535

Defaults No default values or behavior

Command Modes EXEC

EXEC privilege

Command History

Version 7.4.1.0	Introduced

Example

```
Force10#show running-config monitor session
!
monitor session 8
 source GigabitEthernet 10/46 destination GigabitEthernet 10/1 direction rx
!
monitor session 11
 source GigabitEthernet 10/0 destination GigabitEthernet 10/47 direction rx

Force10#show running-config monitor session 11
!
monitor session 11
 source GigabitEthernet 10/0 destination GigabitEthernet 10/47 direction rx
```

Usage Information

The monitoring command is saved in the running configuration at the Monitor Session mode level and can be restored after a chassis reload.

Related Commands

monitor session	Create a session for monitoring.
show monitor session	Display a monitor session.

source

Configure a monitor source.

Syntax

source *interface* **destination** *interface* **direction** {**rx** | **tx** | **both**}

To disable a monitor source, use the **no source** *interface* **destination** *interface* **direction** {**rx** | **tx** | **both**} **command**.

Parameters

interface	Enter the one of the following keywords and slot/port information: • For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information. • For a SONET interface, enter the keyword **sonet** followed by the slot/port information.
destination	Enter the keyword **destination** to indicate the interface destination.
direction {**rx** | **tx** | **both**}	Enter the keyword **direction** followed by one of the packet directional indicators. **rx** : to monitor receiving packets only **tx** : to monitor transmitting packets only **both** : to monitor both transmitting and receiving packets

Defaults

No default behavior or values

Command Modes MONITOR SESSION (conf-mon-sess-*session-ID*)

Command History

Version 7.4.1.0	Introduced

Example

```
Force10(conf-mon-sess-11)#source gi 10/0 destination gi 10/47 direction rx
Force10(conf-mon-sess-11)#
```

Usage Information

Note: A SONET port can only be configured as a monitored port.

Chapter 19 LACP

Force 10's implementation of Link Aggregation Control Protocol (LACP) is based on the standards specified in the IEEE 802.3 Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications.

Use the following commands for LACP:

- clear lacp counters on page 521
- debug lacp on page 522
- lacp long-timeout on page 523
- lacp port-priority on page 523
- lacp system-priority on page 524
- port-channel mode on page 524
- port-channel-protocol lacp on page 525
- show lacp on page 525

clear lacp counters

Clear the port-channel counters.

Syntax **clear lacp port-***channel-number* **counters**

Parameters

port-*channel-number*	Enter the Port Channel number to clear the counters. C-Series Range: 1-128 E-Series Range: 1-32 for EtherScale, 1-255 for TeraScale

Defaults Without a Port Channel specified, the command clears all Port Channel counters.

Command Modes EXEC

EXEC privilege

Command History

Version 6.2.1.1	Introduced

Related Commands

show lacp	Display the LACP matrix

debug lacp

Debug LACP (configuration, events etc.)

Syntax

debug lacp [**config** | **events** | **pdu** [**in** | **out** | [**interface** [**in** | **out**]]]]

To disable LACP debugging, use the **no debug lacp** [**config** | **events** | **pdu** [**in** | **out** | [**interface** [**in** | **out**]]]] command.

Parameters

config	(OPTIONAL) Enter the keyword **config** to debug LACP configuration information.
events	(OPTIONAL) Enter the keyword **events** to debug LACP event information.
pdu in | out	(OPTIONAL) Enter the keyword **pdu** to debug LACP Protocol Data Unit information. Optionally, enter an **in** or **out** parameter to: • Receive enter **in** • Transmit enter **out**
interface in | out	(OPTIONAL) Enter the following keywords and slot/port or number information: • For a 100/1000 Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For a Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For a SONET interface, enter the keyword **sonet** followed by the slot/port information. • For a Ten Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information. Optionally, enter an **in** or **out** parameter: • Receive enter **in** • Transmit enter **out**

Defaults

This command has no default values or behavior

Command Modes

EXEC

EXEC privilege

Command History

Version 6.2.1.1	Introduced

lacp long-timeout

Configure a long timeout period (30 seconds) for an LACP session.

Syntax **lacp long-timeout**

To reset the timout period to a short timeout (1 second), use the **no lacp long-timeout** command.

Defaults 1 second

Command Modes INTERFACE (conf-if-po-*number*)

Command History

Version 7.5.1.0	Introduced

Usage Information This command applies to dynamic port-channel interfaces only. When applied on a static port-channel, the command has no effect.

Related Commands

show lacp	Display the lacp configuration

lacp port-priority

Configure the port priority.

Syntax **lacp port-priority** *priority-value*

To return to the default setting, use the **no lacp port-priority** *priority-value* command.

Parameters

priority-value	Enter the port-priority value. The higher the value number the lower the priority. Range: 1 to 65535 Default: 32768

Defaults 32768

Command Modes INTERFACE

Command History

Version 6.2.1.1	Introduced

lacp system-priority

Configure the LACP system priority.

Syntax **lacp system-priority** *priority-value*

To return to the default setting, use the **no lacp system-priority** *priority-value* command.

Parameters

priority-value	Enter the port-priority value. The higher the value number the lower the priority. Range: 1 to 65535 Default: 32768

Defaults 32768

Command Modes CONFIGURATION

Command History

Version 6.2.1.1	Introduced

port-channel mode

Configure the LACP port channel mode.

Syntax **port-channel** *number* **mode** [**active] [passive] [off**]

Parameters

number	Enter the port-channel number. C-Series Range: 1-128 E-Series Range: 1-32 for EtherScale, 1-255 for TeraScale
active	Enter the keyword **active** to set the mode to the active state.
passive	Enter the keyword **passive** to set the mode to the passive state.
off	Enter the keyword **off** to set the mode to the off state.

Defaults **off**

Command Modes INTERFACE

Command History

Version 6.2.1.1	Introduced

Usage Information The LACP modes are defined in Table 36.

Table 36 LACP Modes

Mode	Function
active	An interface is in an active negotiating state in this mode. LACP runs on any link configured in the active state and also automatically initiates negotiation with other ports by initiating LACP packets.
passive	An interface is not in an active negotiating state in this mode. LACP runs on any link configured in the passive state. Ports in a passive state respond to negotiation requests from other ports that are in active states. Ports in a passive state respond to LACP packets.
off	An interface can not be part of a dynamic port channel in the off mode. LACP will not run on a port configured in the off mode.

port-channel-protocol lacp

Enable LACP on any LAN port.

Syntax **port-channel-protocol lacp**

To disable LACP on a LAN port, use the **no port-channel-protocol lacp** command.

Command Modes INTERFACE

Command History

Version 6.2.1.1	Introduced

show lacp

Display the LACP matrix.

Syntax **show lacp** *port-channel-number* [**sys-id** | **counters**]

Parameters

port-channel-number	Enter the port-channel number to display the LACP matrix. C-Series Range: 1-128 E-Series Range: 1-32 for EtherScale, 1-255 for TeraScale
sys-id	(OPTIONAL) Enter the keyword **sys-id** and the value that identifies a system.
counters	(OPTIONAL) Enter the keyword **counters** to display the LACP counters.

Command Modes EXEC

EXEC privilege

Command History

Version 6.2.1.1	Introduced

Example 1

```
Force10#show lacp 1
Port-channel 1 admin up, oper up, mode lacp
Actor   System ID:  Priority 32768, Address 0001.e800.a12b
Partner System ID:  Priority 32768, Address 0001.e801.45a5
                    Actor Admin Key 1, Oper Key 1, Partner Oper Key 1
                    LACP LAG 1 is an aggregatable link

A - Active LACP, B - Passive LACP, C - Short Timeout, D - Long Timeout
E - Aggregatable Link, F - Individual Link, G - IN_SYNC, H - OUT_OF_SYNC
I - Collection enabled, J - Collection disabled, K - Distribution enabled L - Distribution disabled,
M - Partner Defaulted, N - Partner Non-defaulted, O - Receiver is in expired state,
P - Receiver is not in expired state

Port Gi 10/6 is enabled, LACP is enabled and mode is lacp
  Actor   Admin: State ACEHJLMP Key 1      Priority 128
           Oper: State ACEGIKNP Key 1      Priority 128
  Partner Admin: State BDFHJLMP Key 0      Priority 0
           Oper: State BCEGIKNP Key 1      Priority 128
Force10#
```

Figure 197 show lacp *port-channel-number* command

Example 2

```
Force10#show lacp 1 sys-id
Actor   System ID:  Priority 32768, Address 0001.e800.a12b
Partner System ID:  Priority 32768, Address 0001.e801.45a5

Force10#
```

Figure 198 show lacp sys-id command Example

Example 3

```
Force10#show lacp 1 counters
-------------------------------------------------------------------------
              LACP PDU            Marker PDU         Unknown  Illegal
Port     Xmit       Recv       Xmit       Recv       Pkts Rx  Pkts Rx
-------------------------------------------------------------------------
Gi 10/6  200        200        0          0          0        0
Force10#
```

Figure 199 show lacp counter command Example

Related Commands

clear lacp counters	Clear the LACP counters.

Chapter 20 SONET

C-Series	NO
E-Series	✓

Platform Specific Feature: Packet Over SONET/SDH is supported on E-Series only.

FTOS supports RFC 2558 “Definitions of Managed Objects for the SONET/SDH Interface” and RFC 2615 “PPP-over-SONET/SDH.”

This chapter contains the commands to configure Packet Over SONET/SDH (POS/SDH) interfaces and features, including PPP encapsulation.

- ais-shut on page 528
- alarm-report on page 528
- clock source on page 530
- debug ppp on page 530
- delay triggers on page 531
- down-when-looped on page 532
- encap on page 532
- flag on page 533
- framing on page 533
- interface sonet on page 534
- keepalive on page 534
- loopback on page 535
- ppp authentication on page 536
- ppp chap hostname on page 537
- ppp chap password on page 537
- ppp chap rem-hostname on page 538
- ppp chap rem-password on page 538
- ppp next-hop on page 539
- ppp pap hostname on page 540
- ppp pap password on page 540
- ppp pap rem-hostname on page 541
- ppp pap rem-password on page 541

- scramble-atm on page 542
- show controllers on page 543
- show interfaces on page 545
- speed on page 547

ais-shut

C-Series	No
E-Series	✓

Enable an alarm indication signal (AIS) when the SONET interface is shutdown.

Syntax **ais-shut**

To disable the AIS, enter **no ais-shut**.

Defaults Disabled.

Command Modes INTERFACE

alarm-report

C-Series	No
E-Series	✓

Specify which POS/SDH alarms to report to the remote SNMP server.

Syntax **alarm-report** {**b1-tca** | **b2-tca** | **b3-tca** | **lais** | **lrdi** | **pais** | **plop** | **prdi** | **sd-ber** | **sf-ber** | **slof** | **slos**}

To disable an alarm, use the **no alarm-report** {**b1-tca** | **b2-tca** | **b3-tca** | **lais** | **lrdi** | **pais** | **plop** | **prdi** | **sd-ber** | **sf-ber** | **slof** | **slos**} command.

Parameters

b1-tca	Enter the keyword **b1-tca** to report B1 bit-error rate (BER) threshold crossing alarm (TCA) errors.
b2-tca	Enter the keyword **b2-tca** to report B2 BER TCA errors.
b3-tca	Enter the keyword **b3-tca** to report B3 BER TCA errors.
lais	Enter the keyword **lais** to report line alarm indication signal.
lrdi	Enter the keyword **lrdi** to report line remote defect indicator.

pais	Enter the keyword **pais** to report path alarm indication signal.
plop	Enter the keyword **plop** to report path loss of pointer.
prdi	Enter the keyword **prdi** to report the path remote defect indication.
sd-ber	Enter the keyword **sd-ber** to report signal degradation BER errors.
sf-ber	Enter the keyword **sf-ber** to report signal failure BER errors.
slof	Enter the keyword **slof** to report section loss of frame.
slos	Enter the keyword **slos** to report section loss of signal.

Defaults

Disabled—no alarm reporting for all alarms

Command Modes

INTERFACE

Usage Information

Alarm reporting is available with this command. SNMP traps are available; however, syslogs are not generated. To view active alarms and defects, use the show controllers command. Table 37 defines the alarms that can be enabled by this command. The first three alarms (b1, b2, b3) do not generate reports. The remaining alarms, if enabled for reporting, will generate reports on a trap receiver.

Table 37 Alarm Definitions

Alarm	Description
b1-tca	**B1 BER threshold crossing alarm**
b2-tca	**B2 BER Threshold crossing alarm**
b3-tca	**B3 BER threshold crossing alarm**
lais	**Line Alarm Indication Signal**
lrdi	**Line Remote Defect Indication**
pais	**Path Alarm Indication Signal**
plop	**Path loss of Pointer**
prdi	**Path Remote Defect Indication**
sd-ber	**LBIP BER in excess of Signal Degradation threshold**
sf-ber	**LBIP BER in excess of Signal Failure threshold**
slof	**Section Loss of Frame**
slos	**Section Loss of Signal**

Related Commands

show controllers	Display alarms and defects

clock source

C-Series	No
E-Series	✓

Configure the clock source for each POS/SDH interface.

Syntax **clock source** {**internal** | **line**}

To return to the default setting, enter **no clock source**.

Parameters

internal	Enter the keyword **internal** to use the internal clock from the interface.
line	Enter the keyword **line** to use the recovered clock from the interface. This is the default.

Defaults **line**

Command Modes INTERFACE

debug ppp

C-Series	No
E-Series	✓

View traffic and information in a Point-to-Point Protocol (PPP) network.

Syntax **debug ppp** [**authentication** | **error** | **negotiation** | **packet**] **interface sonet** *slot*/*port*

To disable debugging, enter **no debug ppp**.

Parameters

authentication	(OPTIONAL) Enter the keyword **authentication** to view PPP authentication exchanges (Challenge Authentication Protocol (CHAP) packet exchanges and Password Authentication Protocol (PAP) exchanges) and traffic.
error	(OPTIONAL) Enter the keyword **error** to view PPP error statistics and protocol errors.
negotiation	(OPTIONAL) Enter the keyword **negotiation** to view PPP settings negotiated at startup.
packet	(OPTIONAL) Enter the keyword **packet** to view low-level packet dumps.
interface sonet *slot*/*port*	Enter the keywords **interface sonet** followed by the slot and port information.

Command Modes EXEC privilege

Usage Information If you enter debug ppp on page 530 without parameters, all parameters are enabled.

delay triggers

C-Series	No
E-Series	✓

Delay triggering the line or path alarms with a 100ms delay.

Syntax **delay triggers** {**line** [**lrdi** | **sd-ber** | **sf-ber**] | **path** [**pais** | **prdi**] }

To disable delay trigger (the default), enter **no delay triggers** {**line** [**lrdi** | **sd-ber** | **sf-ber**] | **path** [**pais** | **prdi**] } command.

line	Enter the keyword **line** to delay the specified line alarm.
lrdi	(OPTIONAL) Enter the keyword **lrdi** to specify line remote defect indicator.
sd-ber	(OPTIONAL) Enter the keyword **sd-ber** to specify signal degradation BER errors.
sf-ber	(OPTIONAL) Enter the keyword **sf-ber** to specify signal failure BER errors.
path	Enter the keyword **path** to delay the specified path alarm.
pais	(OPTIONAL) Enter the keyword **pais** to specify path alarm indication signal.
prdi	(OPTIONAL) Enter the keyword **prdi** to specify the path remote defect indication.

Defaults Disabled

Command Modes INTERFACE

Command History

Version 7.4.2.0	Added path option

Usage Information By default, certain alarms (LOS, LOF, LAIS, PLOP) bring the line protocol down immediately. Use this command, with the **line** option, to delay that trigger event by 100ms.

By default, path alarms (AIS, RDI, LOP) *do not* cause (or trigger) the interface line protocol to go down. This command, with the **path** option, can be used to trigger this action with a delay of 100ms.

down-when-looped

C-Series	No
E-Series	✓

Set the interface to send a system message when it detects a loopback condition and goes down.

Syntax **down-when-looped**

To disable notification, enter **no down-when-looped**.

Defaults Enabled

Command Modes INTERFACE

encap

C-Series	No
E-Series	✓

Configure encapsulation for a HDL/PPP interface.

Syntax **encap ppp**

To remove encapsulation, enter **no encap**.

Parameters

ppp	Enter the keyword **ppp** for Point-to-Point Protocol encapsulation.

Defaults Not configured.

Command Modes INTERFACE

Usage Information When you enter the **no encap** command, you administratively shutdown the interface and configuration information (such as IP address) is deleted from the interface. A SONET interface without encapsulation is always operationally down.

When you enable encapsulation on the interface, PPP negotiation begins after you enable the interface (no shutdown command). You can enable authentication and other related commands once negotiation is completed.

Note: Encapsulation must be configured before the interface is enabled for traffic.

flag

C-Series	No
E-Series	✓

Set the overhead bytes in the frame header to ensure interoperability between different vendor equipment.

Syntax **flag** {**c2** | **j0** } *value*

To return to the default value, use **no flag** {**c2** | **j0** } command.

Parameters

c2 *value*	Enter the keyword **c2** followed by value to set the path signal byte. Range: 0x00 to 0xFF hexadecimal (0-255 decimal) Default: 0xCF in hexidecimal (207 in decimal)
j0 *value*	Enter the keyword **j0** to set the section trace byte. Range: 0x00 to 0xFF hexadecimal (0-255 decimal) Default: 0xCF (207 in decimal)

Defaults as above

Command Modes INTERFACE

Usage Information You enter the flag C2 and J0 values in decimal, but the FTOS displays the values in hexidecimal in the **show controllers sonet** command output.

framing

C-Series	No
E-Series	✓

Set the type of framing used on a POS/SDH interface.

Syntax **framing** {**sdh** | **sonet**}

To return to the default, enter **no framing**.

Parameters

sdh	Enter the keyword **sdh** to specify Synchronous Digital Hierarchy (SDH) framing. Default: Sonet
sonet	Enter the keyword **sonet** to specify SONET framing. Default: Sonet

Defaults **sonet**

Command Modes INTERFACE

Usage Information Framing should be changed only when the interfaces are shutdown.

interface sonet

C-Series	No
E-Series	✓

Enter the INTERFACE mode to configure a POS/SDH interface.

Syntax **interface sonet** *slot/port*

Parameters

slot/port	Enter the slot/port information.

Defaults Not configured

Command Modes CONFIGURATION

Example

```
Force10(conf)#interface sonet 8/2
Force10(conf-if-so-8/2)#
```

Figure 200 interface sonet Command Example

Usage Information You cannot delete POS/SDH interfaces. By default, POS/SDH interfaces are disabled (shutdown on page 496). Use the encap on page 532 command to enable encapsulation on the interface.

Related Commands

encap	Configure PPP encapsulation.

keepalive

C-Series	No
E-Series	✓

Send keepalive packets periodically to keep an interface alive when it is not transmitting data.

Syntax **keepalive** [*seconds*]

To stop sending keepalive packets, enter **no keepalive**.

Parameters

seconds	(OPTIONAL) For POS/SDH interfaces with encapsulation enabled, enter the number of seconds between keepalive packets. Range: 0 to 32767 Default: 10 seconds

Defaults Enabled.

Command Modes INTERFACE

loopback

C-Series	**No**
E-Series	✓

Troubleshoot a POS/SDH interface by looping back traffic through the interface or the line.

Syntax **loopback** {**internal** | **line**}

To delete a loopback setting, use the **no loopback** {**internal** | **line**} command.

Parameters

internal	Enter the keyword **internal** to test the physical interface by sending incoming traffic back through the interface.
line	Enter the keyword **line** to test connectivity to the network by sending incoming traffic back to the network.

Defaults Not configured.

Command Modes INTERFACE

Usage Information Use the show config on page 483 command in the INTERFACE mode to determine if the loopback on page 535 command was configured.

Related Commands

show config	View the interface configuration.

ppp authentication

C-Series	No
E-Series	✓

Enable Challenge-Handshake Authentication Protocol (CHAP) and/or Password Authentication Protocol (PAP) authentication on the interface.

Syntax

ppp authentication {**chap** | **chap pap** | **pap** | **pap chap**}

To remove all PPP authentication, enter **no ppp authenticate**.

Parameters

chap	Enter the keyword **chap** to enable CHAP authentication only.
chap pap	Enter the keywords **chap pap** to enable CHAP on one side and PAP on the other.
pap	Enter the keyword **pap** to enable PAP authentication only.
pap chap	Enter the keywords **pap chap** to enable PAP on one side and CHAP on the other side.

Defaults

Not configured.

Command Modes

INTERFACE

Usage Information

Once you configure this command, the remote device must prove its identity before the FTOS sends traffic.

The two authentication types differ slightly:

- With CHAP authentication, the E-Series sends a challenge to the remote device, which must encrypt the response with a shared value and return it to the E-Series with a username. The E-Series checks the local database for a match on the shared value and username.
- With PAP authentication, the remote device must send a username/password set which the FTOS checks against the local database. PAP passwords are sent as “clear text” and could be intercepted and used.

After you enable PPP authentication, you must configure remote hostnames and passwords to initiate authentication on the E-Series.

Related Commands

ppp chap hostname	Configure a hostname for CHAP authentication.
ppp chap password	Configure a password for CHAP authentication.
ppp chap rem-hostname	Configure a remote hostname for CHAP authentication.
ppp chap rem-password	Configure a remote password for CHAP authentication.
ppp pap hostname	Configure a hostname for PAP authentication.
ppp pap password	Configure a password for PAP authentication.
ppp pap rem-hostname	Configure a remote hostname for PAP authentication.
ppp pap rem-password	Configure a remote password for PAP authentication.

ppp chap hostname

C-Series	No
E-Series	✓

Configure a hostname to be used in the CHAP authentication process

Syntax **ppp chap hostname** *name*

To remove the CHAP hostname, enter **no ppp chap hostname**.

Parameters

name	Enter a character string up to 32 characters long.

Defaults Not configured.

Command Modes INTERFACE

Usage Information For peers to successfully negotiate authentication on both sides of the link, you must configure a hostname, password, remote hostname and remote password for CHAP authentication.

Related Commands

ppp authentication	Enable CHAP or PAP or both authentication.
ppp chap password	Configure a password for CHAP authentication.
ppp chap rem-hostname	Configure a remote hostname for CHAP authentication.
ppp chap rem-password	Configure a remote password for CHAP authentication.

ppp chap password

C-Series	No
E-Series	✓

Configure a password to be used in the CHAP authentication process

Syntax **ppp chap password** *password*

To remove the CHAP password, enter **no ppp chap password**.

Parameters

password	Enter a character string up to 32 characters long.

Defaults Not configured.

Command Modes INTERFACE

Usage Information For peers to successfully negotiate authentication on both sides of the link, you must configure a hostname, password, remote hostname and remote password for CHAP authentication.

Related Commands

ppp authentication	Enable CHAP or PAP or both authentication.
ppp chap hostname	Configure a hostname for CHAP authentication.
ppp chap rem-hostname	Configure a remote hostname for CHAP authentication.
ppp chap rem-password	Configure a remote password for CHAP authentication.

ppp chap rem-hostname

C-Series	**No**
E-Series	✓

Configure a remote hostname to be used in the CHAP authentication process.

Syntax

ppp chap rem-hostname *name*

To remove the remote hostname, enter **no ppp chap rem-hostname**.

Parameters

name	Enter a character string up to 32 characters long.

Defaults

Not configured.

Command Modes

INTERFACE

Usage Information

For peers to successfully negotiate authentication on both sides of the link, you must configure a hostname, password, remote hostname and remote password for CHAP authentication.

Related Commands

ppp authentication	Enable CHAP or PAP or both authentication.
ppp chap rem-password	Configure a remote password for CHAP authentication.
ppp chap hostname	Configure a hostname for CHAP authentication.
ppp chap password	Configure a password for CHAP authentication.

ppp chap rem-password

C-Series	**No**
E-Series	✓

Configure a remote password for CHAP authentication.

Syntax **ppp chap rem-password** *password*

To remove a password, enter **no ppp chap rem-password**.

Parameters

password	Enter a character string up to 32 characters long.

Defaults Not configure.

Command Modes INTERFACE

Usage Information For peers to successfully negotiate authentication, you must configure a hostname, password, remote hostname and remote password for CHAP authentication.

Related Commands

ppp authentication	Enable CHAP or PAP or both authentication.
ppp chap rem-hostname	Configure a remote host name for CHAP authentication.
ppp chap hostname	Configure a hostname for CHAP authentication.
ppp chap password	Configure a password for CHAP authentication.

ppp next-hop

C-Series	No
E-Series	✓

Assign an IP address as the next hop for this interface.

Syntax **ppp next-hop** *ip-address*

To delete a next hop address, enter **no ppp next-hop**.

Parameters

ip-address	Enter an IP address in dotted decimal format (A.B.C.D).

Defaults Not configured.

Command Modes INTERFACE

Usage Information This IP address must match the peer's IP address or the link is not established. A peer will configure this IP address.

ppp pap hostname

C-Series	No
E-Series	✓

Configure a host name for PAP authentication.

Syntax

ppp pap hostname *name*

To delete a host name, enter **no ppp pap hostname**.

Parameters

name	Enter a character string up to 32 characters long.

Defaults

Not configured.

Command Modes

INTERFACE

Usage Information

For peers to successfully negotiate authentication, you must configure a hostname, password, remote hostname and remote password for PAP authentication.

Related Commands

ppp authentication	Enable CHAP or PAP or both authentication.
ppp pap password	Configure a password for PAP authentication.
ppp pap rem-hostname	Configure a remote hostname for PAP authentication.
ppp pap rem-password	Configure a remote password for PAP authentication.

ppp pap password

C-Series	No
E-Series	✓

Configure a password for PAP authentication.

Syntax

ppp pap password *password*

To delete a password, enter **no ppp pap password**.

Parameters

password	Enter a character string up to 32 characters long.

Defaults

Not configured.

Command Modes

INTERFACE

Usage Information

For peers to successfully negotiate authentication, you must configure a hostname, password, remote hostname and remote password for PAP authentication.

Related Commands

ppp authentication	Enable CHAP or PAP or both authentication.
ppp pap hostname	Configure a host name for PAP authentication.
ppp pap rem-hostname	Configure a remote hostname for PAP authentication.
ppp pap rem-password	Configure a remote password for PAP authentication.

ppp pap rem-hostname

C-Series	**No**
E-Series	✓

Configure a remote PAP hostname.

Syntax

ppp pap rem-hostname *hostname*

To delete a remote PAP host name, enter **no ppp pap rem-hostname**.

Parameters

hostname	Enter a character string up to 32 characters long.

Defaults

Not configured.

Command Modes

INTERFACE

Usage Information

For peers to successfully negotiate authentication, you must configure a hostname, password, remote hostname and remote password for PAP authentication.

Related Commands

ppp authentication	Enable CHAP or PAP or both authentication.
ppp pap rem-password	Configure remote password for PAP authentication.
ppp pap hostname	Configure a hostname for PAP authentication.
ppp pap password	Configure a password for PAP authentication.

ppp pap rem-password

C-Series	**No**
E-Series	✓

Configure a remote PAP password.

Syntax **ppp pap rem-password** *password*

To delete a remote PAP password, enter **no ppp pap rem-password**.

Parameters

password	Enter a character string up to 32 characters long.

Defaults Not configured.

Command Modes INTERFACE

Usage Information For peers to successfully negotiate authentication, you must configure a hostname, password, remote hostname and remote password for PAP authentication.

Related Commands

ppp authentication	Enable CHAP or PAP or both authentication.
ppp pap rem-hostname	Configure a remote hostname for PAP authentication.
ppp pap hostname	Configure a hostname for PAP authentication.
ppp pap password	Configure a password for PAP authentication.

scramble-atm

C-Series	No
E-Series	✓

Enable POS/SDH payload scrambling on the interface.

Syntax **scramble-atm**

To disable scrambling, enter **no scramble-atm**.

Defaults Disabled

Command Modes INTERFACE

Usage Information You must either enable payload scrambling or disable scambling on both ends of the link.

show controllers

C-Series	No
E-Series	✓

View troubleshooting information, such as the clock source, SONET alarms and error rates, and registers values.

Syntax **show controllers** *interface*

Parameters

interface	Enter the one of the following interface keywords and slot/port information: • For a SONET interface, enter the keyword **sonet** followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information.

Command Modes EXEC

EXEC privilege

Command History

Version 7.4.2.0	Added support for Ten Gigabit Ethernet

Example

```
Force10#show controllers sonet
Interface is SONET 1/2

SECTION
LOF = 0    LOS = 0                            BIP(B1)   = 0

LINE
AIS = 0    RDI = 0               FEBE = 0     BIP(B2) = 0

PATH
AIS = 0    RDI = 0    LOP = 0    FEBE = 0     BIP(B3) = 0

Active Defects: NONE
                    Enabled Alarms are listed here (default is none)
Active Alarms:  NONE

Alarm reporting enabled for:  SLOS SLOF B1-TCA LAIS LRDI B2-TCA PAIS PRDI PLOP B3-TCA SD SF

Framing is SDH, AIS-shut is enabled
Scramble-ATM is enabled, Down-when-looped is enabled
Loopback is disabled, Clock source is internal, Speed is Oc48
CRC is 32-bits, Flag C2 is 0x16, Flag J0 is 0xcc, Flag S1S0 is 0x2

Force10#
```

Figure 201 show controllers sonet Command Example

Example

```
Force10#show controllers te 4/1

Interface is TenGigabitEthernet 4/1

SECTION
LOF = 0    LOS = 0                              BIP(B1)  = 13

LINE
AIS = 0    RDI = 1               FEBE = 7633    BIP(B2) = 19264

PATH
AIS = 0    RDI = 0    LOP = 0    FEBE = 8554    BIP(B3) = 15685

Active Defects:  LRDI

Active Alarms:   LRDI

Alarm reporting enabled for:  SLOS SLOF B1-TCA LAIS LRDI B2-TCA PAIS PRDI PLOP B3-TCA SD SF

 Framing is SONET, AIS-shut is enabled
 Scramble-ATM is enabled, Down-when-looped is enabled
 Loopback is disabled, Clock source is line, Speed is Oc192
 CRC is 32-bits, Flag C2 is 0x1a, Flag J0 is 0xcc, Flag S1S0 is 0x0

Force10#
```

Figure 202 show controllers tengigabitethernet Command Example

Table 38 defines the information displayed in Figure 201 and Figure 202.

Table 38 Lines in show controllers *interface* Command Example

Line	Description
interface is ...	Displays the interface type and the slot and port number information.
SECTION LOF	Displays the section loss of frame (LOF) error. This error is detected when a severely error framing (SEF) defect on the incoming interface signal persist for 3 milliseconds
LOS	Displays the loss of signal (LOS) error. This error is detected when an all-zeros pattern on the incoming interface signal lasts 19 plus or minus 3 microseconds or longer. This defect might also be reported if the received signal level drops below the specified threshold.
BIP(B1)	Displays the bit interleaved parity error for the B1 byte. For B1, the report is calculated by comparing the BIP-8 code with the BIP-8 code extracted from the B1 byte of the following frame. Differences indicate section-level errors.
LINE AIS	Displays the alarm indication signal. This signal is sent by the section terminating equipment (STE) to alert the downstream line terminating equipment (LTE) that a LOS or LOF defect has been detected on the incoming interface section. Path alarm indication signal is sent by the LTE to alert the downstream path terminating equipment (PTE) that it has detected a defect on its incoming line signal.
RDI	Displays remote defect indication. This indication is reported by the downstream LTE when it detects LOF, LOS, or AIS conditions.

Table 38 Lines in show controllers *interface* Command Example (continued)

Line	Description
BIP(B2)	Displays the bit interleaved parity error for the B2 byte. For B2, the report is calculated by comparing the BIP-8/24 code with the BIP-8 code extracted from the B2 byte of the following frame.Differences indicate line-level errors.
PATH AIS	Displays the alarm indication signal. This signal is sent by the section terminating equipment (STE) to alert the downstream line terminating equipment (LTE) that a LOS or LOF defect has been detected on the incoming SONET section. Path alarm indication signal is sent by the LTE to alert the downstream path terminating equipment (PTE) that it has detected a defect on its incoming line signal.
RDI	Displays remote defect indication. This indication is reported by the downstream LTE when it detects LOF, LOS, or AIS conditions.
BIP(B3)	Displays the bit interleaved parity error for the B3 byte. For B3, the bit interleaved parity error report is calculated by comparing the BIP-8 code with the BIP-8 code extracted from the B3 byte of the following frame. Differences indicate path-level errors.
Active Defects:	Lists the current interface defects.
Active Alarms	List the current interface alarms as enforced the interface Alarm Hierarchy.
Alarm reporting enabled for:	List the Alarms enabled. The enabled alarms will generate a trap report. Note that the B1,2,3 threshold crossing alarms (tca) do not generate alarm reports.

show interfaces

C-Series	**No**
E-Series	✓

Display detailed information on the Sonet or 10-Gigabit Ethernet interfaces.

Syntax **show interfaces** *interface*

Parameters

interface	Enter the one of the following interface keywords and slot/port information: • For a SONET interface, enter the keyword **sonet** followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information.

Command Modes EXEC

EXEC privilege

Example

```
Force10>show interfaces sonet 2/0
SONET 2/0 is up, line protocol is up
Hardware is SONET, address is 00:01:e8:00:03:ff
Encapsulation PPP, Framing is SONET, AIS-shut is enabled
 Scramble-ATM is enabled, Down-when-looped is enabled
 Loopback is disabled, Clock source is internal, Speed is Oc48
 CRC is 32-bits, Flag C2 is 0x16, Flag J0 is 0xcc, Flag S1S0 is 0x0
 Keepalive Set (10 Sec)
 LCP  State: OPENED
 IPCP State: OPENED

Internet address is 6.1.5.2/30
MTU 1554 bytes, IP MTU 1500 bytes
LineSpeed 2488 Mbit
ARP type: ARPA, ARP timeout 04:00:00
Last clearing of "show interfaces" counters 17:08:10
Queueing strategy: fifo
     91425052815 packets input, 6188485730919 bytes
     Input 91425040617 IP Packets, 0 Vlans 0 MPLS
     Received 0 input symbol errors, 0 runts, 0 giants, 0 throttles
     0 CRC, 0 IP Checksum, 0 overrun, 0 discarded
     55176128354 packets output, 3677188351652 bytes, 474 underruns
     Output 173858 Multicasts, 0 Broadcasts, 55175954550 Unicasts
     55176116090 IP Packets, 0 Vlans, 0 MPLS
     0 throttles, 474 discarded
Rate info (interval 299 minutes):
     Input 1604.04Mbits/sec,    2583270 packets/sec
     Output 1169.30Mbits/sec,    1913510 packets/sec
Time since last interface status change: 17:10:40


Force10>
```

Figure 203 show interfaces sonet with PPP Encapsulation Command Example

Table 39 defines the information in Figure 203.

Table 39 Fields in the show interfaces sonet with PPP Encapsulation

Field	Description
Sonet 2/0...	Displays the interface's type, slot/port and physical and line protocol status.
Hardware is...	Displays the interface's hardware information and its assigned MAC address.
Encapsulation is ...	Displays the encapsulation method, the framing, and if the ais-shut command is enabled.
Scramble-ATM is enabled	States whether the scramble-atm and the down-when-looped commands are enabled.
Loopback is ...	States whether the loopback, clock source, and speed, and flag commands are configured. This information is displayed over 2 lines.
Keepalive Set	Displays the number of seconds between keepalive messages.
LCP State:	States if LCP was successfully negotiated.
IPCP State:	States if IPCP was successfully negotiated.
Internet address...	States whether an IP address is assigned to the interface. If one is, that address is displayed.

Table 39 Fields in the show interfaces sonet with PPP Encapsulation (continued)

Field	Description
Peer address	Displays the PPP peer's IP address.
MTU 1554...	Displays link and IP MTU.
LineSpeed	Displays interface's line speed.
ARP type:...	Displays the ARP type and the ARP timeout value for the interface.
Last clearing...	Displays the time when the **show interfaces** counters where cleared.
Queuing strategy..	States the packet queuing strategy. FIFO means first in first out.
0 packets...	Displays the number of packets and bytes into the interface.
Input 0 IP packets...	Displays the number of packets with IP headers, VLAN tagged headers and MPLS headers. The number of packets may not add correctly because a VLAN tagged IP packet counts as both a VLAN packet and an IP packet.
0 64-byte...	Displays the size of packets and the number of those packets entering that interface. This information is displayed over 2 lines. Any PPP packet less than 64 bytes in length will be padded out to 64 bytes upon reception. This padding will be counted by the ingress byte counter.
Received 0...	Displays the type and number of error or other specific packets received. This information is displayed over 3 lines.
Output 0...	Displays the type and number of packets sent out the interface. This information is displayed over 2 lines.
Time since...	Displays the time since the last change in the configuration of this interface.

Related Commands

show interfaces switchport	Displays Layer 2 information about the interfaces.
show ip interface	Displays Layer 3 information about the interfaces.

speed

C-Series	No
E-Series	✓

Set the speed of the SONET interface.

Syntax **speed** {**155** | **622** | **2488**}

To return to the default value, enter **no speed**.

Parameters

155	Enter **155** to set the interface as OC3
622	Enter **622** to set the interface as OC12
2488	Enter **2488** to set the interface as OC48

Defaults **622**

Command Modes INTERFACE

Command History

Version 7.4.1.0	Added support for 2488 (OC48)

Chapter 21 Layer 2 Protocol Tunneling

Platform Specific Feature: Layer 2 Protocol Tunneling is supported on E-Series only.

FTOS Layer 2 Protocol Tunneling (L2PT) enables protocols to tunnel through an 802.1q tunnel. The commands are:

- debug protocol-tunnel on page 550
- protocol-tunnel on page 551
- protocol-tunnel enable on page 551
- protocol-tunnel rate-limit on page 552
- show protocol-tunnel on page 553

Important Points to Remember

- L2PT is enabled at the interface VLAN-Stack VLAN level.
- Disable any protocol packet tunneling through 802.1q tunnel is the default behavior.
- Rate-limiting is required to protect against BPDU attacks.
- LACP/port channel is configured as VLAN-Stack access or SP-trunk port.
- ARP packets work as expected across the tunnel.
- FEFD works the same as with Layer 2 links.
- Protocols that use Multicast MAC addresses (OSPF for example) work as expected and carry over to the other end of the VLAN-Stack VLAN.

debug protocol-tunnel

C-Series	No
E-Series	✓

Enable debugging to ensure incoming packets are received and rewritten to a new MAC address.

Syntax

debug protocol-tunnel *interface* {**in** | **out** | **both**} [**vlan** *vlan-id*] [**count** *value*]

To disable debugging, use the **no debug protocol-tunnel** *interface* {**in** | **out** | **both**} [**vlan** *vlan-id*] [**count** *value*] command.

Parameters

interface	Enter one of the following interfaces and slot/port information: • For a Fast Ethernet interface, enter the keyword **FastEthernet** followed by the slot/port information. • For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For Port Channel interface types, enter the keyword **port-channel** followed by a number from 1 to 32 for EtherScale, 1 to 255 for TeraScale. • For a SONET interface, enter the keyword **sonet** followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information.
in | **out** | **both**	Enter the keyword **in**, **out**, or **both** to debug incoming, outgoing or interfaces in both incoming and outgoing.
vlan *vlan-id*	Enter the keyword **vlan** followed by the VLAN ID. Range: 1 to 4094
count *value*	Enter the keyword **count** followed by the number of debug outputs. Range: 1 to 100

Defaults

Debug Disabled

Command Modes

CONFIGURATION

Command History

Version 7.4.1.0	Introduced

protocol-tunnel

C-Series	No
E-Series	✓

Enable protocol tunneling per VLAN-Stack VLAN.

Syntax **protocol-tunnel** {**stp**}

To disable protocol tunneling, use the **no protocol-tunnel** {**stp**} command.

Parameters

stp	Enter the keyword **stp** to enable protocol tunneling on a spanning tree including STP, MSTP, RSTP and PVST.

Defaults No default values or behavior

Command Modes INTERFACE (conf-if-vl-2-stack)

Command History

Version 7.4.1.0	Introduced

Example

```
Force10#conf
Force10(conf)#interface vlan 2
Force10(conf-if-vl-2)#vlan-stack compatible
Force10(conf-if-vl-2)#member Gi1/2-3
Force10(conf-if-vl-2)#protocol-tunnel stp
Force10(conf-if-vl-2)#
```

Usage Information

Note: When VLAN-Stacking is enabled, no protocol packets are tunneled.

Related Commands

show protocol-tunnel	Display tunneling information for all VLANs

protocol-tunnel enable

C-Series	No
E-Series	✓

Enable protocol tunneling.

Syntax **protocol-tunnel enable**

To disable protocol tunneling, use the **no protocol-tunnel enable** command.

Defaults Disabled

Command Modes CONFIGURATION

Command History

Version 7.4.1.0	Introduced

protocol-tunnel rate-limit

C-Series	No
E-Series	✓

Enable traffic rate limiting per box.

Syntax **protocol-tunnel rate-limit** *rate*

To reset the rate limit to the default, use the **no protocol-tunnel rate-limit** *rate* command.

Parameters

rate	Enter the rate in frames per second. Range: 75 to 10000 Default: 75

Defaults 75 Frames per second

Command Modes CONFIGURATION

Command History

Version 7.4.1.0	Introduced

Example

```
Force10#
Force10#conf
Force10(conf)#protocol-tunnel rate-limit 1000
FForce10(conf)#
```

Related Commands

show protocol-tunnel	Display tunneling information for all VLANs
show running-config	Display the current configuration.

show protocol-tunnel

C-Series	No
E-Series	✓

Display the protocol tunnel information for all VLAN-Stack VLANs or a specified VLAN-Stack VLAN.

Syntax **show protocol-tunnel** [**vlan** *vlan-id*]

Parameters

vlan *vlan-id*	(OPTIONAL) Enter the keyword **vlan** followed by the VLAN ID to display information for the one VLAN. Range: 1 to 4094

Defaults No default values or behavior

Command Modes EXEC

Command History

Version 7.4.1.0	Introduced

Example

```
Force10#show protocol-tunnel
System Rate-Limit: 1000 Frames/second
Interface       Vlan    Protocol(s)
Gi1/2           2       STP, PVST
Gi1/3           3       STP, PVST
Po35            4       STP, PVST
Force10#
```

Figure 204 show protocol-tunnel command example

Example

```
Force10#show protocol-tunnel vlan 2
System Rate-Limit: 1000 Frames/second
Interface       Vlan    Protocol(s)
Gi1/2           2       STP, PVST
Force10#
```

Figure 205 show protocol-tunnel command example for a specific VLAN

Related Commands

show running-config	Display the current configuration.

Chapter 22 Layer 2

This chapter describes commands to configure Layer 2 features and contains the following sections.

- MAC Addressing on page 555
- Virtual LANs on page 569

MAC Addressing

The following commands are related to configuring, managing, and viewing MAC addresses:

- clear mac-address-table dynamic on page 556
- mac-address-table aging-time on page 556
- mac-address-table static on page 557
- mac-address-table station-move on page 558
- mac-address-table station-move refresh-arp on page 558
- mac accounting destination on page 559
- mac cam fib-partition on page 559
- mac learning-limit on page 560
- mac learning limit dynamic | no-station-move on page 561
- mac learning-limit learn-limit-violation on page 562
- mac learning-limit station-move-violation on page 562
- mac learning-limit reset on page 563
- show mac-address-table on page 564
- show mac-address-table aging-time on page 566
- show mac accounting destination on page 566
- show mac cam on page 567
- show mac learning-limit on page 568

clear mac-address-table dynamic

Clear the MAC address table of all MAC address learned dynamically.

Syntax **clear mac-address-table dynamic** {**address** *mac-address* | **all** | **interface** *interface* | **vlan** *vlan-id*}

Parameters

address *mac-address*	Enter the keyword **address** followed by a MAC address in nn:nn:nn:nn:nn:nn format.
all	Enter the keyword **all** to delete all MAC address entries in the MAC address table.
interface *interface*	Enter the following keywords and slot/port or number information: • For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For a Port Channel interface, enter the keyword **port-channel** followed by a number: C-Series Range: 1-128 E-Series Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale. • For a SONET interface, enter the keyword **sonet** followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information.
vlan *vlan-id*	Enter the keyword **vlan** followed by a VLAN ID number from 1 to 4094.

Command Modes EXEC privilege

mac-address-table aging-time

Specify an aging time for MAC addresses.

Syntax **mac-address-table aging-time** *seconds*

To delete an aging time or return to the default values, use the **no mac-address-table aging-time** [*seconds*] command.

Parameters

seconds	Enter either zero (0) or a number as the number of seconds before MAC addresses are relearned. To disable aging of the MAC address table, enter 0. Range: 10 and 1000000 Default: 1800 seconds

Defaults 1800 seconds

Command Modes CONFIGURATION

Related Commands		
	show mac-address-table aging-time	View MAC aging time.

mac-address-table static

Associate specific MAC or hardware addresses to an interface and VLANs.

Syntax **mac-address-table static** *mac-address* **output** *interface* **vlan** *vlan-id*

To remove a MAC address, use the **no mac-address-table static** *mac-address* **output** *interface* **vlan** *vlan-id* command.

Parameters

mac-address	Enter the 48-bit hexidecimal address in nn:nn:nn:nn:nn:nn format.
output *interface*	Enter the keyword **output** followed by one of the following interfaces: • For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For a Port Channel interface, enter the keyword **port-channel** followed by a number: C-Series Range: 1-128 E-Series Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale. • For a SONET interface, enter the keyword **sonet** followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information.
vlan *vlan-id*	Enter the keyword **vlan** followed by a VLAN ID. Range:1 to 4094.

Defaults Not configured.

Command Modes CONFIGURATION

Related Commands		
	show mac-address-table	Displays the MAC address table.

mac-address-table station-move

Change the frequency in which the MAC address station-move trap is sent after a MAC address changes in a VLAN. A trap is sent if station move is detected threshold number of times in a given interval.

Syntax **mac-address-table station-move threshold** *number* **interval** *count*

To return to the default setting, enter **no mac-address-table station-move**.

Parameters

threshold *number*	Enter the keyword threshold followed by the number of times MAC addresses in VLANs can change before an SNMP trap is sent. Range: 1 to 10
interval *seconds*	Enter the keyword interval followed by the number of seconds. Range: 5 to 60

Defaults Not configured.

Command Modes CONFIGURATION

Usage Information For information on the specific trap sent and the corresponding Syslog refer to Appendix B, SNMP Traps, on page 1397.

mac-address-table station-move refresh-arp

C-Series	No
E-Series	✓

Ensure that ARP refreshes the egress interface when a station move occurs due to a topology change.

Syntax **mac-address-table station-move refresh-arp**

To return to the default, use the **no mac-address-table station-move refresh-arp** command.

Defaults No default values or behavior

Command Modes CONFIGURATION

Command History

Version 7.4.1.0	Introduced

mac accounting destination

C-Series	No
E-Series	✓

Configure a destination counter for Layer 2 traffic.

Syntax

mac accounting destination {*mac-address* **vlan** *vlan-id* | **vlan}** [**bytes** | **packets**]

To delete a destination counter, enter **no mac accounting destination**.

Parameters

mac-address	Enter the MAC address in the nn:nn:nn:nn:nn:nn format to count Layer 2 packets or bytes sent to that MAC address.
vlan *vlan-id*	Enter the keyword **vlan** followed by the VLAN ID to count Layer 2 packets or bytes sent to the VLAN. Range: 1 to 4094.
bytes	(OPTIONAL) Enter the keyword **bytes** to count only bytes
packets	(OPTIONAL) Enter the keyword **packets** to count only packets.

Defaults

Not configured.

Command Modes

INTERFACE (available on physical interfaces only)

Usage Information

You must place the interface in Layer 2 mode (using the switchport command) prior to configuring the mac accounting destination command.

mac cam fib-partition

C-Series	No
E-Series	✓

Reapportion the amount of Content Addressable Memory (CAM) available for MAC address learning (FIB) versus the amount available for MAC ACLs on a line card.

Syntax

mac cam fib-partition {**25** | **50** | **75** | **100**} *slot-number*

To return to the default setting, enter **no mac cam fib-partition**.

Parameters

25	Enter the keyword **25** to set aside 25% of the CAM for MAC address learning.
50	Enter the keyword **50** to set aside 50% of the CAM for MAC address learning.

75	Enter the keyword **75** to set aside 75% of the CAM for MAC address learning.
100	Enter the keyword **100** to set aside 100% of the MAC CAM for MAC address learning. With this configuration, no MAC ACLs are processed.
slot-number	Enter the line card slot number. Range: 0 to 13 for the E1200 0 to 6 for the E600 0 to 5 for the E300

Defaults **75** (75% of the MAC CAM for MAC address learning)

Command Modes CONFIGURATION

Usage Information After setting the CAM partition size, the line card resets.

Related Commands

show mac cam	View current MAC CAM partition values.

mac learning-limit

C-Series	**No**
E-Series	✓

Limit the maximum number of MAC addresses (static and dynamic) learned on an interface.

Syntax **mac learning-limit** [*address limit*]

To delete the MAC address learning limit, use the **no mac learning-limit** *address limit* command.

Parameters

address limit	Enter the maximum number of MAC addresses learned. Range: 1 to 1000000

Defaults No limit.

Command Modes INTERFACE

Command History

Version 6.5.1.0	Added support for MAC Learning-Limit on LAG

Usage Information You must place the interface in Layer 2 mode (using the switchport command) prior to configuring the mac learning-limit command.

Once the MAC address learning limit is reached, the MAC addresses do not age out. To clear statistics on MAC address learning, use the clear counters with the learning-limit parameter.

Note: If you configure this command on an interface in a routed VLAN, and once the MAC addresses learned reaches the limit set in the mac learning-limit command, IP protocols are affected. For example, VRRP sets multiple VRRP Masters and OSPF may not come up.

When a channel member is added to a port-channel and there is not enough ACL CAM space, then the MAC limit functionality on that port-channel is undefined. When this occurs, unconfigure the existing configuration first and then reapply the limit with a lower value.

Related Commands

clear counters	Clear counters used in the show interface command
switchport	Place the interface in Layer 2 mode
show mac learning-limit	Display details of the mac learning-limit

mac learning limit dynamic | no-station-move

C-Series	**No**
E-Series	✓

Allow aging of MACs even though learning-limit is configured or disallow station move on learnt MACs.

Syntax **mac learning limit** {*address limit*} [**dynamic** | **no-station-move**]

To return to the default, use the **no mac learning limit** {*address limit*} [**dynamic** | **no-station-move**] command.

Parameters

address limit	Enter the maximum number of MAC addresses learned. Range: 1 to 1000000
dynamic	(OPTIONAL) Enter the key **dynamic** to allow aging of MACs even though learning-limit is configured
no-station-move	(OPTIONAL) Enter the keyword **no-station-move** to disallow station-move on learnt MACs

Defaults No default behavior or values

Command Modes INTERFACE (conf-if-*interface-slot/port*)

Command History

Version 7.5.1.0	Introduced

Usage Information

This is supported on physical interfaces, static LAGs, and LACP LAGs.

Related Commands

show mac learning-limit	Display details of the mac learning-limit

mac learning-limit learn-limit-violation

C-Series	No
E-Series	✓

Configure an action for a learn limit violation.

Syntax

mac learning-limit learn-limit-violation {**log** | **shutdown**}

To return to the default, use the **no mac learning-limit learn-limit-violation** {**log** | **shutdown**} command.

Parameters

log	(OPTIONAL) Enter the keyword **log** to generate a Syslog on learn-limit violation.
shutdown	OPTIONAL) Enter the keyword **shutdown** to shutdown the port on learn-limit violation.

Defaults

No default behavior or values

Command Modes

INTERFACE (conf-if-*interface-slot/port*)

Command History

Version 7.5.1.0	Introduced

Usage Information

This is supported on physical interfaces, static LAGs, and LACP LAGs.

Related Commands

show mac learning-limit	Display details of the mac learning-limit

mac learning-limit station-move-violation

C-Series	No
E-Series	✓

Specify the actions for a station move violation.

Syntax **mac learning-limit station-move-violation** {**log** | **shutdown-both** | **shutdown-offending** | **shutdown-original**}

To disable, use the **no mac learning-limit station-move-violation** {**log** | **shutdown-both** | **shutdown-offending** | **shutdown-original**} command.

Parameters

log	(OPTIONAL) Enter the keyword **log** to generate a Syslog on station move violation.
shutdown-both	OPTIONAL) Enter the keyword **shutdown** to shutdown both the original and offending interface and generate a Syslog.
shutdown-offending	(OPTIONAL) Enter the keyword **shutdown-offending** to shutdown the offending interface and generate a Syslog.
shutdown-original	(OPTIONAL) Enter the keyword **shutdown-original** to shutdown the original interface and generate a Syslog.

Defaults No default behavior or values

Command Modes INTERFACE (conf-if-*interface-slot/port*)

Command History

Version 7.5.1.0	Introduced

Usage Information This is supported on physical interfaces, static LAGs, and LACP LAGs.

Related Commands

show mac learning-limit	Display details of the mac learning-limit

mac learning-limit reset

C-Series	No
E-Series	✓

Reset Mac Learning-Limit Error Disabled state.

Syntax **mac learning-limit reset**

Defaults No default behavior or values

Command Modes EXEC

EXEC privilege

Command History

Version 7.5.1.0	Introduced

show mac-address-table

View the MAC address table.

Syntax **show mac-address-table** [**dynamic** | **static**] [**address** *mac-address* | **interface** *interface* | **vlan** *vlan-id*] [**count**]

Parameters

dynamic	(OPTIONAL) Enter the keyword **dynamic** to view only those MAC addresses learned dynamically by the E-Series.
static	(OPTIONAL) Enter the keyword **static** to view only those MAC address specifically configured on the E-Series.
address *mac-address*	(OPTIONAL) Enter the keyword **address** followed by a MAC address in the nn:nn:nn:nn:nn:nn format to view information on that MAC address.
interface *interface*	(OPTIONAL) Enter the keyword **interface** followed by the interface type, slot and port information: • For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For a Port Channel interface, enter the keyword **port-channel** followed by a number: C-Series Range: 1-128 E-Series Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale. • For a SONET interface, enter the keyword **sonet** followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information.
vlan *vlan-id*	(OPTIONAL) Enter the keyword **vlan** followed by the VLAN ID to view the MAC address assigned to the VLAN. Range: 1 to 4094.
count	(OPTIONAL) Enter the keyword **count** to view the Static address, dynamic address count and the total MAC addresses in use.

Command Modes EXEC

EXEC privilege

Example

```
Force10#show mac-address-table

VlanId     Mac Address           Type   Interface        State
 999    00:00:00:00:00:19       Dynamic Gi 0/1          Active
 999    00:00:00:00:00:29       Dynamic Gi 0/2          Active

Force10#
```

Figure 206 show mac-address-table

Table 40 defines the column headings in Figure 206

Table 40 show mac-address-table Information

Column Heading	Description
VlanId	Displays the VLAN ID number.
Mac Address	Displays the MAC address in nn:nn:nn:nn:nn:nn format.
Type	Lists whether the MAC address was manually configured (Static) or learned (Dynamic).
Interface	Displays the interface type and slot/port information. The following abbreviations describe the interface types: • gi—Gigabit Ethernet followed by a slot/port. • po—Port Channel followed by a number. Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale • so—Sonet followed by a slot/port. • te—10-Gigabit Ethernet followed by a slot/port.
State	Lists if the MAC address is in use (Active) or not in use (Inactive).

```
Force10#show mac-address-table count
MAC Entries for all vlans :
Dynamic Address Count :                 5
Static Address (User-defined) Count :   0
Total MAC Addresses in Use:             5
Force10#
```

Figure 207 show mac-address-table count

Table 41 defines the information displayed in Figure 207.

Table 41 show mac-address-table count Information

Line Beginning with	Description
MAC Entries...	Displays the number of MAC entries learnt per VLAN.
Dynamic Address ...	Lists the number of dynamically learned MAC addresses.
Static Address ...	Lists the number of user-defined MAC addresses.
Total MAC...	Lists the total number of MAC addresses used by the E-Series.

Related Commands		
	show mac-address-table aging-time	View MAC aging time.

show mac-address-table aging-time

View the aging times assigned to the E-Series MAC addresses.

Syntax **show mac-address-table aging-time**

Command Modes EXEC

EXEC privilege

Example

```
Force10#show mac-address-table aging-time
 Mac-address-table aging time : 1800

Force10#
```

Figure 208 show mac-address-table aging-time

Related Commands		
	show mac-address-table	View the current MAC address configuration.

show mac accounting destination

C-Series	**No**
E-Series	✓

View destination counters for Layer 2 traffic (available on physical interfaces only).

Syntax **show mac accounting destination** [*mac-address* **vlan** *vlan-id*] [**interface** *interface* [*mac-address* **vlan** *vlan-id*] [**vlan** *vlan-id*]] [**vlan** *vlan-id*]

Parameters

mac-address	(OPTIONAL) Enter the MAC address in the nn:nn:nn:nn:nn:nn format to view information on that MAC address.
interface *interface*	(OPTIONAL) Enter the keyword **interface** followed by the interface type, slot and port information: • For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information.
vlan *vlan-id*	(OPTIONAL) Enter the keyword **vlan** followed by the VLAN ID to view the MAC address assigned to that VLAN. Range: 1 to 4094.

Command Modes EXEC

EXEC privilege

Usage Information MAC Accounting information can be accessed using SNMP via the Force10 Monitor MIB. For more information on enabling SNMP, refer to Chapter 3 of the *FTOS Configuration Guide*.

Note: Currently, the Force10 Monitor MIB does not return the MAC Addresses in an increasing order via SNMP. As a workaround, you can use the the **-C c** option in **snmpwalk** or **snmpbulkwalk** to access the Force10 Monitor MIB. For example:

```
% snmpwalk -C c -v 2c -c public 133.33.33.131 enterprise.6027.3.3.3
```

Example

```
Force10-1#sh mac accounting destination interface gigabitethernet 2/1

Destination         Out  Port   VLAN    Packets      Bytes

00:44:00:00:00:02   Te   11/0   1000    10000        5120000
00:44:00:00:00:01   Te   11/0   1000    10000        5120000
00:22:00:00:00:00   Te   11/0   1000    10000        5120000
00:44:00:00:00:02   Te   11/0   2000    10000        5120000
00:44:00:00:00:01   Te    11/0   2000    10000        5120000

Force10-1#
```

Figure 209 show mac accounting destination

show mac cam

View the CAM size and the portions allocated for MAC addresses and for MAC ACLs.

Syntax **show mac cam**

Command Modes EXEC

EXEC privilege

Example

```
Force10#show mac cam
Slot  Type     MAC CAM Size   MAC FIB Entries   MAC ACL Entries
  0   E24PD     64K entries       48K (75%)          8K (25%)
  2   E24PD2   128K entries       64K (50%)         32K (50%)
 11   EX2YD     64K entries       16K (25%)         24K (75%)
Note: All CAM entries are per portpipe.
Force10#
```

Figure 210 show mac cam

Table 42 defines the information displayed in Figure 210.

Table 42 show mac cam Information

Field	Description
Slot	Lists the active line card slots.
Type	Lists the type of line card present in the slot.
MAC CAM Size	Displays the total CAM size available. **Note**: A portion of the MAC CAM is used for system operations, therefore adding the MAC FIB and MAC ACL will be less than the MAC CAM.
MAC FIB Entries	Displays the amount and percentage of CAM available for MAC addresses.
MAC ACL Entries	Displays the amount and percentage of CAM available for MAC ACLs.

show mac learning-limit

C-Series	**No**
E-Series	✓

View MAC address learning limits set for various interfaces.

Syntax **show mac learning-limit** [**violate-action**] [**detail**] [**interface** *interface*]

Parameters

violate-action	(OPTIONALY) Enter the keyword **violate-action** to display the MAC learning limit violation status.

detail	(OPTIONALY) Enter the keyword **detail** to display the MAC learning limit in detail.
interface *interface*	(OPTIONALY) Enter the keyword **interface** with the following keywords and slot/port or number information: • For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For SONET interfaces, enter the keyword **sonet** followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information. • For Port Channel interface types, enter the keyword **port-channel** followed by a number between 1 and 255.

Command Modes

EXEC
EXEC privilege

Command History

Version 7.5.1.0	Added support for **violate-action** and **detail** options
Version 6.5.1.0	Added support for Port Channel

Example

```
Force10#show mac learning-limit
Interface      Learning       Dynamic        Static              Unknown SA
Slot/port      Limit          MAC count      MAC count           Drops
Gi 0/3         10             9              1                   1449
Po 1           20             20             0                   28970
Force10#
```

Figure 211 show mac learning-limit

Virtual LANs

The following commands configure and monitor Virtual LANs (VLANs). VLANs are a virtual interface and use many of the same commands as physical interfaces.

You can configure an IP address and Layer 3 protocols on a VLAN called Inter-VLAN routing. FTP, TFTP, ACLs and SNMP are not supported on a VLAN.

Occasionally, while sending broadcast traffic over multiple Layer 3 VLANs, the VRRP state of a VLAN interface may continually switch between Master and Backup.

- default vlan-id on page 570
- name on page 570
- show vlan on page 571
- tagged on page 572
- track ip on page 573
- untagged on page 574

default vlan-id

Specify a VLAN as the Default VLAN.

Syntax **default vlan-id** *vlan-id*

To remove the default VLAN status from a VLAN and VLAN 1 does not exist, use the **no default vlan-id** *vlan-id* syntax.

Parameters

vlan-id	Enter the VLAN ID number of the VLAN to become the new Default VLAN. Range: 1 to 4094. Default: 1

Defaults The Default VLAN is VLAN 1.

Command Modes CONFIGURATION

Usage Information To return VLAN 1 as the Default VLAN, use this command syntax (**default-vlan-id 1**).

The Default VLAN contains only untagged interfaces.

name

Assign a name to the VLAN.

Syntax **name** *vlan-name*

To remove the name from the VLAN, enter no name.

Parameters

vlan-name	Enter up to 32 characters as the name of the VLAN.

Defaults Not configured.

Command Modes INTERFACE VLAN

Usage Information To view information about a named VLAN, enter the show vlan command with the name parameter or the show interfaces description command.

show vlan

View the current VLAN configurations on the E-Series.

Syntax **show vlan** [**brief** | **id** *vlan-id* | **name** *vlan-name*]

Parameters

brief	(OPTIONAL) Enter the keyword **brief** to view the following information: • VLAN ID • VLAN name (left blank if none is configured.) • Spanning Tree Group ID • MAC address aging time • IP address
id *vlan-id*	(OPTIONAL) Enter the keyword **id** followed by a number from 1 to 4094. Only information on the VLAN specified is displayed.
name *vlan-name*	(OPTIONAL) Enter the keyword **name** followed by the name configured for the VLAN. Only information on the VLAN named is displayed.

Command Modes EXEC

EXEC privilege

Example

```
Force10#show vlan

Codes: * - Default VLAN, G - GVRP VLANs

    NUM    Status    Q Ports
*   1      Inactive
    2      Active    U Po1(Gi 13/0)
                     T Po20(Gi 13/6)
                     T Gi 13/7
    3      Active    T Po20(Gi 13/6)
                     T Gi 13/7
                     U Gi 13/1
    4      Active    U Po2(Gi 13/2)
                     T Po20(Gi 13/6)
                     T Gi 13/7
    5      Active    T Po20(Gi 13/6)
                     T Gi 13/7
                     U Gi 13/3
    6      Active    U Po3(Gi 13/4)
                     T Po20(Gi 13/6)
                     T Gi 13/7
    7      Active    T Po20(Gi 13/6)
                     T Gi 13/7
                     U Gi 13/5
Force10#
```

Figure 212 show vlan

Table 43 describes the information in Figure 212.

Table 43 show vlan Information

Column Heading	Description
(no heading)	Displays symbols for the Default VLAN.
NUM	Displays the VLAN ID.

Table 43 show vlan Information

Column Heading	Description
Status	Displays the word `Inactive` for inactive VLANs and the word `Active` for active VLANs.
Q	Displays T (for tagged interface) or U (for untagged interface) or M (for Member of a VLAN-Stack VLAN).
Ports	Displays the type, slot and port information.

```
Force10#show vlan br
VLAN Name                              STG   MAC Aging IP Address
---- --------------------------------- ----  --------- ------------------
1                                      0     1800      unassigned
2                                      0     1800      2.2.2.2/24
3                                      0     1800      3.3.3.2/24
Force10#
```

Figure 213 show vlan brief

tagged

Add a Layer 2 interface to a VLAN as a tagged interface.

Syntax **tagged** *interface*

To remove a tagged interface from a VLAN, use **no tagged** *interface* command.

Parameters

interface	Enter the following keywords and slot/port or number information: • For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For a Port Channel interface, enter the keyword **port-channel** followed by a number: C-Series Range: 1-128 E-Series Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information.

Defaults All interfaces in Layer 2 mode are untagged.

Command Modes INTERFACE VLAN

Usage Information When you use the **no tagged** command, the interface is automatically placed in the Default VLAN as an untagged interface unless the interface is a member of another VLAN. If the interface belongs to several VLANs, you must remove it from all VLANs to change it to an untagged interface.

Tagged interfaces can belong to multiple VLANs, while untagged interfaces can only belong to one VLAN at a time.

Related Commands

untagged	Specify interfaces in a VLAN as untagged.

track ip

Track the Layer 3 operational state of a Layer 3 VLAN, using a subset of the VLAN member interfaces.

Syntax **track ip** *interface*

To remove the tracking feature from the VLAN, use the **no track ip** *interface* command.

Parameters

interface	Enter the following keywords and slot/port or number information: • For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For a Port Channel interface, enter the keyword **port-channel** followed by a number: C-Series Range: 1-128 E-Series Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale. • For a SONET interface, enter the keyword **sonet** followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information.

Defaults Not configured

Command Modes INTERFACE VLAN

Usage Information When this command is configured, the VLAN is operationally UP if any of the interfaces specified in the **track ip** command are operationally UP, and the VLAN is operationally DOWN if none of the tracking interfaces are operationally UP.

If the **track ip** command is not configured, the VLAN's Layer 3 operational state depends on all the members of the VLAN.

The Layer 2 state of the VLAN, and hence the Layer 2 traffic is not affected by the **track ip** command configuration.

untagged

Add a Layer 2 interface to a VLAN as an untagged interface.

Syntax **untagged** *interface*

To remove an untagged interface from a VLAN, use the **no untagged** *interface* command.

Parameters

interface	Enter the following keywords and slot/port or number information: • For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For Port Channel interface types, enter the keyword **port-channel** followed by a number from 1 to 32 for EtherScale, 1 to 255 for TeraScale. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information.

Defaults All interfaces in Layer 2 mode are untagged.

Command Modes INTERFACE VLAN

Usage Information Untagged interfaces can only belong to one VLAN.

In the Default VLAN, you cannot use the **no untagged** *interface* command. To remove an untagged interface from all VLANs, including the Default VLAN, enter the INTERFACE mode and use the no switchport command.

Related Commands

tagged	Specify which interfaces in a VLAN are tagged.

Chapter 23 Resilient Ring Protocol

Platform Specific Feature: Resilient Ring Protocol is supported on E-Series only.

Force10's Resilient Ring Protocol (FRRP) is a proprietary protocol that offers fast convergence in a Layer 2 network without having to run the Spanning Tree Protocol. The Resilient Ring Protocol is an efficient protocol that transmits a high-speed token across a ring to verify the link status. All the intelligence is contained in the master node with practically no intelligence required of the transit mode. The FRRP commands are:

- clear frrp on page 576
- debug frrp on page 577
- description on page 577
- disable on page 578
- interface on page 578
- member-vlan on page 580
- mode on page 580
- protocol frrp on page 581
- show frrp on page 581
- timer on page 583

Important Points to Remember

- FRRP is media and speed independent.
- FRRP is a Force10 proprietary protocol that does not interoperate with any other vendor.
- Spanning Tree must be disabled on both primary and secondary interfaces before Resilient Ring protocol is enabled.
- A VLAN configured as control VLAN for a ring cannot be configured as control or member VLAN for any other ring.
- If multiple rings share one or more member VLANs, they cannot share any links between them.
- Each ring can have only one Master node; all others are Transit nodes.

clear frrp

C-Series	No
E-Series	✓

Clear the FRRP statistics counters.

Syntax **clear frrp** [*ring-id*]

Parameters

ring-id	(Optional) Enter the ring identification number. Range: 1 to 255

Defaults No default values or behavior

Command Modes EXEC

Command History

Version 7.5.1.0	Introduced

Example

```
Force10#clear frrp                                  clears the frrp counters for all the available rings

Clear frrp statistics counter on all ring [confirm] yes   confirmation required


Force10#clear frrp 4                                clears the frrp counters on the specfied ring

Clear frrp statistics counter for ring 4 [confirm] yes    confirmation required
Force10#
```

Figure 214 clear frrp command examples

Usage Information Executing this command, without the optional *ring-id,* will clear statistics counters on all the available rings. FTOS requires a command line confirmation before the command is executed. This commands clears the following counters:

- hello Rx
- Tx counters
- Topology change Rx
- Tx counters
- The number of state change counters

Related Commands

show frrp	Display the Resilient Ring Protocol configuration

debug frrp

C-Series	No
E-Series	✓

Enable FRRP debugging.

Syntax **debug frrp** {**event** | **packet** | **detail**} [*ring-id*] [**count** *number*]

To disable debugging, use the **no debug frrp** {**event** | **packet** | **detail**} {*ring-id*} [**count** *number*] command.

Parameters

event	Enter the keyword **event** to display debug information related to ring protocol transitions.
packet	Enter the keyword **packet** to display brief debug information related to control packets.
detail	Enter the keyword **detail** to display detailed debug information related to the entire ring protocol packets.
ring-id	(Optional) Enter the ring identification number. Range: 1 to 255
count *number*	Enter the keyword **count** followed by the number of debug outputs. Range: 1 to 65534

Defaults Disabled

Command Modes CONFIGURATION (conf-frrp)

Command History

Version 7.4.1.0	Introduced

Usage Information

Note: Since the Resilient Ring Protocol can potentially transmit 20 packets per interface, debug information must be restricted.

description

C-Series	No
E-Series	✓

Enter an identifying description of the ring.

Syntax **description** *Word*

To remove the ring description, use the **no description** [*Word*]command.

Parameters		
	Word	Enter a description of the ring. Maximum: 255 characters

Defaults No default values or behavior

Command Modes CONFIGURATION (conf-frrp)

Command History		
	Version 7.4.1.0	Introduced

disable

C-Series	**No**
E-Series	✓

Disable the Resilient Ring Protocol.

Syntax **disable**

To enable the Resilient Ring Protocol, use the **no disable** command.

Defaults Disabled

Command Modes CONFIGURATION (conf-frrp)

Command History		
	Version 7.4.1.0	Introduced

interface

C-Series	**No**
E-Series	✓

Configure the primary, secondary, and control-vlan interfaces.

Syntax **interface** {**primary** *interface* **secondary** *interface* **control-vlan** *vlan-id*}

To return to the default, use the **no interface** {**primary** *interface* **secondary** *interface* **control-vlan** *vlan-id*} command.

Parameters

primary *interface*	Enter the keyword **primary** to configure the primary interface followed by one of the following interfaces and slot/port information: • For a Fast Ethernet interface, enter the keyword **FastEthernet** followed by the slot/port information. • For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For Port Channel interface types, enter the keyword **port-channel** followed by a number from 1 to 255. • For a SONET interface, enter the keyword **sonet** followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information.
secondary *interface*	Enter the keyword **secondary** to configure the secondary interface followed by one of the following interfaces and slot/port information: • For a Fast Ethernet interface, enter the keyword **FastEthernet** followed by the slot/port information. • For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For Port Channel interface types, enter the keyword **port-channel** followed by a number from 1 to 255. • For a SONET interface, enter the keyword **sonet** followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information.
control-vlan *vlan-id*	Enter the keyword **control-vlan** followed by the VLAN ID. Range: 1 to 4094

Defaults

No default values or behavior

Command Modes

CONFIGURATION (conf-frrp)

Command History

Version 7.4.1.0	Introduced

Usage Information

This command causes the Ring Manager to take ownership of these two ports after the configuration is validated by the IFM. Ownership is relinquished for a port only when the interface does not play a part in any control VLAN, that is the interface does not belong to any ring.

Related Commands

show frrp	Display the Resilient Ring Protocol configuration information

member-vlan

C-Series	No
E-Series	✓

Specify the member VLAN identification numbers.

Syntax **member-vlan** {*vlan-range*}

To return to the default, use the **no member-vlan** [*vlan-range*] command.

Parameters

vlan-range	Enter the member VLANs using comma separated VLAN IDs, a range of VLAN IDs, a single VLAN ID, or a combination. For example: Comma separated: 3, 4, 6 Range: 5-10 Combination: 3, 4, 5-10, 8

Defaults No default values or behavior

Command Modes CONFIGURATION (conf-frrp)

Command History

Version 7.4.1.0	Introduced

mode

C-Series	No
E-Series	✓

Set the Master or Transit mode of the ring.

Syntax **mode** {**master** | **transit**}

To reset the mode, use the **no mode** {**master** | **transit**} command.

Parameters

master	Enter the keyword **master** to set the Ring node to Master mode.
transit	Enter the keyword **transit** to set the Ring node to Transit mode.

Defaults Mode None

Command Modes CONFIGURATION (conf-frrp)

Command History

Version 7.4.1.0	Introduced

protocol frrp

C-Series	No
E-Series	✓

Enter the Resilient Ring Protocol and designate a ring identification.

Syntax **protocol frrp** {*ring-id*}

To exit the ring protocol, use the **no protocol frrp** {*ring-id*} command.

Parameters

ring-id	Enter the ring identification number. Range: 1 to 255

Defaults No default values or behavior

Command Modes CONFIGURATION

Command History

Version 7.4.1.0	Introduced

Usage Information This command places you into the Resilient Ring Protocol. After executing this command, the command line prompt changes to conf-frrp.

show frrp

C-Series	No
E-Series	✓

Display the Resilient Ring Protocol configuration.

Syntax **show frrp** [*ring-id* [**summary**]] | [**summary**]

Parameters

ring-id	Enter the ring identification number. Range: 1 to 255
summary	(OPTIONAL) Enter the keyword **summary** to view just a summarized version of the Ring configuration.

Defaults No default values or behavior

Command Modes EXEC

Command History

Version 7.4.1.0	Introduced

Example 1

```
Force10#show frrp summary

Ring-ID     State      Mode        Ctrl_Vlan     Member_Vlans
-------------------------------------------------------------------
2           UP         Master      2             11-20, 25,27-30
31          UP         Transit     31            40-41
50          Down       Transit     50            32
Force10#
```

Figure 215 show frrp summary command

Example 2

```
Force10#show frrp 1
Ring protocol 1 is in Master mode
Ring Protocol Interface:
Primary : GigabitEthernet 0/16 State: Forwarding
Secondary: Port-channel 100 State: Blocking
Control Vlan: 1
Ring protocol Timers: Hello-Interval 50 msec Dead-Interval 150 msec
Ring Master's MAC Address is 00:01:e8:13:a3:19
Topology Change Statistics: Tx:110 Rx:45
Hello Statistics: Tx:13028 Rx:12348
Number of state Changes: 34
Member Vlans: 1000-1009

Force10#
```

Figure 216 show frrp *ring-id* command

Example 3

```
Force10#show frrp 2 summary

Ring-ID    State       Mode     Ctrl_Vlan     Member_Vlans
-------------------------------------------------------------------
2          Up          Master    2             11-20, 25, 27-30
Force10#
```

Figure 217 show frrp *ring-id* summary command

Related Commands

protocol frrp	Enter the Resilient Ring Protocol and designate a ring identification

timer

C-Series	No
E-Series	✓

Set the hello or dead interval for the Ring control packets.

Syntax

timer {**hello-interval** *milliseconds*}| {**dead-interval** *milliseconds*}

To remove the timer, use the **no timer** {**hello-interval** [*milliseconds*]}| {**dead-interval** *milliseconds*} command.

Parameters

hello-interval *milliseconds*	Enter the keyword **hello-interval** followed by the time, in milliseconds, to set the hello interval of the control packets. The milliseconds must be enter in increments of 50 milliseconds, for example 50, 100, 150 and so on. If an invalid value is enter, an error message is generated. Range: 50 to 2000ms Default: 500 ms
dead-interval *milliseconds*	Enter the keyword **dead-interval** followed by the time, in milliseconds, to set the dead interval of the control packets. Range: 50 to 6000ms Default: 1500ms

Defaults

Default as shown

Command Modes

CONFIGURATION (conf-frrp)

Command History

Version 7.4.1.0	Introduced

Usage Information

The Hello Interval is the interval at which ring frames are generated from the Primary Interface of the Master Node. The Dead Interval is the time that elapses before a time out occurs.

Chapter 24 FVRP

Platform Specific Feature: FVRP is supported on E-Series only.

Force10 VLAN Redundancy Protocol (FVRP) is a proprietary protocol that provides rapid failover in Layer 2 networks by taking advantage of bandwidth available in redundant links. When FVRP is configured, one link carries traffic to the core switch for that VLAN and all other links are in standby mode.

- disable on page 586
- fvrp access on page 586
- fvrp aware on page 587
- fvrp control-vlan on page 588
- fvrp core on page 588
- fvrp core region on page 589
- fvrp disable on page 589
- fvrp domain on page 590
- fvrp group on page 591
- fvrp hello-time on page 591
- fvrp preempt on page 592
- fvrp priority (for a VLAN) on page 592
- fvrp priority (for an interface) on page 593
- fvrp uplink on page 594
- protocol fvrp on page 594
- show config on page 595
- show fvrp on page 595

Important Points to Remember

- FVRP is not supported on Default VLAN.
- Core, access, and uplink ports must be members of same VLAN.

- After you enter **no disable** in the FVRP mode, the software initially blocks all access ports for 35 seconds for the Master election.

Refer to the FVRP chapter in the *FTOS Configuration Guide* for more information on the protocol and configuring it.

disable

C-Series	No
E-Series	✓

Enable or disable FVRP globally on the switch.

Syntax **disable**

To enable FVRP, enter **no disable**.

Defaults FVRP is not enabled, by default.

Command Mode PROTOCOL FVRP

Usage Information After you enter **no disable**, the software initially blocks all access ports for 35 seconds to complete the FVRP Master election.

To enable FVRP, you must enable it globally and on each VLAN (using the no fvrp disable command).

Parameters

fvrp disable	Disable or enable FVRP on a VLAN.

fvrp access

C-Series	No
E-Series	✓

Designate a Layer 2 interface as an FVRP access port and then assign it to an FVRP region.

Syntax **fvrp access** [**region** *region-name*]

To remove the FVRP access configuration, enter **no fvrp access**.

Parameters

region *region-name*	(OPTIONAL) Enter the keyword **region** followed by the region name to which interface belongs. Configure the region parameter AFTER you specified the interface as an FVRP access port.

Defaults

Not configured.

Command Modes

INTERFACE

Usage Information

The interface must be enabled (**no shutdown**), in Layer 2 mode (**switchport**) and a member of an FVRP-enabled VLAN.

To assign an FVRP region, the interface must already have the fvrp access command configured. Refer the screen shot below

```
Force10(conf-if)#show config
!
interface GigabitEthernet 0/3
 no ip address
 fvrp access
 shutdown
Force10(conf-if)#fvrp access region nelson
Force10(conf-if)#show config
!
interface GigabitEthernet 0/3
 no ip address
 fvrp access
 fvrp access region nelson
 shutdown
Force10(conf-if)#
```

The interface is configured as an FVRP access port

Now assign a region name

Figure 218 Configuring an FVRP Region Name Example

You cannot assign a region name to an interface that is not an FVRP access interface; FTOS returns an error.

To include the access links in the same region as the core switches configure the same region in the fvrp access command as you configured in the fvrp core region command.

Related Commands

fvrp core region	Configure a region name.

fvrp aware

C-Series	No
E-Series	✓

Identify that the interface is connected to an FVRP aware system.

Syntax **fvrp aware**

To remove the designation, enter **no fvrp aware**.

Defaults Not configured.

Command Modes INTERFACE

fvrp control-vlan

C-Series	No
E-Series	✓

Assign a control VLAN, which is a VLAN that sends and receives FVRP control messages.

Syntax **fvrp control-vlan** *vlan-id*

To remove a VLAN as the control VLAN, use the **no fvrp control-vlan** *vlan-id* command.

Parameters

vlan-id	Enter a VLAN ID as the control VLAN for the FVRP region. Range: 1 to 4095

Defaults Not configured.

Command Modes PROTOCOL FVRP

Usage Information The control VLAN must be configured on all interfaces of FVRP-aware systems and on interfaces that connect FVRP unaware systems to FVRP core switches.

fvrp core

C-Series	No
E-Series	✓

Assign a VLAN as the core switch for a VLAN or FVRP domain.

Syntax **fvrp core**

To remove the core switch designation, enter **no fvrp core**.

Defaults Not configured.

Command Modes VLAN

fvrp core region

C-Series	No
E-Series	✓

Assign a name to the FVRP region. An FVRP region is a collection of access switches that are multi-homed to a common set of core switches.

Syntax **fvrp core region** *region-name*

To remove a region name, use the **no fvrp core region** [*region-name*] command.

Parameters

region-name	Enter a name up to 32 characters long.

Defaults Not configured.

Command Modes PROTOCOL FVRP

Usage Information All access links in this FVRP region must configured with the same region name (using the fvrp access command).

Related Commands

fvrp access	Specify an interface as an FVRP access port and assign it to a region.

fvrp disable

C-Series	No
E-Series	✓

Disable FVRP on a VLAN.

Syntax **fvrp disable**

To enable FVRP on a VLAN, enter **no fvrp disable**.

Defaults FVRP is disabled, by default.

Command Modes VLAN

Usage Information You must also enable FVRP globally on the E-Series by entering no disable in the FVRP mode.

fvrp domain

C-Series	No
E-Series	✓

Assign a Master VLAN and member VLANs of an FVRP domain. An FVRP domain is a group of VLANs that share the same FVRP configuration and FVRP failover behavior.

Syntax **fvrp domain master-vlan** *vlan-id* **vlan-member** *vlan-range*

To remove a FVRP domain, use the **no fvrp domain master-vlan** *vlan-id* **vlan-member** *vlan-range* command.

Parameters

vlan-id	Enter the VLAN ID of the FVRP Master VLAN. Range: 1 to 4095
vlan-member *vlan-range*	Enter the keyword **vlan-member** followed by the VLAN IDs of VLANs that share the same master core and standby core switches within a region. Use commas (,) to list the member VLANs or use a dash (-) to specify a range of VLANs. Range: 1 to 4095

Defaults Not configured.

Command Modes PROTOCOL FVRP

Usage Information

Note: The two core FVRP switches in a domain must contain the same domain configuration (that is, the same master VLAN and same member VLANs).

In an FVRP domain, the master VLAN configuration is applied to the member VLANs.

A VLAN cannot be a member of multiple FVRP domains within a single FVRP region.

fvrp group

C-Series	No
E-Series	✓

Place redundant links between the core and access in a group by assigning them a group number.

Syntax **fvrp** *interface* **group** *number*

To remove an interface from an FVRP group, use the **no fvrp** *interface* **group** *number* command.

Parameters

interface	Enter the following keywords and slot/port or number information: • For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For a Port Channel interface, enter the keyword **port-channel** followed by a number from 1 to 32 for EtherScale, 1 to 255 for TeraScale. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information.
number	After the keyword **group**, enter a group number. When redundant access links are grouped together, the software selects only one link as master link. Default: 1 Range: 1 to 256.

Defaults Not configured.

Command Modes VLAN

Usage Information When you group redundant links together, the software chooses one link as the Master access link and forwards traffic on that link only. If that link fails, the software forwards traffic on another link in the group.

fvrp hello-time

C-Series	No
E-Series	✓

Configure the time interval between FVRP hello packets.

Syntax **fvrp hello-time** *seconds*

To return to the default value, use the **no fvrp hello-time**.

Parameters		
	seconds	Enter the number of seconds between FVRP hello packets. Range: 1 to 256. Default: 1

Defaults 1 second

Command Modes VLAN

fvrp preempt

C-Series	No
E-Series	✓

Permit an interface to become the master if the master link goes down.

Syntax **fvrp** *interface* **preempt**

To disable preemption on an interface, enter **no fvrp** *interface* **preempt**.

Parameters		
	interface	Enter the following keywords and slot/port or number information: • For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For a Port Channel interface, enter the keyword **port-channel** followed by a number from 1 to 32 for EtherScale, 1 to 255 for TeraScale. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information.

Defaults Enabled (that is, if a link goes down, the interface may become Master.)

Command Modes VLAN

fvrp priority (for a VLAN)

C-Series	No
E-Series	✓

Assign a priority to a VLAN or domain. The priority value is used in the FVRP Master switch election for a VLAN or domain.

Syntax **fvrp priority** *priority*

To return to the default, enter **no fvrp priority** *priority*.

Parameters

priority	Enter a number as the priority for the VLAN. Range: 1 to 256. Default: 128

Defaults 128

Command Modes VLAN

Usage Information In the FVRP Master switch election process, the VLAN with the lower priority is favored.

fvrp priority (for an interface)

C-Series	**No**
E-Series	✓

Assign a priority to an access link. This priority is used in the master link election process.

Syntax **fvrp** *interface* **priority** *priority*

To return to the default priority, enter **no fvrp** *interface* **priority**.

Parameters

interface	Enter the following keywords and slot/port or number information: • For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For a Port Channel interface, enter the keyword **port-channel** followed by a number from 1 to 32 for EtherScale, 1 to 255 for TeraScale. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information.
priority	Enter a number as the priority for the interface. Priority is used to determine which interfaces are blocking or forwarding. Default: 128 Range: 1 to 256.

Defaults *priority* = 128

Command Modes VLAN

Usage Information In the FVRP master access link election process, the interface with the lower priority is favored.

fvrp uplink

C-Series	No
E-Series	✓

Designate an interface as an FVRP uplink port.

Syntax **fvrp uplink**

To remove the uplink designation, enter **no fvrp uplink**.

Defaults Not configured.

Command Mode INTERFACE

Usage Information FVRP tracks this link. If this link goes down, the priority value assigned to that interface (fvrp priority (for an interface) command) is added to the priority value for the VLAN. The Master election occurs again and the VLAN with the highest priority (lowest priority value) is chosen as the Master.

protocol fvrp

C-Series	No
E-Series	✓

Enter the Force10 VLAN Redundancy Protocol (FVRP) mode. In this mode, you can enable or disable FVRP for the E-Series.

Syntax **protocol fvrp**

To remove the global FVRP configuration, enter **no protocol fvrp**.

Defaults Not configured.

Command Modes CONFIGURATION

Usage Information FVRP initially blocks all access ports for 35 seconds after the feature is enabled to complete the Master election process.

FVRP is a Force10 proprietary protocol for VLAN redundancy and all VLAN links must be redundant. You can also use this feature for load balancing.

To enable FVRP globally on a switch, enter no disable command in the FVRP mode.

show config

C-Series	No
E-Series	✓

View configuration information.

Syntax **show config**

Command Mode PROTOCOL FVRP

Example

```
Force10(conf-fvrp)#show conf
 no disable
 fvrp control-vlan 4094
 fvrp core region melbourne
 fvrp domain master-vlan 1 member-vlan 1-4000
Force10(conf-fvrp)#
```

Figure 219 show config Command Example

show fvrp

C-Series	No
E-Series	✓

View configuration and status of FVRP for a VLAN. Displays which ports are blocking or forwarding.

Syntax **show fvrp** {**region** [*region-name*] | **vlan** *vlan-id* [*brief*]}

Parameters

region [*region-name*]	Enter the keyword **region** to view the FVRP regions configured on the system. • *region-name:* enter the region name assigned to view information on that region only.
vlan *vlan-id*	Enter the keyword **vlan** followed by the VLAN ID to view the FVRP configuration for the VLAN.
brief	(OPTIONAL) Enter the keyword **brief** to view a subset of the FVRP configuration information.

Command Mode EXEC

EXEC privilege

Example

```
Force10#show fvrp vlan 4
          FVRP Vlan 4 Information
          FVRP Vlan Enabled
          FVRP Vlan Mode: Core
          FVRP Vlan State: Master
          FVRP Vlan priority: 100
          FVRP Vlan Hello time: 1
          FVRP Master Vlan : 1
     Core   Port 1 (GigabitEthernet 0/0)
     Core   Port 2 (GigabitEthernet 0/1)
     Access Port 23 (GigabitEthernet 0/22) group 0 priority 128 is Forwarding
     Access Port 7 (GigabitEthernet 0/6) group 0 priority 128 is Forwarding
Force10#
```

Figure 220 show fvrp Command Example

Table 44 describes the information in Figure 220

Table 44 show frvp Command Example Fields

Fields	Descriptions
FVRP VLAN	States whether FVRP is enabled on the VLAN.
FVRP VLAN Mode	Displays either Core or Access depending on the configuration of the VLAN.
FVRP VLAN State	Displays either Master or Standby, depending on the Master election process.
FVRP VLAN Priority	Displays the FVRP priority.
FVRP VLAN Hello time	Displays the interval between FVRP hello packets.
Core Port	Lists all the VLAN members that are participating as FVRP core ports and connecting FVRP core switches.
Access Port	Lists all the VLAN members that are connecting FVRP core switches to edge devices.
Uplinks	(Not found in all configurations). Lists all VLAN members connecting the FVRP core to another network.

```
Force10#show fvrp region
Core region "dunedin" active ports are :
     Core     Port 1 (GigabitEthernet 0/0)
     Core     Port 2 (GigabitEthernet 0/1)
     Core     Port 24 (GigabitEthernet 0/23)
     Access   Port 7 (GigabitEthernet 0/6)
     Access   Port 23 (GigabitEthernet 0/22)
Domain Master VLAN 1 Member VLANs 1-4000
Force10#
```

Figure 221 show fvrp region Command Example

Chapter 25 VLAN-Stack VLANs

Platform Specific Feature: VLAN-Stack VLANs are supported on E-Series only.

With the VLAN-Stack feature, you can "stack" VLANs into one tunnel and switch them through the network. The commands included are:

- member on page 600
- vlan-stack access on page 600
- vlan-stack compatible on page 601
- vlan-stack protocol-type on page 602
- vlan-stack trunk on page 603

Important Points to Remember

- Spanning-tree BPDU from the customer's networks are tunneled across the VLAN-Stack network if STP is *not* enabled on VLAN-Stack network. However, if STP is enabled in VLAN-Stack network, STP BPDU from the customer's networks are consumed and not tunneled across the network.
- Layer 3 protocols are not supported on a VLAN-Stack network.
- Assigning an IP address to a VLAN-Stack VLAN is supported when all the members are only VLAN-Stack truck ports. IP addresses on a VLAN-Stack enabled VLAN is not supported if the VLAN contains VLAN-Stack access ports. This facility is provided for SNMP management over a VLAN-Stack enabled VLAN containing only VLAN-Stack trunk interfaces. Layer 3 routing protocols on such a VLAN are not supported.
- It is recommended that you do not use the same MAC address, on different customer VLANs, on the same VLAN-Stack VLAN.
- Interfaces configured using VLAN-Stack Access or VLAN-Stack Trunk commands will not switch traffic for the default VLAN. These interfaces will switch traffic only when they are added to a non-default enbalbe VLAN.

member

C-Series	No
E-Series	✓

Assign a VLAN-Stack access or trunk port to a VLAN. The VLAN must contain the vlan-stack compatible command in its configuration.

Syntax **member** *interface*

To remove an interface from a VLAN-Stack, use the **no member** *interface* command.

Parameters

interface	Enter the following keywords and slot/port or number information: • For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For a Port Channel, enter the keyword **port-channel** followed by a number from 1 to 32 for EtherScale, 1 to 255 for TeraScale. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information.

Defaults Not configured.

Command Mode VLAN

Usage Information You must enable VLAN-Stacking (using the vlan-stack compatible command) on the VLAN prior to adding a member to the VLAN.

Related Commands

vlan-stack compatible	Enable VLAN-Stacking on a VLAN.

vlan-stack access

C-Series	No
E-Series	✓

Specify a Layer 2 interface as an Access port to the VLAN-Stack network.

Syntax **vlan-stack access**

To remove access port designation, enter **no vlan-stack access**.

Defaults Not configured.

Command Modes INTERFACE

Usage Information

Prior to enabling this command, you must enter the **switchport** command to place the interface in Layer 2 mode.

To remove the access port designation, the port must be removed (using the **no member** *interface* command) from all VLAN-Stack enabled VLANs.

vlan-stack compatible

C-Series	**No**
E-Series	✔

Enable VLAN-Stacking on a VLAN.

Syntax **vlan-stack compatible**

To disable VLAN-Stacking on a VLAN, enter **no vlan-stack compatible**.

Defaults Not configured.

Command Modes VLAN

Usage Information

You must remove the members prior to disabling VLAN-Stacking on the VLAN.

To view VLAN-Stack VLANs, use the **show vlan** command in the EXEC privilege mode. VLAN-Stack VLANs contain members, designated by the M in the Q column of the command output

```
Force10#show vlan

Codes: * - Default VLAN, G - GVRP VLANs

    NUM    Status    Q Ports
*   1      Inactive
    2      Active    M Gi 13/13
                     M Gi 13/0-2
    3      Active    M Po1(Gi 13/14-15)
                     M Gi 13/18
                     M Gi 13/3
    4      Active    M Po1(Gi 13/14-15)
                     M Gi 13/18
                     M Gi 13/4
    5      Active    M Po1(Gi 13/14-15)
                     M Gi 13/18
                     M Gi 13/5
Force10#
```

Figure 222 show vlan Command Example with VLAN-Stack VLANs

vlan-stack protocol-type

C-Series	No
E-Series	✓

Define the VLAN-Stack tag. If you do not configure this command, the tag 0x9100 is assigned to traffic on VLAN-Stack VLANs.

Syntax **vlan-stack protocol-type** *number*

To return to the default value for the VLAN-Stack tag, enter **no vlan-stack protocol-type**.

Parameters

number	Enter the hexadecimal number as the VLAN-Stack tag. FTOS accepts the Most Significant Byte (MSB) number and then appends the MSB number with the Least Significant Byte (LSB) of all zeros. Default: 9100

Defaults 9100

Command Modes CONFIGURATION

Note: On earlier versions of FTOS, this command required entering the complete VLAN-Stack tag number, for example 9200. Entering the complete value (MSB and LSB) will now generate a “Value out of range” error message.

The example below illustrates how to configure a vlan-stack type of 0x9200.

Example

```
Force10 (config)# vlan-stack protocol-type 92
Force10 (config)# end
```

Figure 223 vlan-stack protocol-type command example

The VLAN-Stack tag is added after the Source MAC Address and Destination MAC Address and before the Tag Header in the frame header.

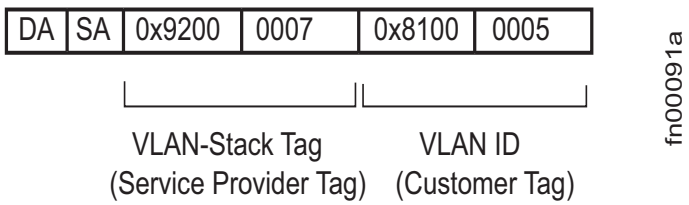


Figure 224 VLAN-Stack Tag

vlan-stack trunk

C-Series	No
E-Series	✓

Specify an interface as a Trunk port to the VLAN-Stack network. You cannot configure VLAN-Stack access ports and VLAN-Stack trunk ports on the same port pipe.

Syntax **vlan-stack trunk**

To remove trunk port designation, enter **no vlan-stack trunk**.

Defaults Not configured.

Command Modes INTERFACE

Usage Information Prior to enabling this command, you must enter the **switchport** command to place the interface in Layer 2 mode.

To remove the trunk port designation, the port must be removed (using the **no member** *interface* command) from all VLAN-Stack enabled VLANs.

Chapter 26 Access Control List

FTOS supports the following types of Access Control Lists (ACLs), IP Prefix Lists, and Route Maps.

- Standard IP ACLs on page 605
- Extended IP ACLs on page 613
- Common IP ACL Commands on page 644
- Standard MAC ACLs on page 647
- Extended MAC ACLs on page 651
- Common MAC Access List Commands on page 656
- IP Prefix List Commands on page 658
- Route Map Commands on page 664
- AS-Path Commands on page 681
- IP Community List Commands on page 685

Standard IP ACLs

Below are the commands needed to configure a Standard IP access control list (ACL).

- deny on page 606
- ip access-list standard on page 607
- permit on page 608
- remark on page 609
- resequence access-list on page 610
- resequence prefix-list ipv4 on page 611
- seq on page 611

deny

Configure a filter to drop packets with a certain IP address.

Syntax **deny** {*source* [*mask*] | **any | host** *ip-address*} [**count** [**byte**] | **log**] [**order**] [**monitor**]

To remove this filter, you have two choices:

- use the **no seq** *sequence-number* command syntax if you know the filter's sequence number or
- use the **no deny** {*source* [*mask*] | **any | host** *ip-address*} command.

Parameters

source	Enter the IP address in dotted decimal format of the network from which the packet was sent.
mask	(OPTIONAL) Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.
any	Enter the keyword **any** to specify that all routes are subject to the filter.
host *ip-address*	Enter the keyword **host** followed by the IP address to specify a host IP address only.
count	(OPTIONAL) Enter the keyword **count** to count packets processed by the filter.
byte	(OPTIONAL) Enter the keyword **byte** to count bytes processed by the filter.
log	(OPTIONAL) Enter the keyword **log** to enter ACL matches in the log.
order	(OPTIONAL) Enter the keyword **order** to specify the QoS order of priority for the ACL entry. Range: 0-254 (where 0 is the highest priority and 254 is the lowest; lower order numbers have a higher priority) Default: If the **order** option is not configure, by default ACLs will have the lowest default order (255).
monitor	(OPTIONAL) Enter the keyword **monitor** to monitor traffic on the monitoring interface specified in the flow-based monitoring session along with the filter operation.

Defaults Not configured.

Command Modes ACCESS-LIST (conf-std-nacl)

Command History

Version 7.4.1.0	Added support for non-contiguous mask and added the **monitor** option.
Version 6.5.1.0	Expanded to include the optional QoS **order** priority for the ACL entry.

Usage Information The **order** option is relevant in the context of the Policy QoS feature only. See the "Quality of Service" chapter of the *FTOS Configuration Guide* for more information.

The **monitor** option is relevant in the context of the flow-based monitoring feature only. See the Chapter 18, “Port Monitoring,” on page 515.

Note: When ACL logging and byte counters are configured simultaneously, byte counters may display an incorrect value. Configure packet counters with logging instead.

Related Commands

ip access-list standard	Configure a standard ACL.
permit	Configure a permit filter.

ip access-list standard

Create a standard access list to filter based on IP address.

Syntax **ip access-list standard** *access-list-name*

To delete an access list, use the **no ip access-list standard** *access-list-name* command.

Parameters

access-list-name	Enter a string up to 16 characters long as the access list name.

Defaults All IP access lists contain an implicit “deny any,” that is, if no match occurs, the packet is dropped.

Example

```
Force10(conf)#ip access-list standard dilling
Force10(config-ext-nacl)#
```

Figure 225 ip access-list standard Command Example

Command Modes CONFIGURATION (conf-std-nacl)

Usage Information The FTOS supports one IP ACL per interface.

The number of entries allowed per ACL is hardware-dependent. Refer to your line card documentation for detailed specification on entries allowed per ACL.

Related Commands

ip access-list extended	Create an extended access list.
show config	View the current configuration.

permit

Configure a filter to permit packets from a specific source IP address to leave the E-Series.

Syntax

permit {*source* [*mask*] | **any** | **host** *ip-address*} [**count** [**byte**] | **log**] [**order**] [**monitor**]

To remove this filter, you have two choices:

- use the **no seq** *sequence-number* command syntax if you know the filter's sequence number or
- use the **no permit** {*source* [*mask*] | **any | host** *ip-address*} command.

Parameters

source	Enter the IP address in dotted decimal format of the network from which the packet was sent.
mask	(OPTIONAL) Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.
any	Enter the keyword **any** to specify that all routes are subject to the filter.
host *ip-address*	Enter the keyword **host** followed by the IP address to specify a host IP address or hostname.
count	(OPTIONAL) Enter the keyword **count** to count packets processed by the filter.
byte	(OPTIONAL) Enter the keyword **byte** to count bytes processed by the filter.
log	(OPTIONAL) Enter the keyword **log** to enter ACL matches in the log.
order	(OPTIONAL) Enter the keyword **order** to specify the QoS order of priority for the ACL entry. Range: 0-254 (where 0 is the highest priority and 254 is the lowest; lower order numbers have a higher priority) Default: If the **order** option is not configure, by default ACLs will have the lowest default order (255).
monitor	(OPTIONAL) Enter the keyword **monitor** to monitor traffic on the monitoring interface specified in the flow-based monitoring session along with the filter operation.

Defaults

Not configured.

Command Modes

ACCESS-LIST (conf-std-nacl)

Command History

Version 7.4.1.0	Added support for non-contiguous mask and added the **monitor** option.
Version 6.5.10	Expanded to include the optional QoS **order** priority for the ACL entry.

Usage Information

The **order** option is relevant in the context of the Policy QoS feature only. See the the "Quality of Service" chapter of the *FTOS Configuration Guide* for more information.

The **monitor** option is relevant in the context of the flow-based monitoring feature only. See the Chapter 18, "Port Monitoring," on page 515.

Note: When ACL logging and byte counters are configured simultaneously, byte counters may display an incorrect value. Configure packet counters with logging instead.

Related Commands

deny	Assign a IP ACL filter to deny IP packets.
ip access-list standard	Create a standard ACL.

remark

Enter a description for an ACL entry.

Syntax

remark [*remark number*] [*description*]

To delete the description, use the **no remark** [*remark number*] command. Note that it is not necessary to include the remark description that you are deleting.

Parameters

remark number	Enter the remark number. Note that the same sequence number can be used for the remark and an ACL rule. Range: 0 to 4294967290
description	Enter a description of up to 80 characters.

Defaults

Not configured

Command Modes

ACCESS-LIST (conf-std-nacl)

Command History

Version 6.4.1.0	Introduced

Example

```
Force10(config-std-nacl)#remark 10 Deny rest of the traffic
Force10(config-std-nacl)#remark 5 Permit traffic from XYZ Inc.
Force10(config-std-nacl)#show config
!
ip access-list standard test
remark 5 Permit traffic from XYZ Inc.
seq 5 permit 1.1.1.0/24
remark 10 Deny rest of the traffic
seq 10 Deny any
Force10(config-std-nacl)#
```

Usage Information

As shown in the example above, the same sequence number is used for the remark and an ACL rule. The remark will precede the rule in the running-configuration because it is assumed that the remark is for that rule or that group of rules that follow the remark. You can configure up to 4294967290 remarks in a given ACL.

Related Commands		
	show config	Display the current ACL configuration.

resequence access-list

Re-assign sequence numbers to entries of an existing access-list.

Syntax **resequence access-list** {**ipv4** | **mac**} {*access-list-name StartingSeqNum Step-to-Increment* }

Parameters

ipv4 | **mac**	Enter the keyword **ipv4**, or **mac** to identify the access list type to resequence.
access-list-name	Enter the name of a configured IP access list.
StartingSeqNum	Enter the starting sequence number to resequence. Range: 0 - 4294967290
Step-to-Increment	Enter the step to increment the sequence number. Range: 1 - 4294967290

Defaults No default values or behavior

Command Modes EXEC

EXEC privilege

Command History

Version 7.4.1.0	Introduced

Usage Information When all sequence numbers have been exhausted, this feature permits re-assigning new sequence number to entries of an existing access-list.

Related Commands		
	resequence prefix-list ipv4	Resequence a prefix list

resequence prefix-list ipv4

Re-assign sequence numbers to entries of an existing prefix list.

Syntax **resequence prefix-list ipv4** {*prefix-list-name StartingSeqNum Step-to-increment*}

Parameters

prefix-list-name	Enter the name of configured prefix list.
StartingSeqNum	Enter the starting sequence number to resequence. Range: 0 – 65535
Step-to-Increment	Enter the step to increment the sequence number. Range: 1 – 65535

Defaults No default values or behavior

Command Modes EXEC

EXEC privilege

Command History

Version 7.4.1.0	Introduced

Usage Information When all sequence numbers have been exhausted, this feature permits re-assigning new sequence number to entries of an existing prefix list.

Related Commands

resequence access-list	Resequence an access-list

seq

Assign a sequence number to a deny or permit filter in an IP access list while creating the filter.

Syntax **seq** *sequence-number* {**deny** | **permit**} {*source* [*mask*] | **any** | **host** *ip-address*}} [**count** [**byte**] | **log**] [**order**] [**monitor**]

To delete a filter, use the **no seq** *sequence-number* command.

Parameters

sequence-number	Enter a number from 0 to 4294967290.
deny	Enter the keyword **deny** to configure a filter to drop packets meeting this condition.

permit	Enter the keyword **permit** to configure a filter to forward packets meeting this criteria.
source	Enter a IP address in dotted decimal format of the network from which the packet was received.
mask	(OPTIONAL) Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.
any	Enter the keyword **any** to specify that all routes are subject to the filter.
host *ip-address*	Enter the keyword **host** followed by the IP address to specify a host IP address or hostname.
count	(OPTIONAL) Enter the keyword **count** to count packets processed by the filter.
byte	(OPTIONAL) Enter the keyword **byte** to count bytes processed by the filter.
log	(OPTIONAL) Enter the keyword **log** to enter ACL matches in the log.
order	(OPTIONAL) Enter the keyword **order** to specify the QoS order of priority for the ACL entry. Range: 0-254 (where 0 is the highest priority and 254 is the lowest; lower order numbers have a higher priority) Default: If the **order** option is not configure, by default ACLs will have the lowest default order (255).
monitor	(OPTIONAL) Enter the keyword **monitor** to monitor traffic on the monitoring interface specified in the flow-based monitoring session along with the filter operation.

Defaults

Not configured

Command Modes

ACCESS-LIST (conf-std-nacl)

Command History

Version 7.4.1.0	Added support for non-contiguous mask and added the **monitor** option.
Version 6.5.10	Expanded to include the optional QoS **order** priority for the ACL entry.

Usage Information

The **monitor** option is relevant in the context of the flow-based monitoring feature only. See the Chapter 18, “Port Monitoring,” on page 515. The **order** option is relevant in the context of the Policy QoS feature only. The following applies:

- The *sequence-number* is applicable only in an ACL-group.
- The **order** option works across ACL-groups that have been applied on an interface via QoS policy framework.
- The **order** option takes precedence over the *sequence-number*.
- If *sequence-number* is **not** configured, then rules with the same order value are ordered according to their configuration-order.
- If the *sequence-number* is configured, then the *sequence-number* is used as a tie breaker for rules with the same order.

Note: When ACL logging and byte counters are configured simultaneously, byte counters may display an incorrect value. Configure packet counters with logging instead.

Related Commands

deny	Configure a filter to drop packets.
permit	Configure a filter to forward packets.

Extended IP ACLs

The following commands configure extended IP ACLs, which in addition to the IP address also examine the packet's protocol type.

- deny on page 613
- deny arp on page 615
- deny ether-type on page 616
- deny icmp on page 618
- deny tcp on page 621
- deny udp on page 623
- ip access-list extended on page 625
- permit on page 626
- permit arp on page 628
- permit ether-type on page 629
- permit icmp on page 631
- permit tcp on page 632
- permit udp on page 635
- resequence access-list on page 637
- resequence prefix-list ipv4 on page 638
- seq arp on page 638
- seq ether-type on page 640
- seq on page 642

deny

Configure a filter that drops IP packets meeting the filter criteria.

Syntax **deny** {**ip** | *ip-protocol-number*} {*source mask* | **any** | **host** *ip-address*} {*destination mask* | **any** | **host** *ip-address*} [**count** [**byte**] | **log**] [**order**] [**monitor**]

To remove this filter, you have two choices:

- use the **no seq** *sequence-number* command syntax if you know the filter's sequence number or
- use the **no deny** {**ip** | *ip-protocol-number*} {*source mask* | **any** | **host** *ip-address*} {*destination mask* | **any** | **host** *ip-address*} command.

Parameters

ip	Enter the keyword **ip** to configure a generic IP access list. The keyword **ip** specifies that the access list will deny all IP protocols.
ip-protocol-number	Enter a number from 0 to 255 to deny based on the protocol identified in the IP protocol header.
source	Enter the IP address of the network or host from which the packets were sent.
mask	Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.
any	Enter the keyword **any** to specify that all routes are subject to the filter.
host *ip-address*	Enter the keyword **host** followed by the IP address to specify a host IP address.
destination	Enter the IP address of the network or host to which the packets are sent.
count	(OPTIONAL) Enter the keyword **count** to count packets processed by the filter.
byte	(OPTIONAL) Enter the keyword **byte** to count bytes processed by the filter.
log	(OPTIONAL) Enter the keyword **log** to enter ACL matches in the log.
order	(OPTIONAL) Enter the keyword **order** to specify the QoS order of priority for the ACL entry. Range: 0-254 (where 0 is the highest priority and 254 is the lowest; lower order numbers have a higher priority) Default: If the **order** option is not configure, by default ACLs will have the lowest default order (255).
monitor	(OPTIONAL) Enter the keyword **monitor** to monitor traffic on the monitoring interface specified in the flow-based monitoring session along with the filter operation.

Defaults

Not configured.

Command Modes

ACCESS-LIST (config-ext-nacl)

Command History

Version 7.4.1.0	Added support for non-contiguous mask and added the **monitor** option.
Version 6.5.10	Expanded to include the optional QoS **order** priority for the ACL entry.

Usage Information

The **order** option is relevant in the context of the Policy QoS feature only. See the the "Quality of Service" chapter of the *FTOS Configuration Guide* for more information.

The **monitor** option is relevant in the context of the flow-based monitoring feature only. See the Chapter 18, "Port Monitoring," on page 515.

Note: When ACL logging and byte counters are configured simultaneously, byte counters may display an incorrect value. Configure packet counters with logging instead.

Related Commands

deny tcp	Assign a filter to deny TCP packets.
deny udp	Assign a filter to deny UDP packets.
ip access-list extended	Create an extended ACL.

deny arp

Configure an egress filter that drops ARP packets on egress ACL supported line cards (see your line card documentation).

Syntax

deny arp {*destination-mac-address mac-address-mask* | **any**} **vlan** *vlan-id* {*ip-address* | **any** | **opcode** *code-number*} [**count** [**byte**] | **log**] [**order**] [**monitor**]

To remove this filter, use one of the following:

- use the **no seq** *sequence-number* command syntax if you know the filter's sequence number or
- use the **no deny arp** {*destination-mac-address mac-address-mask* | **any**} **vlan** *vlan-id* {*ip-address* | **any** | **opcode** *code-number*} command.

Parameters

destination-mac-address mac-address-mask	Enter a MAC address and mask in the nn:nn:nn:nn:nn format. For the MAC address mask, specify which bits in the MAC address must match. The MAC ACL supports an inverse mask, therefore, a mask of ff:ff:ff:ff:ff:ff allows entries that do not match and a mask of 00:00:00:00:00:00 only allows entries that match exactly.
any	Enter the keyword **any** to match and drop any ARP traffic on the interface.
vlan *vlan-id*	Enter the keyword **vlan** followed by the VLAN ID to filter traffic associated with a specific VLAN. Range: 1 to 4094 To filter all VLAN traffic specify VLAN 1.
ip-address	Enter an IP address in dotted decimal format (A.B.C.D) as the target IP address of the ARP.
opcode *code-number*	Enter the keyword **opcode** followed by the number of the ARP opcode. Range: 1 to 23.
count	(OPTIONAL) Enter the keyword **count** to count packets processed by the filter.

byte	(OPTIONAL) Enter the keyword **byte** to count bytes processed by the filter.
log	(OPTIONAL) Enter the keyword **log** to have the information kept in an ACL log file.
order	(OPTIONAL) Enter the keyword **order** to specify the QoS order of priority for the ACL entry. Range: 0-254 (where 0 is the highest priority and 254 is the lowest; lower order numbers have a higher priority) Default: If the **order** option is not configure, by default ACLs will have the lowest default order (255).
monitor	(OPTIONAL) Enter the keyword **monitor** to monitor traffic on the monitoring interface specified in the flow-based monitoring session along with the filter operation.

Defaults

Not configured.

Command Modes

ACCESS-LIST (config-ext-nacl)

Command History

Version 7.4.1.0	Added **monitor** option
Version 6.5.10	Expanded to include the optional QoS **order** priority for the ACL entry.

Usage Information

The **order** option is relevant in the context of the Policy QoS feature only. See the the "Quality of Service" chapter of the *FTOS Configuration Guide* for more information.

The **monitor** option is relevant in the context of the flow-based monitoring feature only. See the Chapter 18, "Port Monitoring," on page 515.

You cannot include IP, TCP or UDP (Layer 3) filters in an ACL configured with ARP or Ether-type (Layer 2) filters. Apply Layer 2 ACLs (ARP and Ether-type) to Layer 2 interfaces only.

Note: When ACL logging and byte counters are configured simultaneously, byte counters may display an incorrect value. Configure packet counters with logging instead.

deny ether-type

Configure an egress filter that drops specified types of Ethernet packets on egress ACL supported line cards (see your line card documentation).

Syntax

deny ether-type *protocol-type-number* {*destination-mac-address mac-address-mask* | **any**} **vlan** *vlan-id* {*source-mac-address mac-address-mask* | **any**} [**count** [**byte**] | **log**] [**order**] [**monitor**]

To remove this filter, use one of the following:

- use the **no seq** *sequence-number* command syntax if you know the filter's sequence number or
- use the **no deny ether-type** *protocol-type-number* {*destination-mac-address mac-address-mask* | **any**} **vlan** *vlan-id* {*source-mac-address mac-address-mask* | **any**} command.

Parameters

protocol-type-number	Enter a number from 600 to FFFF as the specific Ethernet type traffic to drop.
destination-mac-address mac-address-mask	Enter a MAC address and mask in the nn:nn:nn:nn:nn:nn format. For the MAC address mask, specify which bits in the MAC address must match. The MAC ACL supports an inverse mask, therefore, a mask of ff:ff:ff:ff:ff:ff allows entries that do not match and a mask of 00:00:00:00:00:00 only allows entries that match exactly.
any	Enter the keyword **any** to match and drop specific Ethernet traffic on the interface.
vlan *vlan-id*	Enter the keyword **vlan** followed by the VLAN ID to filter traffic associated with a specific VLAN. Range: 1 to 4094 To filter all VLAN traffic specify VLAN 1.
source-mac-address mac-address-mask	Enter a MAC address and mask in the nn:nn:nn:nn:nn:nn format. For the MAC address mask, specify which bits in the MAC address must match. The MAC ACL supports an inverse mask, therefore, a mask of ff:ff:ff:ff:ff:ff allows entries that do not match and a mask of 00:00:00:00:00:00 only allows entries that match exactly.
count	(OPTIONAL) Enter the keyword **count** to count packets processed by the filter.
byte	(OPTIONAL) Enter the keyword **byte** to count bytes processed by the filter.
log	(OPTIONAL) Enter the keyword **log** to have the information kept in an ACL log file.
order	(OPTIONAL) Enter the keyword **order** to specify the QoS order of priority for the ACL entry. Range: 0-254 (where 0 is the highest priority and 254 is the lowest; lower order numbers have a higher priority) Default: If the **order** option is not configure, by default ACLs will have the lowest default order (255).
monitor	(OPTIONAL) Enter the keyword **monitor** to monitor traffic on the monitoring interface specified in the flow-based monitoring session along with the filter operation.

Defaults

Not configured.

Command Modes

ACCESS-LIST (config-ext-nacl)

Command History

Version 7.4.1.0	Added **monitor** option
Version 6.5.10	Expanded to include the optional QoS **order** priority for the ACL entry.

Usage Information

The **order** option is relevant in the context of the Policy QoS feature only. See the the "Quality of Service" chapter of the *FTOS Configuration Guide* for more information.

The **monitor** option is relevant in the context of the flow-based monitoring feature only. See the Chapter 18, "Port Monitoring," on page 515.

You cannot include IP, TCP or UDP (Layer 3) filters in an ACL configured with ARP or Ether-type (Layer 2) filters. Apply Layer 2 ACLs (ARP and Ether-type) to Layer 2 interfaces only.

Note: When ACL logging and byte counters are configured simultaneously, byte counters may display an incorrect value. Configure packet counters with logging instead.

deny icmp

Configure a filter to drop all or specific ICMP messages.

Syntax

deny icmp {*source mask* | **any** | **host** *ip-address*} {*destination mask* | **any** | **host** *ip-address*} [*message-type*] [**count** [**byte**] | **log**] [**order**] [**monitor**]

To remove this filter, you have two choices:

- use the **no seq** *sequence-number* command syntax if you know the filter's sequence number or
- use the **no deny icmp** {*source mask* | **any** | **host** *ip-address*} {*destination mask* | **any** | **host** *ip-address*} command.

Parameters

source	Enter the IP address of the network or host from which the packets were sent.
mask	Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.
any	Enter the keyword **any** to specify that all routes are subject to the filter.
host *ip-address*	Enter the keyword **host** followed by the IP address to specify a host IP address.
destination	Enter the IP address of the network or host to which the packets are sent.
message-type	(OPTIONAL) Enter an ICMP message type, either with the type (and code, if necessary) numbers or with the name of the message type (ICMP message types are listed in Table 45). Range: 0 to 255 for ICMP type; 0 to 255 for ICMP code

count	(OPTIONAL) Enter the keyword **count** to count packets processed by the filter.
byte	(OPTIONAL) Enter the keyword **byte** to count bytes processed by the filter.
log	(OPTIONAL) Enter the keyword **log** to have the information kept in an ACL log file.
order	(OPTIONAL) Enter the keyword **order** to specify the QoS order of priority for the ACL entry. Range: 0-254 (where 0 is the highest priority and 254 is the lowest; lower order numbers have a higher priority) Default: If the **order** option is not configure, by default ACLs will have the lowest default order (255).
monitor	(OPTIONAL) Enter the keyword **monitor** to monitor traffic on the monitoring interface specified in the flow-based monitoring session along with the filter operation.

Defaults

Not configured

Command Modes

ACCESS-LIST (config-ext-nacl)

Command History

Version 7.4.1.0	Added support for non-contiguous mask and added the **monitor** option.
Version 6.5.10	Expanded to include the optional QoS **order** priority for the ACL entry.

Usage Information

The **order** option is relevant in the context of the Policy QoS feature only. See the the "Quality of Service" chapter of the *FTOS Configuration Guide* for more information.

The **monitor** option is relevant in the context of the flow-based monitoring feature only. See the Chapter 18, "Port Monitoring," on page 515.

Note: When ACL logging and byte counters are configured simultaneously, byte counters may display an incorrect value. Configure packet counters with logging instead.

Table 45 lists the keywords displayed in the CLI help and their corresponding ICMP Message Type Name.

Table 45 ICMP Message Type Keywords

Keyword	ICMP Message Type Name
administratively-prohibited	Administratively prohibited
alternate-address	Alternate host address
conversion-error	Datagram conversion error
dod-host-prohibited	Host prohibited
dod-net-prohibited	Net prohibited
echo	Echo
echo-reply	Echo reply

Table 45 ICMP Message Type Keywords (continued)

Keyword	ICMP Message Type Name
general-parameter-problem	Parameter problem
host-isolated	Host isolated
host-precedence-unreachable	Host unreachable for precedence
host-redirect	Host redirect
host-tos-redirect	Host redirect for TOS
host-tos-unreachable	Host unreachable for TOS
host-unknown	Host unknown
host-unreachable	Host unreachable
information-reply	Information replies
information-request	Information requests
mask-reply	Mask replies
mask-request	Mask requests
mobile-redirect	Mobile host redirect
net-redirect	Network redirect
net-tos-redirect	Network redirect for TOS
net-tos-unreachable	Network unreachable for TOS
net-unreachable	Network unreachable
network-unknown	Network unknown
no-room-for-option	Parameter required but no room
option-missing	Parameter required but not present
packet-too-big	Fragmentation needed and DF set
parameter-problem	All parameter problems
port-unreachable	Port unreachable
precedence-unreachable	Precedence cutoff
protocol-unreachable	Protocol unreachable
reassembly-timeout	Reassembly timeout
redirect	All redirects
router-advertisement	Router discovery advertisements
router-solicitation	Router discovery solicitations
source-quench	Source quenches
source-route-failed	Source route failed
time-exceeded	All time exceededs
timestamp-reply	Timestamp replies
timestamp-request	Timestamp requests
traceroute	Traceroute
ttl-exceeded	TTL exceeded
unreachable	All unreachables

deny tcp

Configure a filter that drops TCP packets meeting the filter criteria.

Syntax

deny tcp {*source mask* | **any** | **host** *ip-address*} [*bit*] [*operator port* [*port*]] {*destination mask* | **any** | **host** *ip-address*} [*bit*] [*operator port* [*port*]] [**count** [**byte**] | **log**] [**order**] [**monitor**]

To remove this filter, you have two choices:

- use the **no seq** *sequence-number* command syntax if you know the filter's sequence number or
- use the **no deny tcp** {*source mask* | **any** | **host** *ip-address*} {*destination mask* | **any** | **host** *ip-address*} command.

Parameters

source	Enter the IP address of the network or host from which the packets were sent.
mask	Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.
any	Enter the keyword **any** to specify that all routes are subject to the filter.
host *ip-address*	Enter the keyword **host** followed by the IP address to specify a host IP address.
bit	Enter a flag or combination of bits: **ack:** acknowledgement field **fin**: finish (no more data from the user) **psh:** push function **rst:** reset the connection **syn:** synchronize sequence numbers **urg:** urgent field
operator	(OPTIONAL) Enter one of the following logical operand: • **eq** = equal to • **neq** = not equal to • **gt** = greater than • **lt** = less than • **range** = inclusive range of ports (you must specify two ports for the *port* command parameter.
port port	Enter the application layer port number. Enter two port numbers if using the range logical operand. Range: 0 to 65535. The following list includes some common TCP port numbers: • 23 = Telnet • 20 and 21 = FTP • 25 = SMTP • 169 = SNMP
destination	Enter the IP address of the network or host to which the packets are sent.

mask	Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.
count	(OPTIONAL) Enter the keyword **count** to count packets processed by the filter.
byte	(OPTIONAL) Enter the keyword **byte** to count bytes processed by the filter.
log	(OPTIONAL) Enter the keyword **log** to enter ACL matches in the log. Supported on Jumbo-enabled line cards only.
order	(OPTIONAL) Enter the keyword **order** to specify the QoS order of priority for the ACL entry. Range: 0-254 (where 0 is the highest priority and 254 is the lowest; lower order numbers have a higher priority) Default: If the **order** option is not configure, by default ACLs will have the lowest default order (255).
monitor	(OPTIONAL) Enter the keyword **monitor** to monitor traffic on the monitoring interface specified in the flow-based monitoring session along with the filter operation.

Defaults

Not configured.

Command Modes

ACCESS-LIST (config-ext-nacl)

Command History

Version 7.4.1.0	Added support for non-contiguous mask and added the **monitor** option. Deprecated **established** keyword.
Version 6.5.10	Expanded to include the optional QoS **order** priority for the ACL entry.

Usage Information

The **order** option is relevant in the context of the Policy QoS feature only. See the the "Quality of Service" chapter of the *FTOS Configuration Guide* for more information.

The **monitor** option is relevant in the context of the flow-based monitoring feature only. See the Chapter 18, "Port Monitoring," on page 515.

Note: When ACL logging and byte counters are configured simultaneously, byte counters may display an incorrect value. Configure packet counters with logging instead.

Most ACL rules require one entry in the CAM. However, rules with TCP and UDP port operators (**gt**, **lt**, **range**) may require more than one entry. The range of ports is configured in the CAM based on bitmask boundaries; the space required depends on exactly what ports are included in the range.

For example, an ACL rule with TCP port **range 4000 - 8000** uses 8 entries in the CAM:

```
Rule#       Data              Mask       From  To    #Covered

1     0000111110100000 1111111111100000 4000  4031  32
2     0000111111000000 1111111111000000 4032  4095  64
3     0001000000000000 1111100000000000 4096  6143  2048
4     0001100000000000 1111110000000000 6144  7167  1024
5     0001110000000000 1111111000000000 7168  7679  512
6     0001111000000000 1111111100000000 7680  7935  256
7     0001111100000000 1111111111000000 7936  7999  64
8     0001111101000000 1111111111111111 8000  8000  1

Total Ports: 4001
```

But an ACL rule with TCP port **lt 1023** takes only one entry in the CAM:

```
Rule#       Data              Mask       From  To    #Covered

1     0000000000000000 1111110000000000 0     1023  1024

Total Ports: 1024
```

Related Commands

deny	Assign a filter to deny IP traffic.
deny udp	Assign a filter to deny UDP traffic.

deny udp

Configure a filter to drop UDP packets meeting the filter criteria.

Syntax

deny udp {*source mask* | **any** | **host** *ip-address*} [*operator port* [*port*]] {*destination mask* | **any** | **host** *ip-address*} [*operator port* [*port*]] [**count** [**byte**] | **log**] [**order**] [**monitor**]

To remove this filter, you have two choices:

- use the **no seq** *sequence-number* command syntax if you know the filter's sequence number or
- use the **no deny udp** {*source mask* | **any** | **host** *ip-address*} {*destination mask* | **any** | **host** *ip-address*} command.

Parameters

source	Enter the IP address of the network or host from which the packets were sent.
mask	Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.
any	Enter the keyword **any** to specify that all routes are subject to the filter.
host *ip-address*	Enter the keyword **host** followed by the IP address to specify a host IP address.

operator	(OPTIONAL) Enter one of the following logical operand: • **eq** = equal to • **neq** = not equal to • **gt** = greater than • **lt** = less than • **range** = inclusive range of ports
port port	(OPTIONAL) Enter the application layer port number. Enter two port numbers if using the **range** logical operand. Range: 0 to 65535
destination	Enter the IP address of the network or host to which the packets are sent.
mask	Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.
count	(OPTIONAL) Enter the keyword **count** to count packets processed by the filter.
byte	(OPTIONAL) Enter the keyword **byte** to count bytes processed by the filter.
log	(OPTIONAL) Enter the keyword **log** to enter ACL matches in the log. Supported on Jumbo-enabled line cards only.
order	(OPTIONAL) Enter the keyword **order** to specify the QoS order of priority for the ACL entry. Range: 0-254 (where 0 is the highest priority and 254 is the lowest; lower order numbers have a higher priority) Default: If the **order** option is not configure, by default ACLs will have the lowest default order (255).
monitor	(OPTIONAL) Enter the keyword **monitor** to monitor traffic on the monitoring interface specified in the flow-based monitoring session along with the filter operation.

Defaults

Not configured.

Command Modes

ACCESS-LIST (config-ext-nacl)

Command History

Version 7.4.1.0	Added support for non-contiguous mask and added the **monitor** option.
Version 6.5.10	Expanded to include the optional QoS **order** priority for the ACL entry.

Usage Information

The **order** option is relevant in the context of the Policy QoS feature only. See the the "Quality of Service" chapter of the *FTOS Configuration Guide* for more information

The **monitor** option is relevant in the context of the flow-based monitoring feature only. See the Chapter 18, "Port Monitoring," on page 515..

Note: When ACL logging and byte counters are configured simultaneously, byte counters may display an incorrect value. Configure packet counters with logging instead.

Most ACL rules require one entry in the CAM. However, rules with TCP and UDP port operators (**gt**, **lt**, **range**) may require more than one entry. The range of ports is configured in the CAM based on bitmask boundaries; the space required depends on exactly what ports are included in the range.

For example, an ACL rule with TCP port **range 4000 - 8000** will use 8 entries in the CAM:

```
Rule#       Data             Mask             From  To    #Covered

1     0000111110100000 1111111111100000 4000  4031  32
2     0000111111000000 1111111111000000 4032  4095  64
3     0001000000000000 1111100000000000 4096  6143  2048
4     0001100000000000 1111110000000000 6144  7167  1024
5     0001110000000000 1111111000000000 7168  7679  512
6     0001111000000000 1111111100000000 7680  7935  256
7     0001111100000000 1111111111000000 7936  7999  64
8     0001111101000000 1111111111111111 8000  8000  1

Total Ports: 4001
```

But an ACL rule with TCP port **lt 1023** takes only one entry in the CAM:

```
Rule#       Data             Mask             From  To    #Covered

1     0000000000000000 1111110000000000 0     1023  1024

Total Ports: 1024
```

Related Commands

deny	Assign a deny filter for IP traffic.
deny tcp	Assign a deny filter for TCP traffic.

ip access-list extended

Configure an access list based on IP addresses or protocols.

Syntax **ip access-list extended** *access-list-name*

To delete an access list, use the **no ip access-list extended** *access-list-name* command.

Parameters

access-list-name	Enter a string up to 16 characters long as the access list name.

Defaults All access lists contain an implicit “deny any”; that is, if no match occurs, the packet is dropped.

Example

```
Force10(conf)#ip access-list extended dilling
Force10(config-ext-nacl)#
```

Figure 226 ip access-list extended Command Example

Command Modes CONFIGURATION (config-ext-nacl)

Usage Information The number of entries allowed per ACL is hardware-dependent. Refer to your line card documentation for detailed specification on entries allowed per ACL.

Related Commands

ip access-list standard	Configure a standard access list.
show config	View the current configuration.

permit

Configure a filter to pass IP packets meeting the filter criteria.

Syntax **permit** {**ip |** *ip-protocol-number*} {*source mask* | **any** | **host** *ip-address*} {*destination mask* | **any** | **host** *ip-address*} [**count** [**byte**] | **log**] [**order**] [**monitor**]

To remove this filter, you have two choices:

- use the **no seq** *sequence-number* command syntax if you know the filter's sequence number or
- use the **no deny** {**ip |** *ip-protocol-number*} {*source mask* | **any** | **host** *ip-address*} {*destination mask* | **any** | **host** *ip-address*} command.

Parameters

ip	Enter the keyword **ip** to configure a generic IP access list. The keyword **ip** specifies that the access list will permit all IP protocols.
ip-protocol-number	Enter a number from 0 to 255 to permit based on the protocol identified in the IP protocol header.
source	Enter the IP address of the network or host from which the packets were sent.
mask	Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.
any	Enter the keyword **any** to specify that all routes are subject to the filter.

host *ip-address*	Enter the keyword **host** followed by the IP address to specify a host IP address.
destination	Enter the IP address of the network or host to which the packets are sent.
count	(OPTIONAL) Enter the keyword **count** to count packets processed by the filter.
byte	(OPTIONAL) Enter the keyword **byte** to count bytes processed by the filter.
log	(OPTIONAL) Enter the keyword **log** to enter ACL matches in the log.
order	(OPTIONAL) Enter the keyword **order** to specify the QoS order of priority for the ACL entry. Range: 0-254 (where 0 is the highest priority and 254 is the lowest; lower order numbers have a higher priority) Default: If the **order** option is not configure, by default ACLs will have the lowest default order (255).
monitor	(OPTIONAL) Enter the keyword **monitor** to monitor traffic on the monitoring interface specified in the flow-based monitoring session along with the filter operation.

Defaults

Not configured.

Command Modes

ACCESS-LIST (config-ext-nacl)

Command History

Version 7.4.1.0	Added support for non-contiguous mask and added the **monitor** option.
Version 6.5.10	Expanded to include the optional QoS **order** priority for the ACL entry.

Usage Information

The **order** option is relevant in the context of the Policy QoS feature only. See the the "Quality of Service" chapter of the *FTOS Configuration Guide* for more information.

The **monitor** option is relevant in the context of the flow-based monitoring feature only. See the Chapter 18, "Port Monitoring," on page 515.

Note: When ACL logging and byte counters are configured simultaneously, byte counters may display an incorrect value. Configure packet counters with logging instead.

Related Commands

ip access-list extended	Create an extended ACL.
permit tcp	Assign a permit filter for TCP packets.
permit udp	Assign a permit filter for UDP packets.

permit arp

Configure a filter that forwards ARP packets meeting this criteria.This command is supported only on 12-port GE line cards with SFP optics; refer to your line card documentation for specifications.

Syntax **permit arp** {*destination-mac-address mac-address-mask* | **any**} **vlan** *vlan-id* {*ip-address* | **any** | **opcode** *code-number*} [**count** [**byte**] | **log**] [**order**] [**monitor**]

To remove this filter, use one of the following:

- use the **no seq** *sequence-number* command syntax if you know the filter's sequence number or
- use the **no permit arp** {*destination-mac-address mac-address-mask* | **any**} **vlan** *vlan-id* {*ip-address* | **any** | **opcode** *code-number*} command.

Parameters

destination-mac-address mac-address-mask	Enter a MAC address and mask in the nn:nn:nn:nn:nn format. For the MAC address mask, specify which bits in the MAC address must match. The MAC ACL supports an inverse mask, therefore, a mask of ff:ff:ff:ff:ff:ff allows entries that do not match and a mask of 00:00:00:00:00:00 only allows entries that match exactly.
any	Enter the keyword **any** to match and drop any ARP traffic on the interface.
vlan *vlan-id*	Enter the keyword **vlan** followed by the VLAN ID to filter traffic associated with a specific VLAN. Range: 1 to 4094 To filter all VLAN traffic specify VLAN 1.
ip-address	Enter an IP address in dotted decimal format (A.B.C.D) as the target IP address of the ARP.
opcode *code-number*	Enter the keyword **opcode** followed by the number of the ARP opcode. Range: 1 to 16.
count	(OPTIONAL) Enter the keyword **count** to count packets processed by the filter.
byte	(OPTIONAL) Enter the keyword **byte** to count bytes processed by the filter.
log	(OPTIONAL) Enter the keyword **log** to have the information kept in an ACL log file.
order	(OPTIONAL) Enter the keyword **order** to specify the QoS order of priority for the ACL entry. Range: 0-254 (where 0 is the highest priority and 254 is the lowest; lower order numbers have a higher priority) Default: If the **order** option is not configure, by default ACLs will have the lowest default order (255).
monitor	(OPTIONAL) Enter the keyword **monitor** to monitor traffic on the monitoring interface specified in the flow-based monitoring session along with the filter operation.

Defaults Not configured.

Command Modes ACCESS-LIST (config-ext-nacl)

Command History

Version 7.4.1.0	Added support for non-contiguous mask and added the **monitor** option.
Version 6.5.10	Expanded to include the optional QoS **order** priority for the ACL entry.

Usage Information The **order** option is relevant in the context of the Policy QoS feature only. See the the "Quality of Service" chapter of the *FTOS Configuration Guide* for more information.

The **monitor** option is relevant in the context of the flow-based monitoring feature only. See the Chapter 18, "Port Monitoring," on page 515.

You cannot include IP, TCP or UDP filters in an ACL configured with ARP filters.

Note: When ACL logging and byte counters are configured simultaneously, byte counters may display an incorrect value. Configure packet counters with logging instead.

permit ether-type

Configure a filter that allows traffic with specified types of Ethernet packets. This command is supported only on 12-port GE line cards with SFP optics; refer to your line card documentation for specifications.

Syntax **permit ether-type** *protocol-type-number* {*destination-mac-address mac-address-mask* | **any**} **vlan** *vlan-id* {*source-mac-address mac-address-mask* | **any**} [**count** [**byte**] | **log**] [**order**] [**monitor**]

To remove this filter, use one of the following:

- use the **no seq** *sequence-number* command syntax if you know the filter's sequence number or
- use the **no permit ether-type** *protocol-type-number* {*destination-mac-address mac-address-mask* | **any**} **vlan** *vlan-id* {*source-mac-address mac-address-mask* | **any**} command.

Parameters

protocol-type-number	Enter a number from 600 to FFF as the specific Ethernet type traffic to drop.
destination-mac-address mac-address-mask	Enter a MAC address and mask in the nn:nn:nn:nn:nn format. For the MAC address mask, specify which bits in the MAC address must match. The MAC ACL supports an inverse mask, therefore, a mask of ff:ff:ff:ff:ff:ff allows entries that do not match and a mask of 00:00:00:00:00:00 only allows entries that match exactly.
any	Enter the keyword **any** to match and drop specific Ethernet traffic on the interface.
vlan *vlan-id*	Enter the keyword **vlan** followed by the VLAN ID to filter traffic associated with a specific VLAN. Range: 1 to 4094 To filter all VLAN traffic specify VLAN 1.
source-mac-address mac-address-mask	Enter a MAC address and mask in the nn:nn:nn:nn:nn format. For the MAC address mask, specify which bits in the MAC address must match. The MAC ACL supports an inverse mask, therefore, a mask of ff:ff:ff:ff:ff:ff allows entries that do not match and a mask of 00:00:00:00:00:00 only allows entries that match exactly.
count	(OPTIONAL) Enter the keyword **count** to count packets processed by the filter.
byte	(OPTIONAL) Enter the keyword **byte** to count bytes processed by the filter.
log	(OPTIONAL) Enter the keyword **log** to have the information kept in an ACL log file.
order	(OPTIONAL) Enter the keyword **order** to specify the QoS order of priority for the ACL entry. Range: 0-254 (where 0 is the highest priority and 254 is the lowest; lower order numbers have a higher priority) Default: If the **order** option is not configure, by default ACLs will have the lowest default order (255).
monitor	(OPTIONAL) Enter the keyword **monitor** to monitor traffic on the monitoring interface specified in the flow-based monitoring session along with the filter operation.

Defaults

Not configured.

Command Modes

ACCESS-LIST (config-ext-nacl)

Command History

Version 7.4.1.0	Added **monitor** option
Version 6.5.10	Expanded to include the optional QoS **order** priority for the ACL entry.

Usage Information

The **order** option is relevant in the context of the Policy QoS feature only. See the the "Quality of Service" chapter of the *FTOS Configuration Guide* for more information

The **monitor** option is relevant in the context of the flow-based monitoring feature only. See the Chapter 18, "Port Monitoring," on page 515..

You cannot include IP, TCP or UDP filters in an ACL configured with ARP filters.

Note: When ACL logging and byte counters are configured simultaneously, byte counters may display an incorrect value. Configure packet counters with logging instead.

permit icmp

Configure a filter to allow all or specific ICMP messages.

Syntax **permit icmp** {*source mask* | **any** | **host** *ip-address*} {*destination mask* | **any** | **host** *ip-address*} [*message-type*] [**count** [**byte**] | **log**] [**order**] [**monitor**]

To remove this filter, you have two choices:

- use the **no seq** *sequence-number* command syntax if you know the filter's sequence number or
- use the **no permit icmp** {*source mask* | **any** | **host** *ip-address*} {*destination mask* | **any** | **host** *ip-address*} command.

Parameters

source	Enter the IP address of the network or host from which the packets were sent.
mask	Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.
any	Enter the keyword **any** to specify that all routes are subject to the filter.
host *ip-address*	Enter the keyword **host** followed by the IP address to specify a host IP address.
destination	Enter the IP address of the network or host to which the packets are sent.
message-type	(OPTIONAL) Enter an ICMP message type, either with the type (and code, if necessary) numbers or with the name of the message type (ICMP message types are listed in Table 45). Range: 0 to 255 for ICMP type; 0 to 255 for ICMP code
count	(OPTIONAL) Enter the keyword **count** to count packets processed by the filter.
byte	(OPTIONAL) Enter the keyword **byte** to count bytes processed by the filter.
log	(OPTIONAL) Enter the keyword **log** to have the information kept in an ACL log file.
order	(OPTIONAL) Enter the keyword **order** to specify the QoS order of priority for the ACL entry. Range: 0-254 (where 0 is the highest priority and 254 is the lowest; lower order numbers have a higher priority) Default: If the **order** option is not configure, by default ACLs will have the lowest default order (255).
monitor	(OPTIONAL) Enter the keyword **monitor** to monitor traffic on the monitoring interface specified in the flow-based monitoring session along with the filter operation.

Defaults Not configured

Command Modes ACCESS-LIST (config-ext-nacl)

Command History

Version 7.4.1.0	Added support for non-contiguous mask and added the **monitor** option.
Version 6.5.10	Expanded to include the optional QoS **order** priority for the ACL entry.

Usage Information The **order** option is relevant in the context of the Policy QoS feature only. See the the "Quality of Service" chapter of the *FTOS Configuration Guide* for more information.

The **monitor** option is relevant in the context of the flow-based monitoring feature only. See the Chapter 18, "Port Monitoring," on page 515.

Note: When ACL logging and byte counters are configured simultaneously, byte counters may display an incorrect value. Configure packet counters with logging instead.

permit tcp

Configure a filter to pass TCP packets meeting the filter criteria.

Syntax **permit tcp** {*source mask* | **any** | **host** *ip-address*} [*bit*] [*operator port* [*port*]] {*destination mask* | **any** | **host** *ip-address*} [*bit*] [*operator port* [*port*]] [**count** [**byte**] | **log**] [**order**] [**monitor**]

To remove this filter, you have two choices:

- use the **no seq** *sequence-number* command syntax if you know the filter's sequence number or
- use the **no permit tcp** {*source mask* | **any** | **host** *ip-address*} {*destination mask* | **any** | **host** *ip-address*} command.

Parameters

source	Enter the IP address of the network or host from which the packets were sent.
mask	Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.
any	Enter the keyword **any** to specify that all routes are subject to the filter.
host *ip-address*	Enter the keyword **host** followed by the IP address to specify a host IP address.

bit	Enter a flag or combination of bits: **ack:** acknowledgement field **fin**: finish (no more data from the user) **psh:** push function **rst:** reset the connection **syn:** synchronize sequence numbers **urg:** urgent field
operator	(OPTIONAL) Enter one of the following logical operand: • **eq** = equal to • **neq** = not equal to • **gt** = greater than • **lt** = less than • **range** = inclusive range of ports (you must specify two port for the *port* parameter.)
port port	Enter the application layer port number. Enter two port numbers if using the range logical operand. Range: 0 to 65535. The following list includes some common TCP port numbers: 23 = Telnet 20 and 21 = FTP 25 = SMTP 169 = SNMP
destination	Enter the IP address of the network or host to which the packets are sent.
mask	Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.
count	(OPTIONAL) Enter the keyword **count** to count packets processed by the filter.
byte	(OPTIONAL) Enter the keyword **byte** to count bytes processed by the filter.
log	(OPTIONAL) Enter the keyword **log** to enter ACL matches in the log.
order	(OPTIONAL) Enter the keyword **order** to specify the QoS order of priority for the ACL entry. Range: 0-254 (where 0 is the highest priority and 254 is the lowest; lower order numbers have a higher priority) Default: If the **order** option is not configure, by default ACLs will have the lowest default order (255).
monitor	(OPTIONAL) Enter the keyword **monitor** to monitor traffic on the monitoring interface specified in the flow-based monitoring session along with the filter operation.

Defaults Not configured.

Command Modes ACCESS-LIST (config-ext-nacl)

Command History

Version 7.4.1.0	Added support for non-contiguous mask and added the **monitor** option. Deprecated **established** keyword.
Version 6.5.10	Expanded to include the optional QoS **order** priority for the ACL entry.

Usage Information

The **order** option is relevant in the context of the Policy QoS feature only. See the the "Quality of Service" chapter of the *FTOS Configuration Guide* for more information.

Note: When ACL logging and byte counters are configured simultaneously, byte counters may display an incorrect value. Configure packet counters with logging instead.

The **monitor** option is relevant in the context of the flow-based monitoring feature only. See the Chapter 18, "Port Monitoring," on page 515.

Most ACL rules require one entry in the CAM. However, rules with TCP and UDP port operators (**gt**, **lt**, **range**) may require more than one entry. The range of ports is configured in the CAM based on bitmask boundaries; the space required depends on exactly what ports are included in the range.

For example, an ACL rule with TCP port **range 4000 - 8000** uses 8 entries in the CAM:

```
Rule#       Data             Mask             From  To    #Covered

1     0000111110100000 1111111111100000 4000  4031  32
2     0000111111000000 1111111111000000 4032  4095  64
3     0001000000000000 1111100000000000 4096  6143  2048
4     0001100000000000 1111110000000000 6144  7167  1024
5     0001110000000000 1111111000000000 7168  7679  512
6     0001111000000000 1111111100000000 7680  7935  256
7     0001111100000000 1111111111000000 7936  7999  64
8     0001111101000000 1111111111111111 8000  8000  1

Total Ports: 4001
```

But an ACL rule with TCP port **lt 1023** takes only one entry in the CAM:

```
Rule#       Data             Mask             From  To    #Covered

1     0000000000000000 1111110000000000 0     1023  1024

Total Ports: 1024
```

Related Commands

ip access-list extended	Create an extended ACL.
permit	Assign a permit filter for IP packets.
permit udp	Assign a permit filter for UDP packets.

permit udp

Configure a filter to pass UDP packets meeting the filter criteria.

Syntax **permit udp** {*source mask* | **any** | **host** *ip-address*} [*operator port* [*port*]] {*destination mask* | **any** | **host** *ip-address*} [*operator port* [*port*]] [**count** [**byte**] | **log**] [**order**] [**monitor**]

To remove this filter, you have two choices:

- use the **no seq** *sequence-number* command syntax if you know the filter's sequence number or
- use the **no permit udp** {*source mask* | **any** | **host** *ip-address*} {*destination mask* | **any** | **host** *ip-address*} command.

Parameters

source	Enter the IP address of the network or host from which the packets were sent.
mask	Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.
any	Enter the keyword **any** to specify that all routes are subject to the filter.
host *ip-address*	Enter the keyword **host** followed by the IP address to specify a host IP address.
operator	(OPTIONAL) Enter one of the following logical operand: • **eq** = equal to • **neq** = not equal to • **gt** = greater than • **lt** = less than • **range** = inclusive range of ports (you must specify two ports for the *port* parameter.)
port port	(OPTIONAL) Enter the application layer port number. Enter two port numbers if using the **range** logical operand. Range: 0 to 65535
destination	Enter the IP address of the network or host to which the packets are sent.
count	(OPTIONAL) Enter the keyword **count** to count packets processed by the filter.
byte	(OPTIONAL) Enter the keyword **byte** to count bytes processed by the filter.
log	(OPTIONAL) Enter the keyword **log** to enter ACL matches in the log.

order	(OPTIONAL) Enter the keyword **order** to specify the QoS order of priority for the ACL entry. Range: 0-254 (where 0 is the highest priority and 254 is the lowest; lower order numbers have a higher priority) Default: If the **order** option is not configure, by default ACLs will have the lowest default order (255).
monitor	(OPTIONAL) Enter the keyword **monitor** to monitor traffic on the monitoring interface specified in the flow-based monitoring session along with the filter operation.

Defaults

Not configured.

Command Modes

ACCESS-LIST (config-ext-nacl)

Command History

Version 7.4.1.0	Added support for non-contiguous mask and added the **monitor** option.
Version 6.5.10	Expanded to include the optional QoS **order** priority for the ACL entry.

Usage Information

The **order** option is relevant in the context of the Policy QoS feature only. See the the "Quality of Service" chapter of the *FTOS Configuration Guide* for more information.

The **monitor** option is relevant in the context of the flow-based monitoring feature only. See the Chapter 18, "Port Monitoring," on page 515.

Note: When ACL logging and byte counters are configured simultaneously, byte counters may display an incorrect value. Configure packet counters with logging instead.

Most ACL rules require one entry in the CAM. However, rules with TCP and UDP port operators (**gt**, **lt**, **range**) may require more than one entry. The range of ports is configured in the CAM based on bitmask boundaries; the space required depends on exactly what ports are included in the range.

For example, an ACL rule with TCP port **range 4000 - 8000** uses 8 entries in the CAM:

```
Rule#       Data             Mask       From  To    #Covered

1     0000111110100000 1111111111100000 4000  4031  32
2     0000111111000000 1111111111000000 4032  4095  64
3     0001000000000000 1111100000000000 4096  6143  2048
4     0001100000000000 1111110000000000 6144  7167  1024
5     0001110000000000 1111111000000000 7168  7679  512
6     0001111000000000 1111111100000000 7680  7935  256
7     0001111100000000 1111111111000000 7936  7999  64
8     0001111101000000 1111111111111111 8000  8000  1

Total Ports: 4001
```

But an ACL rule with TCP port **lt 1023** takes only one entry in the CAM:

```
Rule#       Data              Mask       From  To    #Covered
1     0000000000000000 1111110000000000 0     1023  1024
Total Ports: 1024
```

Related Commands

ip access-list extended	Configure an extended ACL.
permit	Assign a permit filter for IP packets.
permit tcp	Assign a permit filter for TCP packets.

resequence access-list

Re-assign sequence numbers to entries of an existing access-list.

Syntax **resequence access-list** {**ipv4** | **mac**} {*access-list-name StartingSeqNum Step-to-Increment* }

Parameters

ipv4 | **mac**	Enter the keyword **ipv4**, or **mac** to identify the access list type to resequence.
access-list-name	Enter the name of a configured IP access list.
StartingSeqNum	Enter the starting sequence number to resequence. Range: 0 - 4294967290
Step-to-Increment	Enter the step to increment the sequence number. Range: 1 - 4294967290

Defaults No default values or behavior

Command Modes EXEC

EXEC privilege

Command History

Version 7.4.1.0	Introduced

Usage Information When all sequence numbers have been exhausted, this feature permits re-assigning new sequence number to entries of an existing access-list.

Related Commands

resequence prefix-list ipv4	Resequence a prefix list

resequence prefix-list ipv4

Re-assign sequence numbers to entries of an existing prefix list.

Syntax **resequence prefix-list ipv4** {*prefix-list-name StartingSeqNum Step-to-increment*}

Parameters

prefix-list-name	Enter the name of configured prefix list.
StartingSeqNum	Enter the starting sequence number to resequence. Range: 0 – 65535
Step-to-Increment	Enter the step to increment the sequence number. Range: 1 – 65535

Defaults No default values or behavior

Command Modes EXEC

EXEC privilege

Command History

Version 7.4.1.0	Introduced

Usage Information When all sequence numbers have been exhausted, this feature permits re-assigning new sequence number to entries of an existing prefix list.

Related Commands

resequence access-list	Resequence an access-list

seq arp

Configure an egress filter with a sequence number that filters ARP packets meeting this criteria. This command is supported only on 12-port GE line cards with SFP optics; refer to your line card documentation for specifications.

Syntax **seq** *sequence-number* {**deny** | **permit}** **arp** {*destination-mac-address mac-address-mask* | **any**} **vlan** *vlan-id* {*ip-address* | **any** | **opcode** *code-number*} [**count** [**byte**] | **log**] [**order**] [**monitor**]

To remove this filter, use the **no seq** *sequence-number* command.

Parameters

sequence-number	Enter a number from 0 to 4294967290.
deny	Enter the keyword **deny** to drop all traffic meeting the filter criteria.

permit	Enter the keyword **permit** to forward all traffic meeting the filter criteria.
destination-mac-address mac-address-mask	Enter a MAC address and mask in the nn:nn:nn:nn:nn format. For the MAC address mask, specify which bits in the MAC address must match. The MAC ACL supports an inverse mask, therefore, a mask of ff:ff:ff:ff:ff:ff allows entries that do not match and a mask of 00:00:00:00:00:00 only allows entries that match exactly.
any	Enter the keyword **any** to match and drop any ARP traffic on the interface.
vlan *vlan-id*	Enter the keyword **vlan** followed by the VLAN ID to filter traffic associated with a specific VLAN. Range: 1 to 4094 To filter all VLAN traffic specify VLAN 1.
ip-address	Enter an IP address in dotted decimal format (A.B.C.D) as the target IP address of the ARP.
opcode *code-number*	Enter the keyword **opcode** followed by the number of the ARP opcode. Range: 1 to 16.
count	(OPTIONAL) Enter the keyword **count** to count packets processed by the filter.
byte	(OPTIONAL) Enter the keyword **byte** to count bytes processed by the filter.
log	(OPTIONAL) Enter the keyword **log** to have the information kept in an ACL log file.
order	(OPTIONAL) Enter the keyword **order** to specify the QoS order of priority for the ACL entry. Range: 0-254 (where 0 is the highest priority and 254 is the lowest; lower order numbers have a higher priority) Default: If the **order** option is not configure, by default ACLs will have the lowest default order (255).
monitor	(OPTIONAL) Enter the keyword **monitor** to monitor traffic on the monitoring interface specified in the flow-based monitoring session along with the filter operation.

Defaults

Not configured.

Command Modes

ACCESS-LIST (config-ext-nacl)

Command History

Version 7.4.1.0	Added **monitor** option
Version 6.5.10	Expanded to include the optional QoS **order** priority for the ACL entry.

Usage Information

The **monitor** option is relevant in the context of the flow-based monitoring feature only. See the Chapter 18, “Port Monitoring,” on page 515.

The **order** option is relevant in the context of the Policy QoS feature only. The following applies:

- The *sequence-number* is applicable only in an ACL-group.

- The **order** option works across ACL-groups that have been applied on an interface via QoS policy framework.
- The **order** option takes precedence over the *sequence-number*.
- If *sequence-number* is **not** configured, then rules with the same order value are ordered according to their configuration-order.
- If the *sequence-number* is configured, then the *sequence-number* is used as a tie breaker for rules with the same order.

Note: When ACL logging and byte counters are configured simultaneously, byte counters may display an incorrect value. Configure packet counters with logging instead.

You cannot include IP, TCP or UDP (Layer 3) filters in an ACL configured with ARP or Ether-type (Layer 2) filters. Apply Layer 2 ACLs to interfaces in Layer 2 mode.

seq ether-type

Configure an egress filter with a specific sequence number that filters traffic with specified types of Ethernet packets. This command is supported only on 12-port GE line cards with SFP optics; refer to your line card documentation for specifications.

Syntax

seq *sequence-number* {**deny | permit**} **ether-type** *protocol-type-number* {*destination-mac-address mac-address-mask* | **any**} **vlan** *vlan-id* {*source-mac-address mac-address-mask* | **any**} [**count** [**byte**] | **log**] [**order**] [**monitor**]

To remove this filter, use the **no seq** *sequence-number* command.

Parameters

sequence-number	Enter a number from 0 to 4294967290.
deny	Enter the keyword **deny** to drop all traffic meeting the filter criteria.
permit	Enter the keyword **permit** to forward all traffic meeting the filter criteria.
protocol-type-number	Enter a number from 600 to FFFF as the specific Ethernet type traffic to drop.
destination-mac-address mac-address-mask	Enter a MAC address and mask in the nn:nn:nn:nn:nn format. For the MAC address mask, specify which bits in the MAC address must match. The MAC ACL supports an inverse mask, therefore, a mask of ff:ff:ff:ff:ff:ff allows entries that do not match and a mask of 00:00:00:00:00:00 only allows entries that match exactly.
any	Enter the keyword **any** to match and drop specific Ethernet traffic on the interface.

vlan *vlan-id*	Enter the keyword **vlan** followed by the VLAN ID to filter traffic associated with a specific VLAN. Range: 1 to 4094 To filter all VLAN traffic specify VLAN 1.
source-mac-address mac-address-mask	Enter a MAC address and mask in the nn:nn:nn:nn:nn format. For the MAC address mask, specify which bits in the MAC address must match. The MAC ACL supports an inverse mask, therefore, a mask of ff:ff:ff:ff:ff:ff allows entries that do not match and a mask of 00:00:00:00:00:00 only allows entries that match exactly.
count	(OPTIONAL) Enter the keyword **count** to count packets processed by the filter.
byte	(OPTIONAL) Enter the keyword **byte** to count bytes processed by the filter.
log	(OPTIONAL) Enter the keyword **log** to have the information kept in an ACL log file.
order	(OPTIONAL) Enter the keyword **order** to specify the QoS order of priority for the ACL entry. Range: 0-254 (where 0 is the highest priority and 254 is the lowest; lower order numbers have a higher priority) Default: If the **order** option is not configure, by default ACLs will have the lowest default order (255).
monitor	(OPTIONAL) Enter the keyword **monitor** to monitor traffic on the monitoring interface specified in the flow-based monitoring session along with the filter operation.

Defaults

Not configured.

Command Modes

ACCESS-LIST (config-ext-nacl)

Command History

Version 7.4.1.0	Added **monitor** option
Version 6.5.10	Expanded to include the optional QoS **order** priority for the ACL entry.

Usage Information

The **monitor** option is relevant in the context of the flow-based monitoring feature only. See the Chapter 18, “Port Monitoring,” on page 515.

The **order** option is relevant in the context of the Policy QoS feature only. The following applies:

- The *sequence-number* is applicable only in an ACL-group.
- The **order** option works across ACL-groups that have been applied on an interface via QoS policy framework.
- The **order** option takes precedence over the *sequence-number*.
- If *sequence-number* is **not** configured, then rules with the same order value are ordered according to their configuration-order.
- If the *sequence-number* is configured, then the *sequence-number* is used as a tie breaker for rules with the same order.

Note: When ACL logging and byte counters are configured simultaneously, byte counters may display an incorrect value. Configure packet counters with logging instead.

You cannot include IP, TCP or UDP (Layer 3) filters in an ACL configured with ARP or Ether-type (Layer 2) filters. Apply Layer 2 filters to interfaces in Layer 2 mode.

seq

Assign a sequence number to a deny or permit filter in an IP access list while creating the filter.

Syntax

seq *sequence-number* {**deny** | **permit**} {*ip-protocol-number* | **icmp | ip | tcp | udp**} {*source mask* | **any** | **host** *ip-address*} {*destination mask* | **any** | **host** *ip-address*} [*operator port* [*port*]] [**count** [**byte**] | **log**] [**order**] [**monitor**]

To delete a filter, use the **no seq** *sequence-number* command.

Parameters

sequence-number	Enter a number from 0 to 4294967290.
deny	Enter the keyword **deny** to configure a filter to drop packets meeting this condition.
permit	Enter the keyword **permit** to configure a filter to forward packets meeting this criteria.
ip-protocol-number	Enter a number from 0 to 255 to filter based on the protocol identified in the IP protocol header.
icmp	Enter the keyword **icmp** to configure an ICMP access list filter.
ip	Enter the keyword **ip** to configure a generic IP access list. The keyword **ip** specifies that the access list will permit all IP protocols.
tcp	Enter the keyword **tcp** to configure a TCP access list filter.
udp	Enter the keyword **udp** to configure a UDP access list filter.
source	Enter the IP address of the network or host from which the packets were sent.
mask	Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.
any	Enter the keyword **any** to specify that all routes are subject to the filter.
host *ip-address*	Enter the keyword **host** followed by the IP address to specify a host IP address.

operator	(OPTIONAL) Enter one of the following logical operands: • **eq** = equal to • **neq** = not equal to • **gt** = greater than • **lt** = less than • **range** = inclusive range of ports (you must specify two ports for the *port* parameter.)
port port	(OPTIONAL) Enter the application layer port number. Enter two port numbers if using the **range** logical operand. Range: 0 to 65535 The following list includes some common TCP port numbers: • 23 = Telnet • 20 and 21 = FTP • 25 = SMTP • 169 = SNMP
destination	Enter the IP address of the network or host to which the packets are sent.
message-type	(OPTIONAL) Enter an ICMP message type, either with the type (and code, if necessary) numbers or with the name of the message type (ICMP message types are listed in Table 45). Range: 0 to 255 for ICMP type; 0 to 255 for ICMP code
count	(OPTIONAL) Enter the keyword **count** to count packets processed by the filter.
byte	(OPTIONAL) Enter the keyword **byte** to count bytes processed by the filter.
log	(OPTIONAL) Enter the keyword **log** to enter ACL matches in the log. Supported on Jumbo-enabled line cards only.
order	(OPTIONAL) Enter the keyword **order** to specify the QoS order of priority for the ACL entry. Range: 0-254 (where 0 is the highest priority and 254 is the lowest; lower order numbers have a higher priority) Default: If the **order** option is not configure, by default ACLs will have the lowest default order (255).
monitor	(OPTIONAL) Enter the keyword **monitor** to monitor traffic on the monitoring interface specified in the flow-based monitoring session along with the filter operation.

Defaults

Not configured.

Command Modes

ACCESS-LIST (config-ext-nacl)

Command History

Version 7.4.1.0	Added support for non-contiguous mask and added the **monitor** option. Deprecated **established** keyword
Version 6.5.10	Expanded to include the optional QoS **order** priority for the ACL entry.

Usage Information

The **monitor** option is relevant in the context of the flow-based monitoring feature only. See the Chapter 18, “Port Monitoring,” on page 515.

The **order** option is relevant in the context of the Policy QoS feature only. The following applies:

- The *sequence-number* is applicable only in an ACL-group.
- The **order** option works across ACL-groups that have been applied on an interface via QoS policy framework.
- The **order** option takes precedence over the *sequence-number*.
- If *sequence-number* is **not** configured, then rules with the same order value are ordered according to their configuration-order.
- If the *sequence-number* is configured, then the *sequence-number* is used as a tie breaker for rules with the same order.

If the *sequence-number* is configured, then the *sequence-number* is used as a tie breaker for rules with the same order.

Note: When ACL logging and byte counters are configured simultaneously, byte counters may display an incorrect value. Configure packet counters with logging instead.

Related Commands

deny	Configure a filter to drop packets.
permit	Configure a filter to forward packets.

Common IP ACL Commands

The following commands allow you to clear, view, and assign IP ACL configurations.

- access-class on page 644
- clear counters ip access-group on page 645
- ip access-group on page 645
- show config on page 646
- show ip accounting access-list on page 646

access-class

Apply a standard ACL to a terminal line.

Syntax

access-class *access-list-name*

To remove an ACL, use the **no access-class** *access-list-name* command.

Parameters

access-list-name	Enter the name of a configured Standard ACL.

Defaults Not configured.

Command Modes LINE

clear counters ip access-group

Erase all counters maintained for access lists.

Syntax **clear counters ip access-group** [*access-list-name*]

Parameters		
	access-list-name	(OPTIONAL) Enter the name of a configured access-list.

Command Modes EXEC privilege

ip access-group

Assign an access list to an interface.

Syntax **ip access-group** *access-list-name* {**in** | **out**} [**implicit-permit**] [**vlan** *vlan-id*]

To delete an IP access-group configuration, use the **no ip access-group** *access-list-name* {**in** | **out**} [**implicit-permit**] [**vlan** *vlan-id*] command.

Parameters		
	access-list-name	Enter the name of a configured access list.
	in	Enter the keyword **in** to apply the ACL to incoming traffic.
	out	Enter the keyword **out** to apply the ACL to outgoing traffic. Only available on 12-port 1-Gigabit Ethernet FLEX line card refer to your line card documentation for specifications. .
	implicit-permit	(OPTIONAL) Enter the keyword **implicit-permit** to change the default action of the ACL from implicit-deny to implicit-permit (that is, if the traffic does not match the filters in the ACL, the traffic is permitted instead of dropped).
	vlan *vlan-id*	(OPTIONAL) Enter the keyword **vlan** followed by the ID numbers of the VLANs. Range: 1 to 4094

Defaults Not enabled.

Command Modes INTERFACE

Usage Information

You can assign one ACL (standard or extended ACL) to an interface.

Note: This command is supported on the loopback interfaces of EE3, and EF series RPMs. This command is not supported on the loopback interfaces ED series RPM.

When you apply an ACL that filters IGMP traffic, all IGMP traffic is redirected to the CPUs and soft-forwarded, if required, in the following scenarios:

- on a Layer 2 interface - if a Layer 3 ACL is applied to the interface.
- on a Layer 3 port or on a Layer 2/Layer 3 port

Related Commands

ip access-list standard	Configure a standard ACL.
ip access-list extended	Configure an extended ACL.

show config

View the current IP ACL configuration.

Syntax **show config**

Command Modes ACCESS-LIST

Example

```
Force10(config-ext-nacl)#show conf
!
ip access-list extended patches
Force10(config-ext-nacl)#
```

Figure 227 show config Command Example

show ip accounting access-list

View the IP access-lists created on the E-Series and the sequence of filters.

Syntax **show ip accounting access-list** *access-list-name* **interface** *interface*

Parameters

access-list-name	Enter the name of the ACL to be displayed.
interface *interface*	Enter the keyword **interface** followed by the interface type and slot/port or number information: • For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For a Port Channel interface, enter the keyword **port-channel** followed by a number: C-Series Range: 1-128 E-Series Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale. • For a SONET interface, enter the keyword **sonet** followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information.

Command Modes

EXEC

EXEC privilege

Example

```
Force10#show ip accounting access FILTER1 interface gig 1/6
Extended IP access list FILTER1
seq 5 deny ip any 191.1.0.0 /16 count (0x00 packets)
seq 10 deny ip any 191.2.0.0 /16 order 4
seq 15 deny ip any 191.3.0.0 /16
seq 20 deny ip any 191.4.0.0 /16
seq 25 deny ip any 191.5.0.0 /16
```

Figure 228 show ip accounting access-lists Command Example (Partial)

Table 46 defines the information in Figure 228.

Table 46 show ip accounting access-lists Command Example Field

Field	Description
“Extended IP ...”	Displays the name of the IP ACL.
“seq 5 ...”	Displays the filter. If the keywords count or byte were configured in the filter, the number of packets or bytes processed by the filter is displayed at the end of the line.
“order 4”	Displays the QoS order of priority for the ACL entry.

Standard MAC ACLs

The following commands configure standard MAC ACLs.

- deny on page 648
- mac access-list standard on page 649
- permit on page 649
- seq on page 650

deny

Configure a filter to drop packets with a the MAC address specified.

Syntax **deny** {**any** | *mac-source-address* [*mac-source-address-mask*]} [**count** [**byte**]] [**log**] [**monitor**]

To remove this filter, you have two choices:

- use the **no seq** *sequence-number* command syntax if you know the filter's sequence number or
- use the **no deny** {**any** | *mac-source-address mac-source-address-mask*} command.

Parameters

any	Enter the keyword **any** to specify that all traffic is subject to the filter.
mac-source-address	Enter a MAC address in nn:nn:nn:nn:nn:nn format.
mac-source-address-mask	(OPTIONAL) Specify which bits in the MAC address must match. If no mask is specified, a mask of 00:00:00:00:00:00 is applied (in other words, the filter allows only MAC addresses that match).
count	(OPTIONAL) Enter the keyword **count** to count packets processed by the filter.
byte	(OPTIONAL) Enter the keyword **byte** to count bytes processed by the filter.
log	(OPTIONAL) Enter the keyword **log** to log the packets.
monitor	(OPTIONAL) Enter the keyword **monitor** to monitor traffic on the monitoring interface specified in the flow-based monitoring session along with the filter operation.

Defaults Not enabled.

Command Modes MAC ACCESS LIST

Command History

Version 7.4.1.0	Added **monitor** option

Note: When ACL logging and byte counters are configured simultaneously, byte counters may display an incorrect value. Configure packet counters with logging instead.

Related Commands

permit	Configure a MAC address filter to pass packets.
seq	Configure a MAC address filter with a specified sequence number.

mac access-list standard

Enter the MAC ACCESS LIST mode to configure a standard MAC Access lists.

Syntax **mac access-list standard** *mac-list-name*

To delete a MAC access list, use the **no mac access-list standard** *mac-list-name* command.

Parameters

mac-list-name	Enter a text string as the name of the standard MAC access list.

Defaults Not configured.

Command Modes CONFIGURATION

Usage Information The number of entries allowed per ACL is hardware-dependent. Refer to your line card documentation for detailed specification on entries allowed per ACL.

Example

```
Force10(conf)#mac-access-list access-list standard zakho
Force10(config-std-macl)#
```

Figure 229 mac-access-list standard Command Example

permit

Configure a filter to forward packets from a specific source MAC address.

Syntax **permit** {**any |** *mac-source-address* [*mac-source-address-mask*]} [**count** [**byte**]] | [**log**] [**monitor**]

To remove this filter, you have two choices:

- use the **no seq** *sequence-number* command syntax if you know the filter's sequence number or
- use the **no permit** {**any** | *mac-source-address mac-source-address-mask*} command.

Parameters

any	Enter the keyword **any** to forward all packets received with a MAC address.
mac-source-address	Enter a MAC address in nn:nn:nn:nn:nn:nn format.

mac-source-address-mask	(OPTIONAL) Specify which bits in the MAC address must match. If no mask is specified, a mask of 00:00:00:00:00:00 is applied (in other words, the filter allows only MAC addresses that match).
count	(OPTIONAL) Enter the keyword **count** to count packets processed by the filter.
byte	(OPTIONAL) Enter the keyword **byte** to count bytes processed by the filter.
log	(OPTIONAL) Enter the keyword **log** to log the packets.
monitor	(OPTIONAL) Enter the keyword **monitor** to monitor traffic on the monitoring interface specified in the flow-based monitoring session along with the filter operation.

Defaults Not configured.

Command Modes MAC ACCESS LIST

Command History

Version 7.4.1.0	Added **monitor** option

Note: When ACL logging and byte counters are configured simultaneously, byte counters may display an incorrect value. Configure packet counters with logging instead.

Related Commands

deny	Configure a MAC ACL filter to drop packets.
seq	Configure a MAC ACL filter with a specified sequence number.

seq

Assign a sequence number to a deny or permit filter in a MAC access list while creating the filter.

Syntax **seq** *sequence-number* {**deny** | **permit**} {**any** | *mac-source-address* [*mac-source-address-mask*]} [**count** [**byte**]] [**log**] [**monitor**]

To remove this filter, use the **no seq** *sequence-number* command.

Parameters

sequence-number	Enter a number between 0 and 65535.
deny	Enter the keyword **deny** to configure a filter to drop packets meeting this condition.
permit	Enter the keyword **permit** to configure a filter to forward packets meeting this criteria.
any	Enter the keyword **any** to filter all packets.

mac-source-address	Enter a MAC address in nn:nn:nn:nn:nn:nn format.
mac-source-address-mask	(OPTIONAL) Specify which bits in the MAC address must match. If no mask is specified, a mask of 00:00:00:00:00:00 is applied (in other words, the filter allows only MAC addresses that match).
count	(OPTIONAL) Enter the keyword **count** to count packets processed by the filter.
byte	(OPTIONAL) Enter the keyword **byte** to count bytes processed by the filter.
log	(OPTIONAL) Enter the keyword **log** to log the packets.
monitor	(OPTIONAL) Enter the keyword **monitor** to monitor traffic on the monitoring interface specified in the flow-based monitoring session along with the filter operation.

Defaults

Not configured.

Command Modes

MAC ACCESS LIST

Command History

Version 7.4.1.0	Added **monitor** option

Note: When ACL logging and byte counters are configured simultaneously, byte counters may display an incorrect value. Configure packet counters with logging instead.

Related Commands

deny	Configure a filter to drop packets.
permit	Configure a filter to forward packets.

Extended MAC ACLs

The following commands configure Extended MAC ACLs.

- deny on page 651
- mac access-list extended on page 653
- permit on page 654
- seq on page 655

deny

Configure a filter to drop packets that match the filter criteria.

Syntax **deny** {**any** | **host** *mac-address* | *mac-source-address mac-source-address-mask*} {**any** | **host** *mac-address* | *mac-destination-address mac-destination-address-mask*} [*ethertype-operator*] [**count** [**byte**]] [**log**] [**monitor**]

To remove this filter, you have two choices:

- use the **no seq** *sequence-number* command syntax if you know the filter's sequence number or
- use the **no deny** {**any** | **host** *mac-address* | *mac-source-address mac-source-address-mask*} {**any** | **host** *mac-address* | *mac-destination-address mac-destination-address-mask*} command.

Parameters

any	Enter the keyword **any** to drop all packets.
host *mac-address*	Enter the keyword **host** followed by a MAC address to drop packets with that host address.
mac-source-address	Enter the source MAC address in nn:nn:nn:nn:nn:nn format.
mac-source-address-mask	Specify which bits in the MAC address must match. The MAC ACL supports an inverse mask, therefore, a mask of ff:ff:ff:ff:ff:ff allows entries that do not match and a mask of 00:00:00:00:00:00 only allows entries that match exactly.
mac-destination-address	Enter the destination MAC address and mask in nn:nn:nn:nn:nn:nn format.
mac-destination-address-mask	Specify which bits in the MAC address must match. The MAC ACL supports an inverse mask, therefore, a mask of ff:ff:ff:ff:ff:ff allows entries that do not match and a mask of 00:00:00:00:00:00 only allows entries that match exactly.
ethertype operator	(OPTIONAL) To filter based on protocol type, enter one of the following Ethertypes: • **ev2** - is the Ethernet II frame format. • **llc** - is the IEEE 802.3 frame format. • **snap** - is the IEEE 802.3 SNAP frame format.
count	(OPTIONAL) Enter the keyword **count** to count packets processed by the filter.
byte	(OPTIONAL) Enter the keyword **byte** to count bytes processed by the filter.
log	(OPTIONAL) Enter the keyword **log** to log the packets.
monitor	(OPTIONAL) Enter the keyword **monitor** to monitor traffic on the monitoring interface specified in the flow-based monitoring session along with the filter operation.

Defaults Not configured.

Command Modes MAC ACCESS LIST

Command History

Version 7.4.1.0	Added **monitor** option

Note: When ACL logging and byte counters are configured simultaneously, byte counters may display an incorrect value. Configure packet counters with logging instead.

Related Commands

permit	Configure a filter to forward based on MAC addresses.
seq	Configure a filter with specific sequence numbers.

mac access-list extended

Enter the MAC ACCESS LIST mode to configure extended MAC access lists.

Syntax **mac access-list extended** *access-list-name*

To delete a MAC access list, use the **no mac access-list extended** *access-list-name* command.

Parameters

access-list-name	Enter a text string as the MAC access list name.

Defaults No default configuration

Command Modes CONFIGURATION

Usage Information The number of entries allowed per ACL is hardware-dependent. Refer to your line card documentation for detailed specification on entries allowed per ACL.

Example

```
Force10(conf)#mac-access-list access-list extended snickers
Force10(config-ext-macl)#
```

Figure 230 mac-access-list extended Command Example

Related Commands

mac access-list standard	Configure a standard MAC access list.

permit

Configure a filter to pass packets matching the criteria specified.

Syntax **permit** {**any** | **host** *mac-address* | *mac-source-address mac-source-address-mask*} {**any** | **host** *mac-address* | *mac-destination-address mac-destination-address-mask*} [*ethertype operator*] [**count** [**byte**]] | [**log**] [**monitor**]

To remove this filter, you have two choices:

- use the **no seq** *sequence-number* command syntax if you know the filter's sequence number or
- use the **no permit** {**any** | **host** *mac-address* | *mac-source-address mac-source-address-mask*} {**any** | *mac-destination-address mac-destination-address-mask*} command.

Parameters

any	Enter the keyword **any** to forward all packets.
host	Enter the keyword **host** followed by a MAC address to forward packets with that host address.
mac-source-address	Enter the source MAC address in nn:nn:nn:nn:nn:nn format.
mac-source-address-mask	Specify which bits in the MAC address must be matched. The MAC ACL supports an inverse mask, therefore, a mask of ff:ff:ff:ff:ff:ff allows entries that do not match and a mask of 00:00:00:00:00:00 only allows entries that match exactly.
mac-destination-address	Enter the destination MAC address and mask in nn:nn:nn:nn:nn:nn format.
mac-destination-address-mask	Specify which bits in the MAC address must be matched. The MAC ACL supports an inverse mask, therefore, a mask of ff:ff:ff:ff:ff:ff allows entries that do not match and a mask of 00:00:00:00:00:00 only allows entries that match exactly.
ethertype operator	(OPTIONAL) To filter based on protocol type, enter one of the following Ethertypes: • **ev2** - is the Ethernet II frame format. • **llc** - is the IEEE 802.3 frame format. • **snap** - is the IEEE 802.3 SNAP frame format.
count	(OPTIONAL) Enter the keyword **count** to count packets processed by the filter.
byte	(OPTIONAL) Enter the keyword **byte** to count bytes processed by the filter.
log	(OPTIONAL) Enter the keyword **log** to log the packets.
monitor	(OPTIONAL) Enter the keyword **monitor** to monitor traffic on the monitoring interface specified in the flow-based monitoring session along with the filter operation.

Defaults Not configured.

Command Modes MAC ACCESS LIST

Command History

Version 7.4.1.0	Added **monitor** option

Note: When ACL logging and byte counters are configured simultaneously, byte counters may display an incorrect value. Configure packet counters with logging instead.

Related Commands

deny	Configure a filter to drop traffic based on the MAC address.
seq	Configure a filter with specific sequence numbers.

seq

Configure a filter with a specific sequence number.

Syntax **seq** *sequence-number* {**deny** | **permit**} {**any** | **host** *mac-address* | *mac-source-address mac-source-address-mask*} {**any** | **host** *mac-address* | *mac-destination-address mac-destination-address-mask*} [*ethertype operator*] [**count** [**byte**]] [**log**] [**monitor**]

To delete a filter, use the **no seq** *sequence-number* command.

Parameters

sequence-number	Enter a number as the filter sequence number. Range: zero (0) to 65535.
deny	Enter the keyword **deny** to drop any traffic matching this filter.
permit	Enter the keyword **permit** to forward any traffic matching this filter.
any	Enter the keyword **any** to filter all packets.
host *mac-address*	Enter the keyword **host** followed by a MAC address to filter packets with that host address.
mac-source-address	Enter the source MAC address in nn:nn:nn:nn:nn:nn format. The MAC ACL supports an inverse mask, therefore, a mask of ff:ff:ff:ff:ff:ff allows entries that do not match and a mask of 00:00:00:00:00:00 only allows entries that match exactly.
mac-source-address-mask	Specify which bits in the MAC address must be matched.
mac-destination-address	Enter the destination MAC address and mask in nn:nn:nn:nn:nn:nn format.

mac-destination-address-mask	Specify which bits in the MAC address must be matched. The MAC ACL supports an inverse mask, therefore, a mask of ff:ff:ff:ff:ff:ff allows entries that do not match and a mask of 00:00:00:00:00:00 only allows entries that match exactly.
ethertype operator	(OPTIONAL) To filter based on protocol type, enter one of the following Ethertypes: • **ev2** - is the Ethernet II frame format. • **llc** - is the IEEE 802.3 frame format. • **snap** - is the IEEE 802.3 SNAP frame format.
count	(OPTIONAL) Enter the keyword **count** to count packets processed by the filter.
byte	(OPTIONAL) Enter the keyword **byte** to count bytes processed by the filter.
log	(OPTIONAL) Enter the keyword **log** to log the packets.
monitor	(OPTIONAL) Enter the keyword **monitor** to monitor traffic on the monitoring interface specified in the flow-based monitoring session along with the filter operation.

Defaults

Not configured.

Command Modes

MAC ACCESS LIST

Command History

Version 7.4.1.0	Added **monitor** option

Note: When ACL logging and byte counters are configured simultaneously, byte counters may display an incorrect value. Configure packet counters with logging instead.

Related Commands

deny	Configure a filter to drop traffic.
permit	Configure a filter to forward traffic.

Common MAC Access List Commands

The following commands allow you to clear, view and assign MAC ACL configurations.

- clear counters mac access-group on page 657
- mac access-group on page 657
- show mac accounting access-list on page 658

clear counters mac access-group

Clear counters for all or a specific MAC ACL.

Syntax **clear counters mac access-group** [*mac-list-name*]

Parameters		
	mac-list-name	(OPTIONAL) Enter the name of a configured MAC access list.

Command Modes EXEC privilege

mac access-group

Apply a MAC ACL to traffic entering or exiting an interface.

Syntax **mac access-group** *access-list-name* {**in** [**vlan** *vlan-range*] | **out**}

To delete a MAC access-group, use the **no mac access-group** *mac-list-name* command.

Parameters		
	access-list-name	Enter the name of a configured MAC access list.
	vlan *vlan-range*	(OPTIONAL) Enter the keyword **vlan** followed a range of VLANs. Note that this option is available only with the **in** keyword option. Range: 1 to 4094
	in	Enter the keyword **in** to configure the ACL to filter incoming traffic.
	out	Enter the keyword **out** to configure the ACL to filter outgoing traffic.

Defaults No default behavior or configuration

Command Modes INTERFACE

Usage Information You can assign one ACL (standard or extended) to an interface.

Related Commands		
	mac access-list standard	Configure a standard MAC ACL.
	mac access-list extended	Configure an extended MAC ACL.

show mac accounting access-list

View MAC access list configurations and counters (if configured).

Syntax **show mac accounting access-list** *access-list-name* **interface** *interface*

Parameters

access-list-name	Enter the name of a configured MAC access list.
interface *interface*	Enter the keyword interface followed by the following keywords and slot/port or number information: • For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For a Port Channel interface, enter the keyword **port-channel** followed by a number: C-Series Range: 1-128 E-Series Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale. • For a SONET interface, enter the keyword **sonet** followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEtherne**t followed by the slot/port information.

Command Modes EXEC

EXEC privilege

Example

```
Force10#show mac accounting access-list mac-ext interface po 1
Extended mac access-list mac-ext on GigabitEthernet 0/11
 seq 5  permit host  00:00:00:00:00:11 host  00:00:00:00:00:19  count (393794576  packets)
 seq 10  deny host  00:00:00:00:00:21 host  00:00:00:00:00:29  count (89076777 packets)
 seq 15  deny host  00:00:00:00:00:31 host  00:00:00:00:00:39  count (0 packets)
 seq 20  deny host  00:00:00:00:00:41 host  00:00:00:00:00:49  count (0 packets)
 seq 25  permit any any  count (0 packets)
Extended mac access-list mac-ext on GigabitEthernet 0/12
 seq 5  permit host  00:00:00:00:00:11 host  00:00:00:00:00:19  count (57589834 packets)
 seq 10  deny host  00:00:00:00:00:21 host  00:00:00:00:00:29  count (393143077 packets)
 seq 15  deny host  00:00:00:00:00:31 host  00:00:00:00:00:39  count (0 packets)
 seq 20  deny host  00:00:00:00:00:41 host  00:00:00:00:00:49  count (0 packets)
 seq 25  permit any any  count (0 packets)
Force10#
```

Figure 231 show mac accounting access-list Command Example

IP Prefix List Commands

Use these commands to configure or enable IP prefix lists.

- clear ip prefix-list on page 659
- deny on page 659
- ip prefix-list on page 660
- permit on page 660

- seq on page 661
- show config on page 662
- show ip prefix-list detail on page 662
- show ip prefix-list summary on page 663

clear ip prefix-list

Reset the number of times traffic met the conditions (“hit” counters) of the configured prefix lists.

Syntax **clear ip prefix-list** [*prefix-name*]

Parameters

prefix-name	(OPTIONAL) Enter the name of the configured prefix list to clear only counters for that prefix list.

Command Modes EXEC privilege

Default Clears “hit” counters for all prefix lists unless a prefix list is specified.

Related Commands

ip prefix-list	Configure a prefix list.

deny

Configure a filter to drop packets meeting the criteria specified.

Syntax **deny** *ip-prefix* [**ge** *min-prefix-length*] [**le** *max-prefix-length*]

To delete a drop filter, use the **no deny** *ip-prefix* command.

Parameters

ip-prefix	Specify an IP prefix in the network/length format. For example, 35.0.0.0/8 means match the first 8 bits of address 35.0.0.0.
ge *min-prefix-length*	(OPTIONAL) Enter the keyword **ge** followed by the minimum prefix length, which is a number from zero (0) to 32.
le *max-prefix-length*	(OPTIONAL) Enter the keyword **le** followed by the maximum prefix length, which is a number from zero (0) to 32.

Defaults Not configured.

Command Modes PREFIX-LIST

Usage Information Sequence numbers for this filter are automatically assigned starting at sequence number 5.

If the options **ge** or **le** are not used, only packets with an exact match to the prefix are filtered.

Related Commands

permit	Configure a filter to pass packets.
seq	Configure a drop or permit filter with a specified sequence number.

ip prefix-list

Enter the PREFIX-LIST mode and configure a prefix list.

Syntax **ip prefix-list** *prefix-name*

To delete a prefix list, use the **no ip prefix-list** *prefix-name* command.

Parameters

prefix-name	Enter a string up to 16 characters long as the name of the prefix list.

Command Modes CONFIGURATION

Usage Information Prefix lists redistribute OSPF and RIP routes meeting specific criteria.

permit

Configure a filter that passes packets meeting the criteria specified.

Syntax **permit** *ip-prefix* [**ge** *min-prefix-length*] [**le** *max-prefix-length*]

To delete a forward filter, use the **no permit** *ip-prefix* command.

Parameters

ip-prefix	Specify an IP prefix in the network/length format. For example, 35.0.0.0/8 means match the first 8 bits of address 35.0.0.0.

ge *min-prefix-length*	(OPTIONAL) Enter the keyword **ge** followed by the minimum prefix length, which is a number from zero (0) to 32.
le *max-prefix-length*	(OPTIONAL) Enter the keyword **le** followed by the maximum prefix length, which is a number from zero (0) to 32.

Command Modes PREFIX-LIST

Usage Information Sequence numbers for this filter are automatically assigned starting at sequence number 5.

If the options **ge** or **le** are not used, only packets with an exact match to the prefix are filtered.

Related Commands

deny	Configure a filter to drop packets.
seq	Configure a drop or permit filter with a specified sequence number.

seq

Assign a sequence number to a deny or permit filter in a prefix list while configuring the filter.

Syntax **seq** *sequence-number* {**deny** | **permit**} {**any**} | [*ip-prefix /nn* {**ge** *min-prefix-length*} {**le** *max-prefix-length* }] | [**bitmask** *number*]

To delete a specific filter, use the **no seq** *sequence-number* {**deny** | **permit**} {**any**} | [*ip-prefix* {**ge** *min-prefix-length*} {**le** *max-prefix-length* }] | [**bitmask** *number*].

Parameters

sequence-number	Enter a number. Range: 1 to 4294967294.
deny	Enter the keyword **deny** to configure a filter to drop packets meeting this condition.
permit	Enter the keyword **permit** to configure a filter to forward packets meeting this condition.
any	(OPTIONAL) Enter the keyword **any** to match any packets.
ip-prefix /nn	(OPTIONAL) Specify an IP prefix in the network/length format. For example, 35.0.0.0/8 means match the first 8 bits of address 35.0.0.0.
ge *min-prefix-length*	(OPTIONAL) Enter the keyword **ge** followed by the minimum prefix length, which is a number from zero (0) to 32.
le *max-prefix-length*	(OPTIONAL) Enter the keyword **le** followed by the maximum prefix length, which is a number from zero (0) to 32.
bitmask *number*	Enter the keyword **bitmask** followed by a bitmask number in dotted decimal format.

Defaults Not configured.

Command Modes PREFIX-LIST

Command History

Version 6.3.1.0	Added bitmask option

Usage Information If the options **ge** or **le** are not used, only packets with an exact match to the prefix are filtered.

Related Commands

deny	Configure a filter to drop packets.
permit	Configure a filter to pass packets.

show config

View the current PREFIX-LIST configurations.

Syntax **show config**

Command Modes PREFIX-LIST

Example

```
Force10(conf-nprefixl)#show config
!
ip prefix-list snickers
Force10(conf-nprefixl)#
```

Figure 232 show config Command Example

show ip prefix-list detail

View details of the configured prefix lists.

Syntax **show ip prefix-list detail** [*prefix-name*]

Parameters

prefix-name	(OPTIONAL) Enter a text string as the name of the prefix list.

Command Modes EXEC

EXEC privilege

Example

```
Force10#show ip prefix-list detail
Prefix-list with the last deletion/insertion: filter_ospf
ip prefix-list filter_in:
count: 3, range entries: 3, sequences: 5 - 10
   seq 5 deny 1.102.0.0/16 le 32 (hit count: 0)
   seq 6 deny 2.1.0.0/16 ge 23 (hit count: 0)
   seq 10 permit 0.0.0.0/0 le 32 (hit count: 0)
ip prefix-list filter_ospf:
count: 4, range entries: 1, sequences: 5 - 10
   seq 5 deny 100.100.1.0/24 (hit count: 5)
   seq 6 deny 200.200.1.0/24 (hit count: 1)
   seq 7 deny 200.200.2.0/24 (hit count: 1)
   seq 10 permit 0.0.0.0/0 le 32 (hit count: 132)
Force10#
```

Figure 233 show ip prefix-list detail Command Example

show ip prefix-list summary

View a summary of the configured prefix lists.

Syntax **show ip prefix-list summary** [*prefix-name*]

Parameters

prefix-name	(OPTIONAL) Enter a text string as the name of the prefix list.

Command Modes EXEC

EXEC privilege

Example

```
Force10#show ip prefix summ
Prefix-list with the last deletion/insertion: test
ip prefix-list test:
count: 3, range entries: 1, sequences: 5 - 15
ip prefix-list test1:
count: 2, range entries: 2, sequences: 5 - 10
ip prefix-list test2:
count: 1, range entries: 1, sequences: 5 - 5
ip prefix-list test3:
count: 1, range entries: 1, sequences: 5 - 5
ip prefix-list test4:
count: 1, range entries: 1, sequences: 5 - 5
ip prefix-list test5:
count: 1, range entries: 1, sequences: 5 - 5
ip prefix-list test6:
count: 1, range entries: 1, sequences: 5 - 5
Force10#
```

Figure 234 show ip prefix-list summary Command Example

Route Map Commands

The following commands allow you to configure route maps and their redistribution criteria.

- continue on page 664
- match as-path on page 666
- match community on page 666
- match interface on page 667
- match ip address on page 667
- match ip next-hop on page 668
- match ip route-source on page 669
- match metric on page 669
- match origin on page 670
- match route-type on page 670
- match tag on page 671
- route-map on page 672
- set as-path on page 673
- set automatic-tag on page 673
- set comm-list delete on page 674
- set community on page 675
- set level on page 676
- set local-preference on page 676
- set metric on page 677
- set metric-type on page 677
- set next-hop on page 678
- set origin on page 679
- set tag on page 679
- set weight on page 680
- show config on page 680
- show route-map on page 681

continue

Configure a route-map to go to a route-map entry with a higher sequence number.

Syntax **continue** [*sequence-number*]

To remove the continue clause, use the **no continue** [*sequence-number*] command.

Parameters

sequence-number	(OPTIONAL) Enter the route map sequence number. Range: 1 - 65535 Default: no sequence number

Defaults

Not Configured

Command Modes

ROUTE-MAP

Command History

Version 7.4.1.0	Introduced

Usage Information

The **continue** feature allows movement from one route-map entry to a specific route-map entry (the **sequence number**). If the sequence number is not specified, the **continue** feature simply moves to the next sequence number (also known as an implied continue). If a match clause exists, the **continue** feature executes only after a successful match occurs. If there are no successful matches, **continue** is ignored.

Match clause with Continue clause

In addition, the **continue** feature can exist without a match clause. The continue clause without a match clause executes and jumps to the specified route-map entry.

With a match clause and a continue clause, the match clause executes first and the continue clause next in a specified route map entry. The continue clause launches only after a successful match. The behavior is:

- A successful match with a continue clause—the route map executes the set clauses and then goes to the specified route map entry upon execution of the continue clause.
- If the next route map entry contains a continue clause, the route map will execute the continue clause if a successful match occurs.
- If the next route map entry does not contain a continue clause, the route map evaluates normally. If a match does not does not occur, the route map does not continue and will fall through to the next sequence number, if one exists.

Set clause with Continue clause

If the route-map entry contains sets with the continue clause, then set actions is performed first followed by the continue clause jump to the specified route map entry.

- If a set actions occurs in the first route map entry and then the same set action occurs with a different value in a subsequent route map entry, the last set of actions overrides the previous set of actions with the same **set** command.
- If **set community additive** and **set as-path prepend** are configure, the communities and AS numbers are pre-pended.

Related Commands

set community	Specify a COMMUNITY attribute
set as-path	Configure a filter to modify the AS path

match as-path

Configure a filter to match routes that have a certain AS number in their BGP path.

Syntax **match as-path** *as-path-name*

To delete a match AS path filter, use the **no match as-path** *as-path-name* command.

Parameters

as-path-name	Enter the name of an established AS-PATH ACL.

Defaults Not configured.

Command Modes ROUTE-MAP

Related Commands

set as-path	Add information to the BGP AS_PATH attribute.

match community

Configure a filter to match routes that have a certain COMMUNITY attribute in their BGP path.

Syntax **match community** *community-list-name* [**exact**]

To delete a community match filter, use the **no match community** command.

Parameters

community-list-name	Enter the name of a configured community list.
exact	(OPTIONAL) Enter the keywords **exact** to process only those routes with this community list name.

Defaults Not configured.

Command Modes ROUTE-MAP

Related Commands

ip community-list	Configure an Community Access list.
set community	Specify a COMMUNITY attribute.
neighbor send-community	Send COMMUNITY attribute to peer or peer group.

match interface

Configure a filter to match routes whose next hop is on the interface specified.

Syntax **match interface** *interface*

To remove a match, use the **no match interface** *interface* command.

Parameters

interface	Enter the following keywords and slot/port or number information: • For a Fast Ethernet interface, enter the keyword **FastEthernet** followed by the slot/port information. • For a Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For the loopback interface, enter the keyword **loopback** followed by a number from zero (0) to 16383. • For a Port Channel interface, enter the keyword **port-channel** followed by a number: C-Series Range: 1-128 E-Series Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale. • For a SONET interface, enter the keyword **sonet** followed by the slot/port information. • For a Ten Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information. • For a VLAN, enter the keyword vlan followed by a number from 1 to 4094.

Defaults Not configured.

Command Modes ROUTE-MAP

Related Commands

match ip address	Redistribute routes that match an IP address.
match ip next-hop	Redistribute routes that match the next-hop IP address.
match ip route-source	Redistribute routes that match routes advertised by other routers.
match metric	Redistribute routes that match a specific metric.
match route-type	Redistribute routes that match a route type.
match tag	Redistribute routes that match a specific tag.

match ip address

Configure a filter to match routes based on IP addresses specified in an access list.

Syntax **match ip address** *prefix-list-name*

To delete a match, use the **no match ip address** *prefix-list-name* command.

Parameters		
	prefix-list-name	Enter the name of configured prefix list.

Defaults Not configured.

Command Modes ROUTE-MAP

Related Commands		
	match interface	Redistribute routes that match the next-hop interface.
	match ip next-hop	Redistribute routes that match the next-hop IP address.
	match ip route-source	Redistribute routes that match routes advertised by other routers.
	match metric	Redistribute routes that match a specific metric.
	match route-type	Redistribute routes that match a route type.
	match tag	Redistribute routes that match a specific tag.

match ip next-hop

Configure a filter to match based on the next-hop IP addresses specified in an IP access list or IP prefix list.

Syntax **match ip next-hop** {*access-list* | **prefix-list** *prefix-list-name*}

To delete a match, use the **no match ip next-hop** {*access-list-name* | **prefix-list** *prefix-list-name*} command.

Parameters		
	access-list-name	Enter the name of a configured IP access list.
	prefix-list *prefix-list-name*	Enter the keywords **prefix-list** followed by the name of configured prefix list.

Defaults Not configured.

Command Modes ROUTE-MAP

Related Commands		
	match interface	Redistribute routes that match the next-hop interface.
	match ip address	Redistribute routes that match an IP address.
	match ip route-source	Redistribute routes that match routes advertised by other routers.
	match metric	Redistribute routes that match a specific metric.
	match route-type	Redistribute routes that match a route type.
	match tag	Redistribute routes that match a specific tag.

match ip route-source

Configure a filter to match based on the routes advertised by routes specified in IP access lists or IP prefix lists.

Syntax **match ip route-source** {*access-list* | **prefix-list** *prefix-list-name*}

To delete a match, use the **no match ip route-source** {*access-list* | **prefix-list** *prefix-list-name*} command.

Parameters

access-list-name	Enter the name of a configured IP access list.
prefix-list *prefix-list-name*	Enter the keywords **prefix-list** followed by the name of configured prefix list.

Defaults Not configured.

Command Modes ROUTE-MAP

Related Commands

match interface	Redistribute routes that match the next-hop interface.
match ip address	Redistribute routes that match an IP address.
match ip next-hop	Redistribute routes that match the next-hop IP address.
match metric	Redistribute routes that match a specific metric.
match route-type	Redistribute routes that match a route type.
match tag	Redistribute routes that match a specific tag.

match metric

Configure a filter to match on a specified value.

Syntax **match metric** *metric-value*

To delete a value, use the **no match metric** [*metric-value*] command.

Parameters

metric-value	Enter a value to match. Range: zero (0) to 4294967295.

Defaults Not configured.

Command Modes ROUTE-MAP

Related Commands

match interface	Redistribute routes that match the next-hop interface.
match ip address	Redistribute routes that match an IP address.
match ip next-hop	Redistribute routes that match the next-hop IP address.
match ip route-source	Redistribute routes that match routes advertised by other routers.
match route-type	Redistribute routes that match a route type.
match tag	Redistribute routes that match a specific tag.

match origin

Configure a filter to match routes based on the value found in the BGP path ORIGIN attribute.

Syntax **match origin** {**egp** | **igp** | **incomplete**}

To disable matching filter, use the **no match origin** {**igp** | **egp** | **incomplete**} command.

Parameters

egp	Enter the keyword **egp** to match routes originating outside the AS.
igp	Enter the keyword **igp** to match routes originating within the same AS.
incomplete	Enter the keyword **incomplete** to match routes with incomplete routing information.

Defaults Not configured.

Command Modes ROUTE-MAP

match route-type

Configure a filter to match routes based on the how the route is defined.

Syntax **match route-type** {**external** [**type-1** | **type-2**] | **internal** | **level-1** | **level-2** | **local**}

To delete a match, use the **no match route-type** {**local** | **internal** | **external** [**type-1** | **type-2**] | **level-1** | **level-2**} command.

Parameters

external [**type-1**| **type-2**]	Enter the keyword **external** followed by either **type-1** or **type-2** to match only on OSPF Type 1 routes or OSPF Type 2 routes.
internal	Enter the keyword **internal** to match only on routes generated within OSPF areas.
level-1	Enter the keyword **level-1** to match IS-IS Level 1 routes.
level-2	Enter the keyword **level-2** to match IS-IS Level 2 routes.
local	Enter the keyword **local** to match only on routes generated within the E-Series.

Defaults Not configured.

Command Modes ROUTE-MAP

Related Commands

match interface	Redistribute routes that match the next-hop interface.
match ip address	Redistribute routes that match an IP address.
match ip next-hop	Redistribute routes that match the next-hop IP address.
match ip route-source	Redistribute routes that match routes advertised by other routers.
match metric	Redistribute routes that match a specific metric.
match tag	Redistribute routes that match a tag.

match tag

Configure a filter to redistribute only routes that match a specified tag value.

Syntax **match tag** *tag-value*

To remove a match, use the **no match tag** command.

Parameters

tag-value	Enter a value as the tag on which to match. Range: zero (0) to 4294967295.

Defaults Not configured.

Command Modes ROUTE-MAP

Related Commands

match interface	Redistribute routes that match the next-hop interface.
match ip address	Redistribute routes that match an IP address.
match ip next-hop	Redistribute routes that match the next-hop IP address.
match ip route-source	Redistribute routes that match routes advertised by other routers.

match metric	Redistribute routes that match a specific metric.
match route-type	Redistribute routes that match a route type.

route-map

Enable a route map statement and configure its action and sequence number. This command also places you in the ROUTE-MAP mode.

Syntax

route-map *map-name* [**permit** | **deny**] [*sequence-number*]

To delete a route map, use the **no route-map** *map-name* [**permit** | **deny**] [*sequence-number*] command.

Parameters

map-name	Enter a text string to name the route map for easy identification.
permit	(OPTIONAL) Enter the keyword **permit** to set the route map default as permit. If no keyword is specified, the default is **permit**.
deny	(OPTIONAL) Enter the keyword **deny** to set the route map default as deny.
sequence-number	(OPTIONAL) Enter a number to identify the route map for editing and sequencing with other route maps. You are prompted for a sequence number if there are multiple instances of the route map. Range: 1 to 65535.

Defaults

Not configured.

If no keyword (**permit** or **deny**) is defined for the route map, the **permit** action is the default.

Command Modes

CONFIGURATION

Example

```
Force10(conf)#route-map dempsey
Force10(config-route-map)#
```

Figure 235 route-map Command Example

Usage Information

Use caution when you delete route maps because if you do not specify a sequence number, all route maps with the same *map-name* are deleted when you use **no route-map** *map-name* command.

Related Commands		
	show config	View the current configuration.

set as-path

Configure a filter to modify the AS path for BGP routes.

Syntax **set as-path prepend** *as-number* [... *as-number*]

To remove an AS-Path setting, use the **no set as-path** {**prepend** *as-number* | **tag**} command.

Parameters		
	prepend *as-number*	Enter the keyword **prepend** followed by up to eight AS numbers to be inserted into the BGP path information. Range: 1 to 65535

Defaults Not configured.

Command Modes ROUTE-MAP

Usage Information You can prepend up to eight AS numbers to a BGP route.

This command influences best path selection in BGP by inserting a tag or AS number into the AS_PATH attribute.

Related Commands		
	match as-path	Redistribute routes that match an AS-PATH attribute.
	ip as-path access-list	Configure an AS-PATH access list.
	neighbor filter-list	Configure a BGP filter based on the AS-PATH attribute.
	show ip community-lists	View configured IP Community access lists.

set automatic-tag

Configure a filter to automatically compute the tag value of the route.

Syntax **set automatic-tag**

To return to the default, enter **no set automatic-tag**.

Defaults Not configured.

Command Modes ROUTE-MAP

Related Commands

set level	Specify the OSPF area for route redistribution.
set metric	Specify the metric value assigned to redistributed routes.
set metric-type	Specify the metric type assigned to redistributed routes.
set tag	Specify the tag assigned to redistributed routes.

set comm-list delete

Configure a filter to remove the specified community list from the BGP route's COMMUNITY attribute.

Syntax **set comm-list** *community-list-name* **delete**

To insert the community list into the COMMUNITY attribute, use the **no set comm-list** *community-list-name* **delete** command.

Parameters

community-list-name	Enter the name of an established Community list.

Defaults Not configured.

Command Modes ROUTE-MAP

Usage Information The community list used in the **set comm-list delete** command must be configured so that each filter contains only one community. For example, the filter `deny 100:12` is acceptable, but the filter `deny 120:13 140:33` results in an error.

If the **set comm-list delete** command and the **set community** command are configured in the same route map sequence, then the deletion command (**set comm-list delete**) is processed before the insertion command (**set community**).

Related Commands

ip community-list	Configure community access list.
match community	Redistribute routes that match the COMMUNITY attribute.
set community	Specify a COMMUNITY attribute.

set community

Allows you to assign a BGP COMMUNITY attribute.

Syntax

set community {*community-number* | **local-as** | **no-advertise** | **no-export** | **none**} [**additive**]

To delete a BGP COMMUNITY attribute assignment, use the **no set community** {*community-number* | **local-as** | **no-advertise** | **no-export** | **none**} command.

Parameters

community-number	Enter the community number in AA:NN format where AA is the AS number (2 bytes) and NN is a value specific to that autonomous system.
local-AS	Enter the keywords **local-AS** to drop all routes with the COMMUNITY attribute of NO_EXPORT_SUBCONFED. All routes with the NO_EXPORT_SUBCONFED (0xFFFFFF03) community attribute must not be advertised to external BGP peers.
no-advertise	Enter the keywords **no-advertise** to drop all routes containing the well-known community attribute of NO_ADVERTISE. All routes with the NO_ADVERTISE (0xFFFFFF02) community attribute must not be advertised to other BGP peers.
no-export	Enter the keywords **no-export** to drop all routes containing the well-known community attribute of NO_EXPORT. All routes with the NO_EXPORT (0xFFFFFF01) community attribute must not be advertised outside a BGP confederation boundary.
none	Enter the keywords **none** to remove the community attribute from routes meeting the route map criteria.
additive	(OPTIONAL) Enter the keyword **additive** add the communities to already existing communities.

Defaults

Not configured.

Command Modes

ROUTE-MAP

Related Commands

ip community-list	Configure a Community access list.
match community	Redistribute routes that match a BGP COMMUNITY attribute.
neighbor send-community	Assign the COMMUNITY attribute.
show ip bgp community	View BGP community groups.
show ip community-lists	View configured Community access lists.

set level

Configure a filter to specify the IS-IS level or OSPF area to which matched routes are redistributed.

Syntax **set level** {**backbone** | **level-1** | **level-1-2** | **level-2** | **stub-area**}

To remove a set level condition, use the **no set level** {**backbone** | **level-1** | **level-1-2** | **level-2** | **stub-area**} command.

Parameters

backbone	Enter the keyword **backbone** to redistribute matched routes to the OSPF backbone area (area 0.0.0.0).
level-1	Enter the keyword **level-1** to redistribute matched routes to IS-IS Level 1.
level-1-2	Enter the keyword **level-1-2** to redistribute matched routes to IS-IS Level 1 and Level 2.
level-2	Enter the keyword **level-2** to redistribute matched routes to IS-IS Level 2.
stub-area	Enter the keyword **stub** to redistributed matched routes to OSPF stub areas.

Defaults Not configured.

Command Modes ROUTE-MAP

Related Commands

set automatic-tag	Compute the tag value of the route.
set metric	Specify the metric value assigned to redistributed routes.
set metric-type	Specify the metric type assigned to redistributed routes.
set tag	Specify the tag assigned to redistributed routes.

set local-preference

Configure a filter to set the BGP LOCAL_PREF attribute for routers within the local autonomous system.

Syntax **set local-preference** *value*

To delete a BGP LOCAL_PREF attribute, enter **no set local-preference**.

Parameters

value	Enter a number as the LOCAL_PREF attribute value. Range: 0 to 4294967295

Defaults Not configured.

Command Modes ROUTE-MAP

Usage Information The set local-preference command changes the LOCAL_PREF attribute for routes meeting the route map criteria. To change the LOCAL_PREF for all routes, use the bgp default local-preference command.

Related Commands

bgp default local-preference	Change default LOCAL_PREF attribute for all routes.

set metric

Configure a filter to assign a new metric to redistributed routes.

Syntax **set metric** [**+** | **-**] *metric-value*

To delete a setting, enter **no set metric**.

Parameters

+	(OPTIONAL) Enter + to add a metric-value to the redistributed routes.
-	(OPTIONAL) Enter - to subtract a metric-value from the redistributed routes.
metric-value	Enter a number as the new metric value. Range: zero (0) to 4294967295

Defaults Not configured.

Command Modes ROUTE-MAP

Related Commands

set automatic-tag	Compute the tag value of the route.
set level	Specify the OSPF area for route redistribution.
set metric-type	Specify the route type assigned to redistributed routes.
set tag	Specify the tag assigned to redistributed routes.

set metric-type

Configure a filter to assign a new route type for routes redistributed to OSPF.

Syntax **set metric-type** {**internal** | **external** | **type-1** | **type-2**}

To delete a setting, enter **no set metric-type**.

Parameters

internal	Enter the keyword **internal** to assign the Interior Gateway Protocol metric of the next hop as the route's BGP MULTI_EXIT_DES (MED) value.
external	Enter the keyword **external** to assign the IS-IS external metric.
type-1	Enter the keyword **type-1** to assign the OSPF Type 1 metric.
type-2	Enter the keyword **type-2** to assign the OSPF Type 2 metric.

Defaults Not configured.

Command Modes ROUTE-MAP

Related Commands

set automatic-tag	Compute the tag value of the route.
set level	Specify the OSPF area for route redistribution.
set metric	Specify the metric value assigned to redistributed routes.
set tag	Specify the tag assigned to redistributed routes.

set next-hop

Configure a filter to specify an IP address as the next hop.

Syntax **set next-hop** *ip-address*

To delete the setting, use the **no set next-hop** *ip-address* command.

Parameters

ip-address	Specify an IP address in dotted decimal format.

Defaults Not configured.

Command Modes ROUTE-MAP

Usage Information If the set next-hop command is configured, its configuration takes precedence over the neighbor next-hop-self command in the ROUTER BGP mode.

If you configure the set next-hop command with the interface's (either Loopback or physical) IP address, the software declares the route unreachable.

Related Commands

match ip next-hop	Redistribute routes that match the next-hop IP address.
neighbor next-hop-self	Configure the routers as the next hop for a BGP neighbor.

set origin

Configure a filter to manipulate the BGP ORIGIN attribute.

Syntax **set origin** {**igp** | **egp** | **incomplete**}

To delete an ORIGIN attribute setting, enter **no set origin**.

Parameters

egp	Enter the keyword **egp** to set routes originating from outside the local AS.
igp	Enter the keyword **igp** to set routes originating within the same AS.
incomplete	Enter the keyword **incomplete** to set routes with incomplete routing information.

Defaults Not configured.

Command Modes ROUTE-MAP

set tag

Configure a filter to specify a tag for redistributed routes.

Syntax **set tag** *tag-value*

To delete a setting, enter **no set tag**.

Parameters

tag-value	Enter a number as the tag. Range: zero (0) to 4294967295.

Defaults Not configured.

Command Modes ROUTE-MAP

Related Commands

set automatic-tag	Compute the tag value of the route.
set level	Specify the OSPF area for route redistribution.
set metric	Specify the metric value assigned to redistributed routes.
set metric-type	Specify the route type assigned to redistributed routes.

set weight

Configure a filter to add a non-RFC compliant attribute to the BGP route to assist with route selection.

Syntax **set weight** *weight*

To delete a weight specification, use the **no set weight** *weight* command.

Parameters

weight	Enter a number as the weight to be used by the route meeting the route map specification. Routes with a higher weight are preferred when there are multiple routes to the same destination. Range: 0 to 65535 Default: router-originated = 32768; all other routes = 0

Defaults router-originated = 32768; all other routes = 0.

Command Modes ROUTE-MAP

Usage Information If you do not use the set weight command, router-originated paths have a weight attribute of 32768 and all other paths have a weight attribute of zero.

show config

View the current route map configuration.

Syntax **show config**

Command Modes ROUTE-MAP

Example

```
Force10(config-route-map)#show config
!
route-map hopper permit 10
Force10(config-route-map)#
```

Figure 236 show config Command Example

show route-map

View the current route map configurations.

Syntax **show route-map** [*map-name*]

Parameters		
	map-name	(OPTIONAL) Enter the name of a configured route map.

Command Modes EXEC

EXEC privilege

Example

```
Force10#show route-map
route-map firpo, permit, sequence 10
 Match clauses:
 Set clauses:
  tag  34
Force10#
```

Figure 237 show route-map Command Example

Related Commands		
	route-map	Configure a route map.

AS-Path Commands

C-Series	NO
E-Series	✓

Platform Specific Feature: This feature is supported on E-Series only.

Below are the commands to configure AS-Path ACLs.

- deny on page 682
- ip as-path access-list on page 682
- permit on page 683
- show config on page 684
- show ip as-path-access-lists on page 685

deny

C-Series	No
E-Series	✓

Create a filter to drop routes that match the route's AS-PATH attribute. Use regular expressions to identify which routes are affected by the filter.

Syntax

deny *as-regular-expression*

To remove this filter, use the **no deny** *as-regular-expression* command.

Parameters

as-regular-expression	Enter a regular expression to match BGP AS-PATH attributes. Use one or a combination of the following: • . = (period) matches on any single character, including white space • * = (asterisk) matches on sequences in a pattern (zero or more sequences) • + = (plus sign) matches on sequences in a pattern (one or more sequences) • ? = (question mark) matches sequences in a pattern (0 or 1 sequences). **You must enter an escape sequence (CNTL+v) prior to entering the ? regular expression.** • [ ] = (brackets) matches a range of single-character patterns. • ^ = (caret) matches the beginning of the input string. (If the caret is used at the beginning of a sequence or range, it matches on everything BUT the characters specified.) • $ = (dollar sign) matches the end of the output string. • _ = (underscore) matches a comma (,), left brace ({), right brace (}), left parenthesis, right parenthesis, the beginning of the input string, the end of the input string, or a space. • | = (pipe) matches either character.

Defaults

Not configured.

Command Modes

AS-PATH ACL

Usage Information

The regular expression must match part of the ASCII-text in the AS-PATH attribute of the BGP route.

ip as-path access-list

Enter the AS-PATH ACL mode and configure an access control list based on the BGP AS_PATH attribute.

C-Series	No
E-Series	✓

Syntax **ip as-path access-list** *as-path-name*

To delete an AS-PATH ACL, use the **no ip as-path access-list** *as-path-name* command.

Parameters

as-path-name	Enter a text string (can be composed of letters or numbers) as the name.

Defaults Not configured

Command Modes CONFIGURATION

Example

```
Force10(conf)#ip as-path access-list snickers
Force10(config-as-path)#
```

Figure 238 ip as-path access-list Command Example

Usage Information Use the match as-path or neighbor filter-list commands to apply the AS-PATH ACL to BGP routes.

Related Commands

match as-path	Match on routes contain a specific AS-PATH.
neighbor filter-list	Configure filter based on AS-PATH information.

permit

C-Series	No
E-Series	✓

Create a filter to forward BGP routes that match the route's AS-PATH attributes. Use regular expressions to identify which routes are affected by this filter.

Syntax **permit** *as-regular-expression*

To remove this filter, use the **no permit** *as-regular-expression* command.

Parameters	*as-regular-expression*	Enter a regular expression to match BGP AS-PATH attributes. Use one or a combination of the following: • . = (period) matches on any single character, including white space • * = (asterisk) matches on sequences in a pattern (zero or more sequences) • + = (plus sign) matches on sequences in a pattern (one or more sequences) • ? = (question mark) matches sequences in a pattern (0 or 1 sequences). **You must enter an escape sequence (CNTL+v) prior to entering the ? regular expression.** • [] = (brackets) matches a range of single-character patterns. • ^ = (caret) matches the beginning of the input string. (If the caret is used at the beginning of a sequence or range, it matches on everything BUT the characters specified.) • $ = (dollar sign) matches the end of the output string. • _ = (underscore) matches a comma (,), left brace ({), right brace (}), left parenthesis, right parenthesis, the beginning of the input string, the end of the input string, or a space. • | = (pipe) matches either character.

Defaults Not configured.

Command Modes AS-PATH ACL

show config

C-Series	**No**
E-Series	✓

View the current configuration.

Syntax **show config**

Command Mode AS-PATH ACL

Example

```
Force10(config-as-path)#show config
!
ip as-path access-list snickers
 deny .3
Force10(config-as-path)#
```

Figure 239 show config Command Example in AS-PATH ACL mode

show ip as-path-access-lists

C-Series	No
E-Series	✓

View the all AS-PATH access lists configured on the E-Series.

Syntax **show ip as-path-access-lists**

Command Modes EXEC

EXEC privilege

Example

```
Force10#show ip as-path-access-list
ip as-path access-list 1
 permit ^$
 permit ^\(.*\)$
 deny .*
ip as-path access-list 91
 permit ^$
 deny .*
 permit ^\(.*\)$
Force10#
```

Figure 240 show ip as-path-access-lists Command Example

IP Community List Commands

C-Series	NO
E-Series	✓

Platform Specific Feature: IP Community List is supported on E-Series only.

Below are the commands necessary to configure an IP Community List ACL.

- deny on page 686
- ip community-list on page 687
- permit on page 687
- show config on page 688
- show ip community-lists on page 689

deny

C-Series	No
E-Series	✓

Create a filter to drop routes matching a BGP COMMUNITY number.

Syntax

deny {*community-number* | **local-AS** | **no-advertise** | **no-export | quote-regexp** *regular-expressions-list* | **regexp** *regular-expression*}

To delete a description, enter **no deny** {*community-number* | **local-AS** | **no-advertise** | **no-export | quote-regexp** *regular-expressions-list* | **regexp** *regular-expression*}.

Parameters

community-number	Enter the community number in AA:NN format where AA is the AS number (2 bytes) and NN is a value specific to that autonomous system.
local-AS	Enter the keywords **local-AS** to drop all routes with the COMMUNITY attribute of NO_EXPORT_SUBCONFED. All routes with the NO_EXPORT_SUBCONFED (0xFFFFFF03) community attribute must not be advertised to external BGP peers.
no-advertise	Enter the keywords **no-advertise** to drop all routes containing the well-known community attribute of NO_ADVERTISE. All routes with the NO_ADVERTISE (0xFFFFFF02) community attribute must not be advertised to other BGP peers.
no-export	Enter the keywords **no-export** to drop all routes containing the well-known community attribute of NO_EXPORT. All routes with the NO_EXPORT (0xFFFFFF01) community attribute must not be advertised outside a BGP confederation boundary.
regexp *regular-expression*	Enter the keyword **regexp** followed by a regular expression. Use one or a combination of the following: • . = (period) matches on any single character, including white space • * = (asterisk) matches on sequences in a pattern (zero or more sequences) • + = (plus sign) matches on sequences in a pattern (one or more sequences) • ? = (question mark) matches sequences in a pattern (0 or 1 sequences). **You must enter an escape sequence (CNTL+v) prior to entering the ? regular expression.** • [] = (brackets) matches a range of single-character patterns. • ^ = (caret) matches the beginning of the input string. (If the caret is used at the beginning of a sequence or range, it matches on everything BUT the characters specified.) • $ = (dollar sign) matches the end of the output string. • _ = (underscore) matches a comma (,), left brace ({), right brace (}), left parenthesis, right parenthesis, the beginning of the input string, the end of the input string, or a space. • | = (pipe) matches either character.

Defaults

Not configured.

Command Modes

COMMUNITY-LIST

ip community-list

C-Series	No
E-Series	✓

Enter COMMUNITY-LIST mode and create an IP community-list for BGP.

Syntax **ip community-list** *comm-list-name*

To delete a community-list, use the **no ip community-list** *comm-list-name* command.

Parameters

comm-list-name	Enter a text string as the name of the community-list.

Command Modes CONFIGURATION

Example

```
Force10(conf)#ip community-list dilling
Force10(config-community-list)#
```

Figure 241 ip community-list Command Example

permit

C-Series	No
E-Series	✓

Configure a filter to forward routes that match the route's COMMUNITY attribute.

Syntax **permit** {*community-number* | **local-AS** | **no-advertise** | **no-export | quote-regexp** *regular-expressions-list* **| regexp** *regular-expression*}

To remove this filter, use the **no permit** {*community-number* | **local-AS** | **no-advertise** | **no-export | quote-regexp** *regular-expressions-list* **| regexp** *regular-expression*} command.

Parameters

community-number	Enter the community number in AA:NN format where AA is the AS number (2 bytes) and NN is a value specific to that autonomous system.
local-AS	Enter the keywords **local-AS** to drop all routes with the COMMUNITY attribute of NO_EXPORT_SUBCONFED. All routes with the NO_EXPORT_SUBCONFED (0xFFFFFF03) community attribute must not be advertised to external BGP peers.

no-advertise	Enter the keywords **no-advertise** to drop all routes containing the well-known community attribute of NO_ADVERTISE. All routes with the NO_ADVERTISE (0xFFFFFF02) community attribute must not be advertised to other BGP peers.
no-export	Enter the keywords **no-export** to drop all routes containing the well-known community attribute of NO_EXPORT. All routes with the NO_EXPORT (0xFFFFFF01) community attribute must not be advertised outside a BGP confederation boundary.
regexp *regular-expression*	Enter the keyword **regexp** followed by a regular expression. Use one or a combination of the following: • . = (period) matches on any single character, including white space • * = (asterisk) matches on sequences in a pattern (zero or more sequences) • + = (plus sign) matches on sequences in a pattern (one or more sequences) • ? = (question mark) matches sequences in a pattern (0 or 1 sequences). **You must enter an escape sequence (CNTL+v) prior to entering the ? regular expression.** • [] = (brackets) matches a range of single-character patterns. • ^ = (caret) matches the beginning of the input string. (If the caret is used at the beginning of a sequence or range, it matches on everything BUT the characters specified.) • $ = (dollar sign) matches the end of the output string. • _ = (underscore) matches a comma (,), left brace ({), right brace (}), left parenthesis, right parenthesis, the beginning of the input string, the end of the input string, or a space. • | = (pipe) matches either character.

Defaults Not configured.

Command Modes COMMUNITY-LIST

show config

C-Series	No
E-Series	✓

View the non-default information in the current configuration.

Syntax **show config**

Command Mode COMMUNITY-LIST

Example

```
Force10(config-std-community-list)#show config
!
ip community-list standard patches
 deny 45:1
 permit no-export
Force10(config-std-community-list)#
```

Figure 242 show config Command Example in COMMUNITY-LIST mode

show ip community-lists

C-Series	No
E-Series	✓

View configured IP community lists in alphabetic order.

Syntax **show ip community-lists** [*name*]

Parameters

name	(OPTIONAL) Enter the name of the standard or extended IP community list.

Command Modes EXEC

EXEC privilege

Example

```
Force10#show ip community-lists
ip community-list standard 1
 deny 701:20
 deny 702:20
 deny 703:20
 deny 704:20
 deny 705:20
 deny 14551:20
 deny 701:112
 deny 702:112
 deny 703:112
 deny 704:112
 deny 705:112
 deny 14551:112
 deny 701:666
 deny 702:666
 deny 703:666
 deny 704:666
 deny 705:666
 deny 14551:666
Force10#
```

Figure 243 show ip community-lists Command Example

Chapter 27 IPv6 Access Control Lists

Platform Specific Feature: IPv6 Access Control Lists are supported on E-Series only.

FTOS supports IPv6 Extended Access Control Lists (ACLs) and IPv6 Route Maps commands.

- IPv6 Extended ACLs on page 691
- Route Map Commands on page 713

Important Points to Remember

- IPv6 Extended ACLs is a TeraScale only feature (IPv6-ExtACL CAM profile).
- Egress IPv6 ACL and IPv6 ACL on Loopback interface is not supported.
- Reference to an empty ACL will permit any traffic.
- ACLs are not applied to self-originated traffic (e.g. Control Protocol traffic not affected by IPv6 ACL since the routed bit is not set for Control Protocol traffic and for egress ACLs the routed bit must be set)
- The same access list name can be used for both IPv4 and IPv6 ACLs.
- IPv6 ACLs can be applied on physical interface and a logical interface (Port-channel/ VLAN).
- Both IPv4 and IPv6 ACLs can be applied on an interfaces.
- Non-contiguous mask are not supported in source or destination addresses in IPv6 ACL entries.
- Since prefix mask is specified in **/x** format in IPv6 ACLs, inverse mask is not supported.

IPv6 Extended ACLs

The following commands configure IPv6 Extended ACLs:

- clear counters ipv6 access-group on page 692

- deny on page 692
- deny icmp on page 693
- deny tcp on page 695
- deny udp on page 697
- ipv6 access-group on page 699
- ipv6 access-list on page 700
- permit on page 701
- permit icmp on page 701
- permit tcp on page 703
- permit udp on page 705
- remark on page 707
- resequence access-list on page 708
- resequence prefix-list ipv6 on page 708
- seq on page 709
- show config on page 711
- show ipv6 accounting access-list on page 712
- show running-config acl on page 713

clear counters ipv6 access-group

C-Series	No
E-Series	✓

Erase all counters maintained for the IPv6 access lists.

Syntax **clear counters ipv6 access-group** [*access-list-name*]

Parameters

access-list-name	(OPTIONAL) Enter the name of a configured access-list.

Command Modes EXEC

EXEC privilege

deny

Configure a filter that drops IPv6 packets that match the filter criteria.

C-Series	No
E-Series	✓

Syntax **deny** {*ipv6-protocol-number* | **icmp** | **ipv6** | **tcp** | **udp**}

To remove this filter, you have two choices:

- use the **no seq** *sequence-number* command syntax if you know the filter's sequence number or
- use the **no deny** {*ipv6-protocol-number* | **icmp** | **ipv6** | **tcp** | **udp**} command.

Parameters

ip-protocol-number	Enter an IPv6 protocol number. Range: 0 to 255
icmp	Enter the keyword **icmp** to deny Internet Control Message Protocol version 6.
ipv6	Enter the keyword **ipv6** to deny any Internet Protocol version 6.
tcp	Enter the keyword **tcp** to deny the Transmission Control protocol.
udp	Enter the keyword **udp** to deny the User Datagram Protocol.

Defaults Not configured.

Command Modes ACCESS-LIST (conf-ipv6-acl)

deny icmp

C-Series	No
E-Series	✓

Configure a filter to drop all or specific ICMP messages.

Syntax **deny icmp** {*source address mask* | **any** | **host** *ipv6-address*} {*destination address* | **any** | **host** *ipv6-address*} [*message-type*] [**count** [**byte**]] | [**log**] [**monitor**]

To remove this filter, you have two choices:

- use the **no seq** *sequence-number* command syntax if you know the filter's sequence number or
- use the **no deny icmp** {*source address mask* | **any** | **host** *ipv6-address*} {*destination address* | **any** | **host** *ipv6-address*} command.

Parameters

source address	Enter the IPv6 address of the network or host from which the packets were sent in the **x:x:x:x::x** format followed by the prefix length in the **/x** format. Range: /0 to /128 The **::** notation specifies successive hexadecimal fields of zero.
mask	Enter a network mask in /prefix format (**/x**).
any	Enter the keyword **any** to specify that all routes are subject to the filter.
host *ipv6-address*	Enter the keyword **host** followed by the IPv6 address of the host in the **x:x:x:x::x** format. The **::** notation specifies successive hexadecimal fields of zero
destination address	Enter the IPv6 address of the network or host to which the packets are sent in the **x:x:x:x::x** format followed by the prefix length in the **/x** format. Range: /0 to /128 The **::** notation specifies successive hexadecimal fields of zero.
message-type	(OPTIONAL) Enter an ICMP message type, either with the type (and code, if necessary) numbers or with the name of the message type (ICMP message types are listed in Table 47). Range: 0 to 255 for ICMP type; 0 to 255 for ICMP code
count	(OPTIONAL) Enter the keyword **count** to count packets processed by the filter.
byte	(OPTIONAL) Enter the keyword **byte** to count bytes processed by the filter.
log	(OPTIONAL) Enter the keyword **log** to have the information kept in an ACL log file.
monitor	(OPTIONAL) Enter the keyword **monitor** to monitor traffic on the monitoring interface specified in the flow-based monitoring session along with the filter operation.

Defaults

Not configured

Command Modes

ACCESS-LIST (conf-ipv6-acl)

Command History

Version 7.4.1.0	Added **monitor** option

Usage Information

Table 47 lists the keywords displayed in the CLI help and their corresponding ICMP Message Type Name.

Table 47 ICMP Message Type Keywords

Keyword	ICMP Message Type Name
dest-unreachable	Destination unreachable
echo	Echo request (ping)
echo-reply	Echo reply
inverse-nd-na	Inverse neighbor discovery advertisement
inverse-nd-ns	Inverse neighbor discovery solicitation

Table 47 ICMP Message Type Keywords (continued)

Keyword	ICMP Message Type Name
log	Log matches against this entry
mobile-advertisement	Mobile prefix advertisement
mobile-solicitation	Mobile prefix solicitation
mrouter-advertisement	Multicast router advertisement
mrouter-solicitation	Multicast router solicitation
mrouter-termination	Multicast router termination
nd-na	Neighbor advertisement
nd-ns	Neighbor solicitation
packet-too-big	Packet is too big
parameter-problem	Parameter problems
redirect	Neighbor redirect
router-advertisement	Neighbor discovery router advertisement
router-renumbering	All routers renumbering
router-solicitation	Neighbor discovery router solicitation
time-exceeded	All time exceeded

deny tcp

C-Series	No
E-Series	✓

Configure a filter that drops TCP packets that match the filter criteria.

Syntax **deny tcp** {*source address mask* | **any** | **host** *ipv6-address*} [*operator port* [*port*]] {*destination address* | **any** | **host** *ipv6-address*} [*bit*] [*operator port* [*port*]] [**count** [**byte**]] | [**log**] [**monitor**]

To remove this filter, you have two choices:

- use the **no seq** *sequence-number* command syntax if you know the filter's sequence number or
- use the **no deny tcp** {*source address mask* | **any** | **host** *ipv6-address*} {*destination address* | **any** | **host** *ipv6-address*} command.

Parameters

source address	Enter the IPv6 address of the network or host from which the packets were sent in the **x:x:x:x::x** format followed by the prefix length in the **/x** format. Range: /0 to /128 The **::** notation specifies successive hexadecimal fields of zero.
mask	Enter a network mask in /prefix format (**/x**).
any	Enter the keyword **any** to specify that all routes are subject to the filter.
host *ipv6-address*	Enter the keyword **host** followed by the IPv6 address of the host in the **x:x:x:x::x** format. The **::** notation specifies successive hexadecimal fields of zero
operator	(OPTIONAL) Enter one of the following logical operand: • **eq** = equal to • **neq** = not equal to • **gt** = greater than • **lt** = less than • **range** = inclusive range of ports (you must specify two ports for the *port* command parameter.
port port	Enter the application layer port number. Enter two port numbers if using the range logical operand. Range: 0 to 65535. The following list includes some common TCP port numbers: • 23 = Telnet • 20 and 21 = FTP • 25 = SMTP • 169 = SNMP
destination address	Enter the IPv6 address of the network or host to which the packets are sent in the **x:x:x:x::x** format followed by the prefix length in the **/x** format. Range: /0 to /128 The **::** notation specifies successive hexadecimal fields of zero.
bit	Enter a flag or combination of bits: **ack:** acknowledgement field **fin**: finish (no more data from the user) **psh:** push function **rst:** reset the connection **syn:** synchronize sequence numbers **urg:** urgent field
count	(OPTIONAL) Enter the keyword **count** to count packets processed by the filter.
byte	(OPTIONAL) Enter the keyword **byte** to count bytes processed by the filter.
log	(OPTIONAL) Enter the keyword **log** to enter ACL matches in the log. Supported on Jumbo-enabled line cards only.
monitor	(OPTIONAL) Enter the keyword **monitor** to monitor traffic on the monitoring interface specified in the flow-based monitoring session along with the filter operation.

Defaults Not configured.

Command Modes ACCESS-LIST (conf-ipv6-acl)

Command History

Version 7.4.1.0	Added **monitor** option

Usage Information Most ACL rules require one entry in the CAM. However, rules with TCP and UDP port operators (**gt**, **lt**, **range**) may require more than one entry. The range of ports is configured in the CAM based on bitmask boundaries; the space required depends on exactly what ports are included in the range.

For example, an ACL rule with TCP port **range 4000 - 8000** uses 8 entries in the CAM:

```
Rule#       Data             Mask       From  To    #Covered

1     0000111110100000 1111111111100000 4000  4031  32
2     0000111111000000 1111111111000000 4032  4095  64
3     0001000000000000 1111100000000000 4096  6143  2048
4     0001100000000000 1111110000000000 6144  7167  1024
5     0001110000000000 1111111000000000 7168  7679  512
6     0001111000000000 1111111100000000 7680  7935  256
7     0001111100000000 1111111111000000 7936  7999  64
8     0001111101000000 1111111111111111 8000  8000  1

Total Ports: 4001
```

But an ACL rule with TCP port **lt 1023** takes only one entry in the CAM:

```
Rule#       Data             Mask       From  To    #Covered

1     0000000000000000 1111110000000000 0     1023  1024

Total Ports: 1024
```

Related Commands

deny	Assign a filter to deny IP traffic.
deny udp	Assign a filter to deny UDP traffic.

deny udp

C-Series	No
E-Series	✓

Configure a filter to drop UDP packets meeting the filter criteria.

Syntax **deny udp** {*source address mask* | **any** | **host** *ipv6-address*} [*operator port* [*port*]] {*destination address* | **any** | **host** *ipv6-address*} [*operator port* [*port*]] [**count** [**byte**]] | [**log**] [**monitor**]

To remove this filter, you have two choices:

- use the **no seq** *sequence-number* command syntax if you know the filter's sequence number or
- use the **no deny udp** {*source address mask* | **any** | **host** *ipv6-address*} {*destination address* | **any** | **host** *ipv6-address*} command.

Parameters

source address	Enter the IPv6 address of the network or host from which the packets were sent in the **x:x:x:x::x** format followed by the prefix length in the **/x** format. Range: /0 to /128 The **::** notation specifies successive hexadecimal fields of zero.
mask	Enter a network mask in /prefix format (**/x**).
any	Enter the keyword **any** to specify that all routes are subject to the filter.
host *ipv6-address*	Enter the keyword **host** followed by the IPv6 address of the host in the **x:x:x:x::x** format. The **::** notation specifies successive hexadecimal fields of zero
operator	(OPTIONAL) Enter one of the following logical operand: • **eq** = equal to • **neq** = not equal to • **gt** = greater than • **lt** = less than • **range** = inclusive range of ports
port port	(OPTIONAL) Enter the application layer port number. Enter two port numbers if using the **range** logical operand. Range: 0 to 65535
destination address	Enter the IPv6 address of the network or host to which the packets are sent in the **x:x:x:x::x** format followed by the prefix length in the **/x** format. Range: /0 to /128 The **::** notation specifies successive hexadecimal fields of zero.
count	(OPTIONAL) Enter the keyword **count** to count packets processed by the filter.
byte	(OPTIONAL) Enter the keyword **byte** to count bytes processed by the filter.
log	(OPTIONAL) Enter the keyword **log** to enter ACL matches in the log. Supported on Jumbo-enabled line cards only.
monitor	(OPTIONAL) Enter the keyword **monitor** to monitor traffic on the monitoring interface specified in the flow-based monitoring session along with the filter operation.

Defaults

Not configured.

Command Modes

ACCESS-LIST (conf-ipv6-acl)

Command History

Version 7.4.1.0	Added **monitor** option

Usage Information

Most ACL rules require one entry in the CAM. However, rules with TCP and UDP port operators (**gt**, **lt**, **range**) may require more than one entry. The range of ports is configured in the CAM based on bitmask boundaries; the space required depends on exactly what ports are included in the range.

For example, an ACL rule with TCP port **range 4000 - 8000** will use 8 entries in the CAM:

```
Rule#       Data             Mask             From  To    #Covered

1     0000111110100000 1111111111100000 4000  4031  32
2     0000111111000000 1111111111000000 4032  4095  64
3     0001000000000000 1111100000000000 4096  6143  2048
4     0001100000000000 1111110000000000 6144  7167  1024
5     0001110000000000 1111111000000000 7168  7679  512
6     0001111000000000 1111111100000000 7680  7935  256
7     0001111100000000 1111111111000000 7936  7999  64
8     0001111101000000 1111111111111111 8000  8000  1

Total Ports: 4001
```

But an ACL rule with TCP port **lt 1023** takes only one entry in the CAM:

```
Rule#       Data             Mask             From  To    #Covered

1     0000000000000000 1111110000000000 0     1023  1024

Total Ports: 1024
```

Related Commands

deny	Assign a deny filter for IP traffic.
deny tcp	Assign a deny filter for TCP traffic.

ipv6 access-group

C-Series	**No**
E-Series	✓

Assign an IPv6 access-group to an interface.

Syntax

ipv6 access-group *access-list-name* {**in** | **out**} [**implicit-permit**] [**vlan** *range*]

To delete an IPv6 access-group configuration, use the **no ipv6 access-group** *access-list-name* {**in**} [**implicit-permit**] [**vlan** *range*] command.

Parameters

access-list-name	Enter the name of a configured access list.
in | **out**	Enter either the keyword **in** or **out** to apply the IPv6 ACL to incoming traffic (ingress) or outgoing traffic (egress).

implicit-permit	(OPTIONAL) Enter the keyword **implicit-permit** to change the default action of the IPv6 ACL from implicit-deny to implicit-permit (that is, if the traffic does not match the filters in the IPv6 ACL, the traffic is permitted instead of dropped).
vlan *range*	(OPTIONAL) Enter the keyword **vlan** followed by the VLAN range in a comma separated format. Range: 1 to 4094

efaults Disabled

Command Modes INTERFACE

Usage Information You can assign an IPv6 access group to a physical, LAG, or VLAN interface context.

Example

```
Force10(conf-if-gi-9/0)#ipv6 access-group AclList1 in implicit-permit vlan 10-20

Force10(conf-if-gi-9/0)#show config
!
interface GigabitEthernet 9/0
 no ip address
 ipv6 access-group AclList1 in implicit-permit Vlan 10-20
 no shutdown
Force10conf-if-gi-9/0)#
```

Figure 244 ipv6 access-group Command Example

ipv6 access-list

C-Series	No
E-Series	✓

Configure an access list based on IPv6 addresses or protocols.

Syntax **ipv6 access-list** *access-list-name*

To delete an access list, use the **no ipv6 access-list** *access-list-name* command.

access-list-name	Enter a string of up to 16 characters long as the access list name.

Parameters

Defaults All access lists contain an implicit “deny any”; that is, if no match occurs, the packet is dropped.

Command Modes CONFIGURATION

Usage Information The number of entries allowed per ACL is hardware-dependent. Refer to your line card documentation for detailed specification on entries allowed per ACL.

Related Commands		
	show config	View the current configuration.

permit

C-Series	No
E-Series	✓

Select an IPv6 protocol number, ICMP, IPv6, TCP, or UDP to configure a filter that match the filter criteria.

Syntax **permit** {*ipv6-protocol-number* | **icmp** | **ipv6** | **tcp** | **udp**}

To remove this filter, you have two choices:

- use the **no seq** *sequence-number* command syntax if you know the filter's sequence number or
- use the **no permit** {*ipv6-protocol-number* | **icmp** | **ipv6** | **tcp** | **udp**} command.

Parameters

ip-protocol-number	Enter an IPv6 protocol number. Range: 0 to 255
icmp	Enter the keyword **icmp** to filter Internet Control Message Protocol version 6.
ipv6	Enter the keyword **ipv6** to filter any Internet Protocol version 6.
tcp	Enter the keyword **tcp** to filter the Transmission Control protocol.
udp	Enter the keyword **udp** to filter the User Datagram Protocol.

Defaults Not configured.

Command Modes ACCESS-LIST

permit icmp

C-Series	No
E-Series	✓

Configure a filter to allow all or specific ICMP messages.

Syntax **permit icmp** {*source address mask* | **any** | **host** *ipv6-address*} {*destination address* | **any** | **host** *ipv6-address*} [*message-type*] [**count** [**byte**]] | [**log**] [**monitor**]

To remove this filter, you have two choices:

- use the **no seq** *sequence-number* command syntax if you know the filter's sequence number or
- use the **no permit icmp** {*source address mask* | **any** | **host** *ipv6-address*} {*destination address* | **any** | **host** *ipv6-address*} command.

Parameters

source address	Enter the IPv6 address of the network or host from which the packets were sent in the **x:x:x:x::x** format followed by the prefix length in the **/x** format. Range: /0 to /128 The **::** notation specifies successive hexadecimal fields of zero.
mask	Enter a network mask in /prefix format (**/x**).
any	Enter the keyword **any** to specify that all routes are subject to the filter.
host *ipv6-address*	Enter the keyword **host** followed by the IPv6 address of the host in the **x:x:x:x::x** format. The **::** notation specifies successive hexadecimal fields of zero
destination address	Enter the IPv6 address of the network or host to which the packets are sent in the **x:x:x:x::x** format followed by the prefix length in the **/x** format. Range: /0 to /128 The **::** notation specifies successive hexadecimal fields of zero.
message-type	(OPTIONAL) Enter an ICMP message type, either with the type (and code, if necessary) numbers or with the name of the message type (ICMP message types are listed in Table 47). Range: 0 to 255 for ICMP type; 0 to 255 for ICMP code
count	(OPTIONAL) Enter the keyword **count** to count packets processed by the filter.
byte	(OPTIONAL) Enter the keyword **byte** to count bytes processed by the filter.
log	(OPTIONAL) Enter the keyword **log** to have the information kept in an ACL log file.
monitor	(OPTIONAL) Enter the keyword **monitor** to monitor traffic on the monitoring interface specified in the flow-based monitoring session along with the filter operation.

Defaults

Not configured

Command Modes

ACCESS-LIST (conf-ipv6-acl)

Command History

Version 7.4.1.0	Added **monitor** option

permit tcp

C-Series	No
E-Series	✓

Configure a filter to pass TCP packets that match the filter criteria.

Syntax

permit tcp {*source address mask* | **any** | **host** *ipv6-address*} [*operator port* [*port*]] {*destination address* | **any** | **host** *ipv6-address*} [*bit*] [*operator port* [*port*]] [**count** [**byte**]] | [**log**] [**monitor**]

To remove this filter, you have two choices:

- use the **no seq** *sequence-number* command syntax if you know the filter's sequence number or
- use the **no permit tcp** {*source address mask* | **any** | **host** *ipv6-address*} {*destination address* | **any** | **host** *ipv6-address*} command.

Parameters

source address	Enter the IPv6 address of the network or host from which the packets were sent in the **x:x:x:x::x** format followed by the prefix length in the **/x** format. Range: /0 to /128 The **::** notation specifies successive hexadecimal fields of zero.
mask	Enter a network mask in /prefix format (**/x**).
any	Enter the keyword **any** to specify that all routes are subject to the filter.
host *ipv6-address*	Enter the keyword **host** followed by the IPv6 address of the host in the **x:x:x:x::x** format. The **::** notation specifies successive hexadecimal fields of zero
operator	(OPTIONAL) Enter one of the following logical operand: • **eq** = equal to • **neq** = not equal to • **gt** = greater than • **lt** = less than • **range** = inclusive range of ports (you must specify two port for the *port* parameter.)
port port	Enter the application layer port number. Enter two port numbers if using the range logical operand. Range: 0 to 65535. The following list includes some common TCP port numbers: 23 = Telnet 20 and 21 = FTP 25 = SMTP 169 = SNMP
destination address	Enter the IPv6 address of the network or host to which the packets are sent in the **x:x:x:x::x** format followed by the prefix length in the **/x** format. Range: /0 to /128 The **::** notation specifies successive hexadecimal fields of zero.

bit	Enter a flag or combination of bits: **ack:** acknowledgement field **fin**: finish (no more data from the user) **psh:** push function **rst:** reset the connection **syn:** synchronize sequence numbers **urg:** urgent field
count	(OPTIONAL) Enter the keyword **count** to count packets processed by the filter.
byte	(OPTIONAL) Enter the keyword **byte** to count bytes processed by the filter.
log	(OPTIONAL) Enter the keyword **log** to enter ACL matches in the log.
monitor	(OPTIONAL) Enter the keyword **monitor** to monitor traffic on the monitoring interface specified in the flow-based monitoring session along with the filter operation.

Defaults Not configured.

Command Modes ACCESS-LIST (conf-ipv6-acl)

Command History

Version 7.4.1.0	Added **monitor** option

Usage Information Most ACL rules require one entry in the CAM. However, rules with TCP and UDP port operators (**gt**, **lt**, **range**) may require more than one entry. The range of ports is configured in the CAM based on bitmask boundaries; the space required depends on exactly what ports are included in the range.

For example, an ACL rule with TCP port **range 4000 - 8000** uses 8 entries in the CAM:

```
Rule#       Data             Mask             From  To    #Covered

1     0000111110100000 1111111111100000 4000  4031  32
2     0000111111000000 1111111111000000 4032  4095  64
3     0001000000000000 1111100000000000 4096  6143  2048
4     0001100000000000 1111110000000000 6144  7167  1024
5     0001110000000000 1111111000000000 7168  7679  512
6     0001111000000000 1111111100000000 7680  7935  256
7     0001111100000000 1111111111000000 7936  7999  64
8     0001111101000000 1111111111111111 8000  8000  1

Total Ports: 4001
```

But an ACL rule with TCP port **lt 1023** takes only one entry in the CAM:

```
Rule#       Data             Mask             From  To    #Covered

1     0000000000000000 1111110000000000 0     1023  1024

Total Ports: 1024
```

Related Commands

permit	Assign a permit filter for IPv6 packets.
permit udp	Assign a permit filter for UDP packets.

permit udp

C-Series	**No**
E-Series	✓

Configure a filter to pass UDP packets meeting the filter criteria.

Syntax

permit udp {*source address mask* | **any** | **host** *ipv6-address*} [*operator port* [*port*]] {*destination address* | **any** | **host** *ipv6-address*} [*operator port* [*port*]] [**count** [**byte**]] | [**log**] [**monitor**]

To remove this filter, you have two choices:

- use the **no seq** *sequence-number* command syntax if you know the filter's sequence number or
- use the **no permit udp** {*source address mask* | **any** | **host** *ipv6-address*} {*destination address* | **any** | **host** *ipv6-address*} command.

Parameters

source address	Enter the IPv6 address of the network or host from which the packets were sent in the **x:x:x:x::x** format followed by the prefix length in the **/x** format. Range: /0 to /128 The **::** notation specifies successive hexadecimal fields of zero.
mask	Enter a network mask in /prefix format (**/x**).
any	Enter the keyword **any** to specify that all routes are subject to the filter.
host *ipv6-address*	Enter the keyword **host** followed by the IPv6 address of the host in the **x:x:x:x::x** format. The **::** notation specifies successive hexadecimal fields of zero
operator	(OPTIONAL) Enter one of the following logical operand: • **eq** = equal to • **neq** = not equal to • **gt** = greater than • **lt** = less than • **range** = inclusive range of ports (you must specify two ports for the *port* parameter.)
port port	(OPTIONAL) Enter the application layer port number. Enter two port numbers if using the **range** logical operand. Range: 0 to 65535

destination address	Enter the IPv6 address of the network or host to which the packets are sent in the **x:x:x:x::x** format followed by the prefix length in the **/x** format. Range: /0 to /128 The **::** notation specifies successive hexadecimal fields of zero.
count	(OPTIONAL) Enter the keyword **count** to count packets processed by the filter.
byte	(OPTIONAL) Enter the keyword **byte** to count bytes processed by the filter.
log	(OPTIONAL) Enter the keyword **log** to enter ACL matches in the log.
monitor	(OPTIONAL) Enter the keyword **monitor** to monitor traffic on the monitoring interface specified in the flow-based monitoring session along with the filter operation.

Defaults

Not configured.

Command Modes

ACCESS LIST (conf-ipv6-acl)

Command History

Version 7.4.1.0	Added **monitor** option

Usage Information

Most ACL rules require one entry in the CAM. However, rules with TCP and UDP port operators (**gt**, **lt**, **range**) may require more than one entry. The range of ports is configured in the CAM based on bitmask boundaries; the space required depends on exactly what ports are included in the range.

For example, an ACL rule with TCP port **range 4000 - 8000** uses 8 entries in the CAM:

```
Rule#       Data              Mask       From  To    #Covered

1     0000111110100000 1111111111100000 4000  4031  32
2     0000111111000000 1111111111000000 4032  4095  64
3     0001000000000000 1111100000000000 4096  6143  2048
4     0001100000000000 1111110000000000 6144  7167  1024
5     0001110000000000 1111111000000000 7168  7679  512
6     0001111000000000 1111111100000000 7680  7935  256
7     0001111100000000 1111111111000000 7936  7999  64
8     0001111101000000 1111111111111111 8000  8000  1

Total Ports: 4001
```

But an ACL rule with TCP port **lt 1023** takes only one entry in the CAM:

```
Rule#       Data              Mask       From  To    #Covered

1     0000000000000000 1111110000000000 0     1023  1024

Total Ports: 1024
```

Related Commands

permit	Assign a permit filter for IP packets.
permit tcp	Assign a permit filter for TCP packets.

remark

C-Series	No
E-Series	✓

Enter a description for an IPv6 ACL entry.

Syntax **remark** *remark number* [*description*]

To delete the description, use the **no remark** *remark number* command (it is not necessary to include the remark description that you are deleting).

Parameters

remark number	Enter the remark number. Note that the same sequence number can be used for the remark and an ACL rule. Range: 0 to 4294967290
description	Enter a description of up to 80 characters.

Defaults Not configured

Command Modes ACCESS-LIST (conf-ipv6-acl)

Example

```
Force10(config-ipv6-acl)#remark 10 Remark for Entry # 10
Force10(config-ipv6-acl)#show config
!
ipv6 access-list Acl1
 description IPV6 Access-list
 seq 5 permit ipv6 1111::2222/127 host 3333::1111 log count bytes
 remark 10 Remark for Entry # 10
 seq 10 permit icmp host 3333:: any mobile-advertisement log
 seq 15 deny tcp any any rst
 seq 20 permit udp any any gt 100 count
!Force10(config-ipv6-acl)#
```

Usage Information As shown in the example above, the same sequence number is used for the remark and an ACL rule. The remark will precede the rule in the running-configuration because it is assumed that the remark is for that rule or that group of rules that follow the remark. You can configure up to 4294967290 remarks in a given ACL.

Related Commands

show config	Display the current ACL configuration.

resequence access-list

C-Series	No
E-Series	✓

Re-assign sequence numbers to entries of an existing access-list.

Syntax

resequence access-list {**ipv6** | **mac**} {*access-list-name StartingSeqNum Step-to-Increment* }

Parameters

ipv6 | **mac**	Enter the keyword **ipv6** or **mac** to identify the access list type to resequence.
access-list-name	Enter the name of a configured IP access list.
StartingSeqNum	Enter the starting sequence number to resequence. Range: 0 - 4294967290
Step-to-Increment	Enter the step to increment the sequence number. Range: 1 - 4294967290

Defaults

No default values or behavior

Command Modes

EXEC

EXEC privilege

Command History

Version 7.4.1.0	Introduced

Usage Information

When all sequence numbers have been exhausted, this feature permits re-assigning new sequence number to entries of an existing access-list.

Related Commands

resequence prefix-list ipv6	Resequence a prefix list

resequence prefix-list ipv6

C-Series	No
E-Series	✓

Re-assign sequence numbers to entries of an existing prefix list.

Syntax

resequence prefix-list ipv6 {*prefix-list-name StartingSeqNum Step-to-increment*}

Parameters

prefix-list-name	Enter the name of configured prefix list.
StartingSeqNum	Enter the starting sequence number to resequence. Range: 0 – 65535
Step-to-Increment	Enter the step to increment the sequence number. Range: 1 – 65535

Defaults

No default values or behavior

Command Modes

EXEC

EXEC privilege

Command History

Version 7.4.1.0	Introduced

Usage Information

When all sequence numbers have been exhausted, this feature permits re-assigning new sequence number to entries of an existing prefix list.

Related Commands

resequence access-list	Resequence an access-list

seq

C-Series	**No**
E-Series	✓

Assign a sequence number to a deny or permit filter in an IPv6 access list while creating the filter.

Syntax

seq *sequence-number* {**deny** | **permit**} {*ipv6-protocol-number* | **icmp | ip | tcp | udp**} {*source address mask* | **any** | **host** *ipv6-address*} {*destination address* | **any** | **host** *ipv6-address*} [*operator port* [*port*]] [**count** [**byte**]] | [**log**] [**monitor**]

To delete a filter, use the **no seq** *sequence-number* command.

Parameters

sequence-number	Enter a number from 0 to 4294967290.
deny	Enter the keyword **deny** to configure a filter to drop packets meeting this condition.
permit	Enter the keyword **permit** to configure a filter to forward packets meeting this criteria.
ipv6-protocol-number	Enter an IPv6 protocol number. Range: 0 to 255

icmp	Enter the keyword **icmp** to configure an Internet Control Message Protocol version 6 filter.
ipv6	Enter the keyword **ipv6** to configure any Internet Protocol version 6 filter.
tcp	Enter the keyword **tcp** to configure a Transmission Control protocol filter.
udp	Enter the keyword **udp** to configure a User Datagram Protocol filter.
source address	Enter the IPv6 address of the network or host from which the packets were sent in the **x:x:x:x::x** format followed by the prefix length in the **/x** format. Range: /0 to /128 The **::** notation specifies successive hexadecimal fields of zero.
mask	Enter a network mask in /prefix format (**/x**).
any	Enter the keyword **any** to specify that all routes are subject to the filter.
host *ipv6-address*	Enter the keyword **host** followed by the IPv6 address of the host in the **x:x:x:x::x** format. The **::** notation specifies successive hexadecimal fields of zero
operator	(OPTIONAL) Enter one of the following logical operands: • **eq** = equal to • **neq** = not equal to • **gt** = greater than • **lt** = less than • **range** = inclusive range of ports (you must specify two ports for the *port* parameter.)
port port	(OPTIONAL) Enter the application layer port number. Enter two port numbers if using the **range** logical operand. Range: 0 to 65535 The following list includes some common TCP port numbers: • 23 = Telnet • 20 and 21 = FTP • 25 = SMTP • 169 = SNMP
destination address	Enter the IPv6 address of the network or host to which the packets are sent in the **x:x:x:x::x** format followed by the prefix length in the **/x** format. Range: /0 to /128 The **::** notation specifies successive hexadecimal fields of zero.
message-type	(OPTIONAL) Enter an ICMP message type, either with the type (and code, if necessary) numbers or with the name of the message type (ICMP message types are listed in Table 47). Range: 0 to 255 for ICMP type; 0 to 255 for ICMP code
count	(OPTIONAL) Enter the keyword **count** to count packets processed by the filter.
byte	(OPTIONAL) Enter the keyword **byte** to count bytes processed by the filter.

log	(OPTIONAL) Enter the keyword **log** to enter ACL matches in the log. Supported on Jumbo-enabled line cards only.
monitor	(OPTIONAL) Enter the keyword **monitor** to monitor traffic on the monitoring interface specified in the flow-based monitoring session along with the filter operation.

Defaults Not configured.

Command Modes ACCESS-LIST (conf-ipv6-acl)

Command History

Version 7.4.1.0	Added **monitor** option

Related Commands

deny	Configure a filter to drop packets.
permit	Configure a filter to forward packets.

show config

C-Series	**No**
E-Series	✓

View the current IPv6 ACL configuration.

Syntax **show config**

Command Modes CONFIGURATION (conf-ipv6-acl)

Example

```
Force10(conf-ipv6-acl)#show config
!
ipv6 access-list Acl1
 seq 5 permit ipv6 1111::2222/127 host 3333::1111 log count bytes
 seq 10 permit icmp host 3333:: any mobile-advertisement log
 seq 15 deny tcp any any rst
 seq 20 permit udp any any gt 100 count
Force10(conf-ipv6-acl)#
```

Figure 245 show config Command Example

show ipv6 accounting access-list

C-Series	No
E-Series	✓

View the IPv6 access-lists created on the E-Series and the sequence of filters.

Syntax **show accounting access-list** *access-list-name* **interface** *interface*

Parameters

access-list-name	Enter the name of the ACL to be displayed.
interface *interface*	Enter the keyword **interface** followed by the interface type and slot/port or number information: • For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For a Port Channel interface, enter the keyword **port-channel** followed by a number from 1 to 32 for EtherScale, 1 to 255 for TeraScale. • For a SONET interface, enter the keyword **sonet** followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information.

Command Modes EXEC

EXEC privilege

Example

```
Force10#show ipv6 accounting access-list
!
Ingress IPv6 access list AclList1 on GigabitEthernet 9/0
Total cam count 15
 seq 10 permit icmp host 3333:: any mobile-advertisement log
 seq 15 deny tcp any any rst
 seq 20 permit udp any any gt 101 count (0 packets)
!
Force10#
```

Figure 246 show ipv6 accounting access-lists Command Example)

Table 48 defines the information in Figure 246.

Table 48 show ip accounting access-lists Command Example Field

Field	Description
“Ingress IPv6...”	Displays the name of the IPv6 ACL, in this example “AclList1”.
“seq 10 ...”	Displays the filter. If the keywords count or byte were configured in the filter, the number of packets or bytes processed by the filter is displayed at the end of the line.

show running-config acl

C-Series	No
E-Series	✓

Display the ACL running configuration.

Syntax **show running-config acl**

Command Modes EXEC

EXEC Privlege

Example

```
Force10#show running-config acl
!
ip access-list extended ext-acl1
!
ip access-list standard std-acl1
!
ipv6 access-list Acl1
 description IPV6 Access-list
 seq 5 permit ipv6 1111::2222/127 host 3333::1111 log count bytes
 remark 10 Remark for Entry # 10
 seq 10 permit icmp host 3333:: any mobile-advertisement log
 seq 15 deny tcp any any rst
 seq 20 permit udp any any gt 100 count
!Force10#
```

Figure 247 show running-config acl Command Example

Route Map Commands

The following commands allow you to configure route maps and their redistribution criteria.

- match ipv6 address on page 714
- match ipv6 next-hop on page 714
- match ipv6 route-source on page 715
- route-map on page 715
- set ipv6 next-hop on page 716
- show config on page 716
- show route-map on page 717

match ipv6 address

C-Series	No
E-Series	✓

Configure a filter to match routes based on IPv6 addresses specified in an access list.

Syntax **match ipv6 address** *prefix-list-name*

To delete a match, use the **no match ipv6 address** *prefix-list-name* command.

Parameters

prefix-list-name	Enter the name of IPv6 prefix list name.

Defaults Not configured.

Command Modes ROUTE-MAP (config-route-map)

Related Commands

match ipv6 next-hop	Redistribute routes that match the next-hop IP address.
match ipv6 route-source	Redistribute routes that match routes advertised by other routers.

match ipv6 next-hop

C-Series	No
E-Series	✓

Configure a filter which matches based on the next-hop IPv6 addresses specified in the IPv6 prefix list.

Syntax **match ipv6 next-hop prefix-list** *prefix-list-name*

To delete a match, use the **no match ipv6 next-hop prefix-list** *prefix-list-name* command.

Parameters

prefix-list *prefix-list-name*	Enter the keywords **prefix-list** followed by the name of configured prefix list.

Defaults Not configured.

Command Modes ROUTE-MAP (config-route-map)

Related Commands

match ipv6 address	Redistribute routes that match an IP address.
match ipv6 route-source	Redistribute routes that match routes advertised by other routers.

match ipv6 route-source

C-Series	No
E-Series	✓

Configure a filter which matches based on the routes advertised in the IPv6 prefix lists.

Syntax **match ipv6 route-source prefix-list** *prefix-list-name*

To delete a match, use the **no match ipv6 route-source prefix-list** *prefix-list-name* command.

Parameters

prefix-list *prefix-list-name*	Enter the keywords **prefix-list** followed by the name of configured prefix list.

Defaults Not configured.

Command Modes ROUTE-MAP (config-route-map)

Related Commands

match ipv6 address	Redistribute routes that match an IP address.
match ipv6 next-hop	Redistribute routes that match the next-hop IP address.

route-map

C-Series	No
E-Series	✓

Designate a IPv6 route map name and enter the ROUTE-MAP mode.

Syntax **route-map** *map-name*

To delete a route map, use the **no route-map** *map-name* command.

Parameters

map-name	Enter a text string to name the route map for easy identification.

Defaults Not configured

Command Modes CONFIGURATION (config-route-map)

Example

```
Force10(conf)#route-map Rmap1

Force10(config-route-map)#match ?
…
ip                      IP specific information
ipv6                    IPv6 specific information
…
```

Figure 248 route-map Command Example

Related Commands

show config	View the current configuration.

set ipv6 next-hop

C-Series	**No**
E-Series	✓

Configure a filter that specifies IPv6 address as the next hop.

Syntax **set ipv6 next-hop** *ipv6-address*

To delete the setting, use the **no set ipv6 next-hop** *ipv6-address* command.

Parameters

ipv6-address	Enter the IPv6 address in the **x:x:x:x::x** format. **Note:** The **::** notation specifies successive hexadecimal fields of zeros

Defaults Not configured.

Command Modes ROUTE-MAP (config-route-map)

Usage Information The set ipv6 next-hop command is the only way to set an IPv6 Next-Hop.

show config

C-Series	**No**
E-Series	✓

View the current route map configuration.

Syntax **show config**

Command Modes ROUTE-MAP (config-route-map)

Example

```
Force10(config-route-map)#show config
!
route-map Rmap1 permit 10
 match ip address v4plist
 match ipv6 address plist1
 match ipv6 next-hop prefix-list plist2
 match ipv6 route-source prefix-list plist3
 set next-hop 1.1.1.1
 set ipv6 next-hop 3333:2222::
Force10(config-route-map)#
```

Figure 249 show config Command Example

show route-map

C-Series	No
E-Series	✓

View the current route map configurations.

Syntax **show route-map**

Command Modes EXEC

EXEC privilege

Example

```
Force10#show route-map
!
route-map Rmap1, permit, sequence 10
 Match clauses:
  ip address: v4plist
  ipv6 address: plist1
  ipv6 next-hop prefix-lists: plist2
  ipv6 route-source prefix-lists: plist3
 Set clauses:
  next-hop 1.1.1.1
  ipv6 next-hop 3333:2222::
Force10#
```

Figure 250 show route-map Command Example

Related Commands

route-map	Configure a route map.

Chapter 28 IP Routing Commands

IP-related commands are described in this chapter. The IP-related commands are:

- arp on page 720
- arp timeout on page 721
- clear arp-cache on page 721
- clear host on page 722
- clear ip fib linecard on page 723
- clear ip route on page 723
- clear tcp statistics on page 724
- debug arp on page 724
- debug ip dhcp on page 725
- debug ip icmp on page 726
- debug ip packet on page 727
- hash-algorithm ecmp on page 728 (C-Series)
- hash-algorithm on page 729 (E-Series)
- ip address on page 731
- ip directed-broadcast
- ip domain-list on page 732
- ip domain-lookup on page 733
- ip domain-name on page 734
- ip fib download-igp-only on page 734
- ip helper-address on page 735
- ip helper-address hop-count disable on page 735
- ip host on page 736
- ip max-frag-count on page 736
- ip mtu on page 737
- ip name-server on page 738
- ip proxy-arp on page 739
- ip redirects on page 739
- ip route on page 740
- ip source-route on page 741
- ip unreachables on page 741

- ip vlan-flooding on page 742
- load-balance (C-Series) on page 742 (C-Series)
- load-balance (E-Series) on page 744 (E-Series)
- management route on page 745
- show arp on page 747
- show hosts on page 749
- show ip cam on page 750
- show ip fib linecard on page 753
- show ip flow on page 754
- show ip interface on page 755
- show ip management-route on page 757
- show ip protocols on page 758
- show ip route on page 758
- show ip route list on page 760
- show ip route summary on page 761
- show ip traffic on page 762
- show protocol-termination-table on page 764
- show tcp statistics on page 765

arp

Use Address Resolution Protocol (ARP) to associate an IP address with a MAC address in the E-Series.

Syntax

arp *ip-address mac-address interface*

To remove an ARP address, use the **no arp** *ip-address* command.

Parameters

ip-address	Enter an IP address in dotted decimal format.
mac-address	Enter a MAC address in nnnn.nnnn.nnnn format.
interface	Enter the following keywords and slot/port or number information: • For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For the Management interface, enter the keyword **ManagementEthernet** followed by the slot/port information. The slot range is 0-1 and the port range is 0. • For a Port Channel interface, enter the keyword **port-channel** followed by a number: C-Series Range: 1-128 E-Series Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale. • For a SONET interface, enter the keyword **sonet** followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information.

Defaults Not configured.

Command Modes CONFIGURATION

Usage Information You cannot use Class D or Class E IP addresses or zero IP address (0.0.0.0) when creating a static ARP. Zero MAC addresses (00:00:00:00:00:00) are also invalid.

Related Commands

clear arp-cache	Clear dynamic ARP entries from the ARP table.
show arp	Display ARP table.

arp timeout

Set the time interval for an ARP entry to remain in the ARP cache.

Syntax **arp timeout** *minutes*

To return to the default value, enter **no arp timeout**.

Parameters

seconds	Enter the number of minutes. Range: 0 to 35790. Default: 240 minutes.

Defaults 240 minutes (4 hours)

Command Modes INTERFACE

Related Commands

show interfaces	Displays the ARP timeout value for all available interfaces.

clear arp-cache

Clear the dynamic ARP entries from a specific interface or optionally delete (**no-refresh**) ARP entries from CAM.

Syntax **clear arp-cache** [*interface* | **ip** *ip-address*] [**no-refresh**]

Parameters

interface	(OPTIONAL) Enter the following keywords and slot/port or number information: • For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For the Management interface, enter the keyword **ManagementEthernet** followed by the slot/port information. The slot range is 0-1 and the port range is 0. • For a Port Channel interface, enter the keyword **port-channel** followed by a number: C-Series Range: 1-128 E-Series Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale. • For a SONET interface, enter the keyword **sonet** followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information. • For a VLAN, enter the keyword **vlan** followed by a number from 1 to 4094.
ip *ip-address*	(OPTIONAL) Enter the keyword ip followed by the IP address of the ARP entry you wish to clear.
no-refresh	(OPTIONAL) Enter the keyword **no-refresh** to delete the ARP entry from CAM. Or use this option with *interface* or **ip** *ip-address* to specify which dynamic ARP entires you want to delete. **Note:** Transit traffic may not be forwarded during the period when deleted ARP entries are resolved again and re-installed in CAM. Use this option with extreme caution.

Command Modes EXEC privilege

clear host

Remove one or all dynamically learnt host table entries.

Syntax **clear host** *name*

Parameters

name	Enter the name of the host to delete. Enter * to delete all host table entries.

Command Modes EXEC privilege

clear ip fib linecard

Clear all Forwarding Information Base (fib) entries in the specified line card (use this command with caution, see Usage Information below)

Syntax **clear ip fib linecard** *slot-number*

Parameters

slot-number	Enter the number of the line card slot. C-Series Range: 0-7 on the C300 E-Series Range: 0 to 13 on a E1200, 0 to 6 on a E600/E600i, and 0 to 5 on a E300

Command Mode EXEC

EXEC privilege

Usage Information Use this command to clear Layer 3 CAM inconsistencies.

Caution: Executing this command will cause traffic disruption.

Related Commands

show ip fib linecard	Show FIB entries

clear ip route

Clear one or all routes in the routing table.

Syntax **clear ip route** {* | *ip-address mask*}

Parameters

*	Enter an asterisk (*) to clear all learned IP routes.
ip-address mask	Enter a specific IP address and mask in dotted decimal format to clear that IP address from the routing table.

Command Modes EXEC privilege

Related Commands

ip route	Assign an IP route to the E-Series.
show ip route	View the routing table.
show ip route summary	View a summary of the routing table.

clear tcp statistics

Clear TCP counters.

Syntax **clear tcp statistics** {**all** | **cp** | **rp1** | **rp2**}

Parameters

all	Enter the keyword **all** to clear all TCP statistics maintained on all E-Series processors.
cp	(OPTIONAL) Enter the **cp** to clear only statistics from the Control Processor.
rp1	(OPTIONAL) Enter the keyword **rp1** to clear only the statistics from Route Processor 1.
rp2	(OPTIONAL) Enter the keyword **rp2** to clear only the statistics from Route Processor 2.

Command Modes EXEC privilege

debug arp

View information on ARP transactions.

Syntax **debug arp** [*interface*] [**count** *value*]

To stop debugging ARP transactions, enter **no debug arp**.

Parameters

interface	(OPTIONAL) Enter the following keywords and slot/port or number information: • For a 1-Gigabit Ethernet interface, enter the keyword **gigabitethernet** followed by the slot/port information. • For the Management interface, enter the keyword **managementethernet** followed by the slot/port information. The slot range is 0-1 and the port range is 0. • For a Port Channel interface, enter the keyword **port-channel** followed by a number: C-Series Range: 1-128 E-Series Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale. • For a SONET interface, enter the keyword **sonet** followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **tengigabitethernet** followed by the slot/port information. • For a VLAN, enter the keyword **vlan** followed by a number from 1 to 4094.
count *value*	(OPTIONAL) Enter the keyword **count** followed by the count value. Range: 1 to 65534

Command Modes EXEC privilege

Command History

Version 6.3.1.0	Added the count option

Defaults No default behavior or values

Usage Information Use the **count** option to stop packets from flooding the user terminal when debugging is turned on.

debug ip dhcp

Enable debug information for DHCP relay transactions and display the information on the console.

Syntax **debug ip dhcp**

To disable debug, use the **no debug ip dhcp** command.

Defaults Debug disabled

Command Modes EXEC privilege

Command History

Version 6.4.10	Introduced

Example

```
Force10#debug ip dhcp
00:12:21 : %RELAY-I-PACKET: BOOTP REQUEST (Unicast) received at interface 113.3.3.17 BOOTP
Request, hops = 0, XID = 0xbf05140f, secs = 0, hwaddr = 00:60:CF:20:7B:8C, giaddr = 0.0.0.0
00:12:21 : %RELAY-I-BOOTREQUEST: Forwarded BOOTREQUEST for 00:60:CF:20:7B:8C to 14.4.4.2
00:12:26 : %RELAY-I-PACKET: BOOTP REQUEST (Unicast) received at interface 113.3.3.17 BOOTP
Request, hops = 0, XID = 0xbf05140f, secs = 5, hwaddr = 00:60:CF:20:7B:8C, giaddr = 0.0.0.0
00:12:26 : %RELAY-I-BOOTREQUEST: Forwarded BOOTREQUEST for 00:60:CF:20:7B:8C to 14.4.4.2
00:12:40 : %RELAY-I-PACKET: BOOTP REQUEST (Unicast) received at interface 113.3.3.17 BOOTP
Request, hops = 0, XID = 0xda4f9503, secs = 0, hwaddr = 00:60:CF:20:7B:8C, giaddr = 0.0.0.0
00:12:40 : %RELAY-I-BOOTREQUEST: Forwarded BOOTREQUEST for 00:60:CF:20:7B:8C to 14.4.4.2
00:12:42 : %RELAY-I-PACKET: BOOTP REPLY (Unicast) received at interface 14.4.4.1 BOOTP Reply,
hops = 0, XID = 0xda4f9503, secs = 0, hwaddr = 00:60:CF:20:7B:8C, giaddr = 113.3.3.17
00:12:42 : %RELAY-I-BOOTREPLY: Forwarded BOOTREPLY for 00:60:CF:20:7B:8C to 113.3.3.254
00:12:42 : %RELAY-I-PACKET: BOOTP REQUEST (Unicast) received at interface 113.3.3.17 BOOTP
Request, hops = 0, XID = 0xda4f9503, secs = 0, hwaddr = 00:60:CF:20:7B:8C, giaddr = 0.0.0.0
00:12:42 : %RELAY-I-BOOTREQUEST: Forwarded BOOTREQUEST for 00:60:CF:20:7B:8C to 14.4.4.2
00:12:42 : %RELAY-I-PACKET: BOOTP REPLY (Unicast) received at interface 14.4.4.1 BOOTP Reply,
hops = 0, XID = 0xda4f9503, secs = 0, hwaddr = 00:60:CF:20:7B:8C, giaddr = 113.3.3.17
00:12:42 : %RELAY-I-BOOTREPLY: Forwarded BOOTREPLY for 00:60:CF:20:7B:8C to 113.3.3.254
Force10#
```

Related Commands

ip helper-address	Specify the destination broadcast or host address for DHCP server request.
ip helper-address hop-count disable	Disable hop-count increment for DHCP relay agent.

debug ip icmp

View information on the Internal Control Message Protocol (ICMP).

Syntax **debug ip icmp** [*interface*] [**count** *value*]

To disable debugging, use the **no debug ip icmp** command.

Parameters

interface	(OPTIONAL) Enter the following keywords and slot/port or number information: • For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For the Management interface, enter the keyword **ManagementEthernet** followed by the slot/port information. The slot range is 0 and the port range is 0-1. • For a Port Channel interface, enter the keyword **port-channel** followed by a number: C-Series Range: 1-128 E-Series Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale. • For a SONET interface, enter the keyword **sonet** followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information. • For VLAN, enter the keyword **vlan** followed by a number from 1 to 4095.
count *value*	(OPTIONAL) Enter the keyword **count** followed by the count value. Range: 1 to 65534 Default: Infinity

Command Modes EXEC privilege

Command History

Version 6.3.1.0	Added the count option

Example

```
ICMP: echo request rcvd from src 40.40.40.40
ICMP: src 40.40.40.40, dst 40.40.40.40, echo reply
ICMP: src 40.40.40.40, dst 40.40.40.40, echo reply
ICMP: echo request sent to dst 40.40.40.40
ICMP: echo request rcvd from src 40.40.40.40
ICMP: src 40.40.40.40, dst 40.40.40.40, echo reply
ICMP: src 40.40.40.40, dst 40.40.40.40, echo reply
ICMP: echo request sent to dst 40.40.40.40
```

Figure 251 debug ip icmp Command Example (Partial)

Usage Information Use the **count** option to stop packets from flooding the user terminal when debugging is turned on.

debug ip packet

View a log of IP packets sent and received.

Syntax **debug ip packet** [*interface*] [**count** *value*]

To disable debugging, use the **no debug ip packet** command.

Parameters

interface	(OPTIONAL) Enter the following keywords and slot/port or number information: • For a 1-Gigabit Ethernet interface, enter the keyword **gigabitethernet** followed by the slot/port information. • For the management interface on the RPM, enter the keyword **managementethernet** followed by the slot/port information. The slot range is 0-1 and the port range is 0. • For a Port Channel interface, enter the keyword **port-channel** followed by a number: C-Series Range: 1-128 E-Series Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale. • For a SONET interface, enter the keyword **sonet** followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **tengigabitethernet** followed by the slot/port information. • For a VLAN, enter the keyword **vlan** followed by a number from 1 to 4095.
count *value*	(OPTIONAL) Enter the keyword **count** followed by the count value. Range: 1 to 65534 Default: Infinity

Command Mode EXEC privilege

Command History

Version 6.3.1.0	Added the count option

Example

```
IP: s=10.1.2.62 (local), d=10.1.2.206 (Ma 0/0), len 54, sending
    TCP src=23, dst=40869, seq=2112994894, ack=606901739, win=8191 ACK PUSH
IP: s=10.1.2.206 (Ma 0/0), d=10.1.2.62, len 40, rcvd
    TCP src=0, dst=0, seq=0, ack=0, win=0
IP: s=10.1.2.62 (local), d=10.1.2.206 (Ma 0/0), len 226, sending
    TCP src=23, dst=40869, seq=2112994896, ack=606901739, win=8192 ACK PUSH
IP: s=10.1.2.216 (Ma 0/0), d=10.1.2.255, len 78, rcvd
    UDP src=0, dst=0
IP: s=10.1.2.62 (local), d=10.1.2.3 (Ma 0/0), len 1500, sending fragment
    IP Fragment, Ident = 4741, fragment offset = 0
    ICMP type=0, code=0
IP: s=10.1.2.62 (local), d=10.1.2.3 (Ma 0/0), len 1500, sending fragment
    IP Fragment, Ident = 4741, fragment offset = 1480
IP: s=40.40.40.40 (local), d=224.0.0.5 (Gi 4/11), len 64, sending broad/multicast
proto=89
IP: s=40.40.40.40 (local), d=224.0.0.6 (Gi 4/11), len 28, sending broad/multicast
proto=2
IP: s=0.0.0.0, d=30.30.30.30, len 100, unroutable
    ICMP type=8, code=0
IP: s=0.0.0.0, d=30.30.30.30, len 100, unroutable
    ICMP type=8, code=0
```

Figure 252 debug ip packet Command Example (Partial)

Table 49 describes the information in Figure 252.

Table 49 debug ip packet Command Example Fields

Field	Description
s=	Lists the source address of the packet and the name of the interface (in parentheses) that received the packet.
d=	Lists the destination address of the packet and the name of the interface (in parentheses) through which the packet is being sent out on the network.
len	Displays the packet's length.
sending rcvd fragment sending broad/multicast proto unroutable	The last part of each line lists the status of the packet.
TCP src=	Displays the source and destination ports, the sequence number, the acknowledgement number, and the window size of the packets in that TCP packets.
UDP src=	Displays the source and destination ports for the UDP packets.
ICMP type=	Displays the ICMP type and code.
IP Fragment	States that it is a fragment and displays the unique number identifying the fragment (Ident) and the offset (in 8-byte units) of this fragment (fragment offset) from the beginning of original datagram.

Usage Information

Use the **count** option to stop packets from flooding the user terminal when debugging is turned on.

hash-algorithm ecmp

C-Series	✓
E-Series	No

Change the hash algorithm used to distribute traffic flows across an ECMP group.

Syntax

hash-algorithm ecmp {**crc-upper**} | {**dest-ip**} | {**lsb**}

To return to the default and remove all hash algorithm configurations, use the **no hash-algorithm** command.

Parameters

crc-upper	Uses the upper 32 bits of key for hash computation Default : **crc-lower**
dest-ip	Uses destination IP for ECMP hashing Default = **enabled**
lsb	Returns the LSB of the key as the hash Default = **crc-lower**

Defaults **crc-lower, dest-ip enabled**

Command Modes CONFIGURATION

Command History

Version 7.5.1.0	Introduced on C-Series

Usage Information

The hash value calculated with the hash-algorithm command is unique to the entire chassis. The default ECMP hash configuration is **crc-lower**. This takes the lower 32 bits of the hash key to compute the egress port and is the "fall-back" configuration if the user hasn't configured anything else.

The different hash algorithms are based on the number of ECMP group members and packet values. The default hash algorithm yields the most balanced results in various test scenarios, but if the default algorithm does not provide satisfactory distribution of traffic, then use the hash-algorithm command to designate another algorithm.

When a member leaves or is added to the ECMP group, the hash algorithm is recalculated to balance traffic across the members.

Related Commands

load-balance (C-Series) (C-Series)	Change the traffic balancing method on a C-Series chassis.

hash-algorithm

C-Series	No
E-Series	✔

Change the hash algorithm used to distribute traffic flows across a Port Channel. The ECMP, LAG, and line card options are supported only on the E-Series TeraScale chassis.

Syntax **hash-algorithm** {*algorithm-number*} | {**ecmp** *number*} {**lag** *number*} {**linecard** *number* **ip-sa-mask** *value* **ip-da-mask** *value*}

To return to the default and remove all hash algorithm configurations, use the **no hash-algorithm** command.

To remove the hash algorithm on ECMP, use the **no hash-algorithm ecmp** *number* command

To remove the hash algorithm on line card(s) only, use the **no hash-algorithm linecard** *number* command.

To return to a zero value, use the **no hash-algorithm** *algorithm-number* command.

Parameters

algorithm-number	Enter the algorithm number. Range: 0 to 47 **Note:** For EtherScale, only range 0 to 15 is valid; 16 to 47 will be considered as 15.
ecmp *number*	TeraScale Only: Enter the keyword **ecmp** followed by the ECMP number. Range: 0 to 47
lag *number*	TeraScale Only: Enter the keyword **lag** followed by the LAG number. Range: 0 to 47
linecard *number*	(OPTIONAL) TeraScale Only: Enter the keyword **linecard** followed by the linecard slot number. Range: 0 to 13 on a E1200, 0 to 6 on a E600/E600i, and 0 to 5 on a E300
ip-sa-mask *value*	(OPTIONAL) Enter the keyword **ip-sa-mask** followed by the ECMP/LAG hash mask value. Range: 0 to FF Default: FF
ip-da-mask *value*	(OPTIONAL) Enter the keyword **ip-da-mask** followed by the ECMP/LAG hash mask value. Range: 0 to FF Default: FF

Defaults

0 for hash-algorithm

IPSA and IPDA mask value is FF for line card

Command Modes

CONFIGURATION

Command History

Version 6.5.1.0	Added support for the line card option on TeraScale only
Version 6.3.1.0	Added the support for ECMP and LAG on TeraScale only

Usage Information

The hash value calculated with the hash-algorithm command is unique to the entire chassis. The hash algorithm command with the line card option changes the hash for a particular line card by applying the mask specified in the IPSA and IPDA fields.

The line card option is applicable with the lag-hash-align microcode only (refer to cam-profile default microcode on page 273). Any other microcode returns an error message as follows:

```
Force10(conf)#hash-algorithm linecard 5 ip-sa-mask ff ip-da-mask ff
% Error: This command is not supported in the current microcode configuration.
```

In addition, the **linecard** *number* **ip-sa-mask** *value* **ip-da-mask** *value* option has the following behavior to maintain bi-directionality:

- When hashing is done on both IPSA and IPDA, the **ip-sa-mask** and **ip-da-mask** values must be equal. (Single Linecard)

- When hashing is done only on IPSA or IPDA, FTOS maintains bi-directionality with masks set to XX 00 for line card 1 and 00 XX for line card 2 (**ip-sa-mask** and **ip-da-mask**). The mask value must be the same for both line cards when using multiple line cards as ingress (where *XX* is any value from 00 to FF for both line cards). For example, assume traffic is flowing between linecard 1 and linecard 2:

  hash-algorithm linecard 1 ip-sa-mask aa ip-da-mask 00
  hash-algorithm linecard 2 ip-sa-mask 00 ip-da-mask aa

The different hash algorithms are based on the number of Port Channel members and packet values. The default hash algorithm (number 0) yields the most balanced results in various test scenarios, but if the default algorithm does not provide a satisfactory distribution of traffic, then use the hash-algorithm command to designate another algorithm.

When a Port Channel member leaves or is added to the Port Channel, the hash algorithm is recalculated to balance traffic across the members.

On TeraScale if the keyword **ECMP** or **LAG** is not entered, FTOS assumes it to be common for both. If the keyword **ECMP** or **LAG** is entered separately, both should fall in the range of 0 to 23 or 24 to 47 since compression enable/disable is common for both.

For EtherScale, only the range 0 to 15 is valid; 16 to 47 is considerd as 15.

0-11	**Compression Enabled**
	rotate [0 - 11]
12 - 23	**Compression Enabled**
	shift [0 - 11]
24 - 35	**Compression Disabled**
	rotate [0 - 11]
36 - 47	**Compression Disabled**
	shift [0 - 11]

Related Commands

load-balance (E-Series)	Change the traffic balancing method.

ip address

Assign a primary and secondary IP address to the interface.

Syntax **ip address** *ip-address mask* [**secondary**]

To delete an IP address from an interface, use the **no ip address** [*ip-address*] command.

Parameters

ip-address	Enter an IP address in dotted decimal format.
mask	Enter the mask of the IP address in slash prefix format (for example, /24).
secondary	(OPTIONAL) Enter the keyword **secondary** to designate the IP address as the secondary address.

Defaults Not configured.

Command Modes INTERFACE

Usage Information You must be in the INTERFACE mode before you add an IP address to an interface. Assign an IP address to an interface prior to entering the ROUTER OSPF mode.

ip directed-broadcast

Enables the interface to receive directed broadcast packets.

Syntax ip directed-broadcast

To disable the interface from receiving directed broadcast packets, enter no ip directed-broadcast.

Defaults Disabled (that is, the interface does not receive directed broadcast packets)

Command Modes INTERFACE

ip domain-list

Configure names to complete unqualified host names.

Syntax **ip domain-list** *name*

To remove the name, use the **no ip domain-list** *name* command.

Parameters

name	Enter a domain name to be used to complete unqualified names (that is, incomplete domain names that cannot be resolved).

Defaults Disabled.

Command Modes CONFIGURATION

Usage Information Configure the ip domain-list command up to 6 times to configure a list of possible domain names.

If both the ip domain-name and ip domain-list commands are configured, the software will try to resolve the name using the ip domain-name command. If the name is not resolved, the software goes through the list of names configured with the ip domain-list command to find a match.

Use the following steps to enable dynamic resolution of hosts:

- specify a domain name server with the ip name-server command.
- enable DNS with the ip domain-lookup command.

To view current bindings, use the show hosts command. To view DNS related configuration, use the **show running-config resolve** command.

Related Commands

ip domain-name	Specify a DNS server.

ip domain-lookup

Enable dynamic host-name to address resolution (that is, DNS).

Syntax **ip domain-lookup**

To disable DNS lookup, use the **no ip domain-lookup**.

Defaults Disabled.

Command Mode CONFIGURATION

Usage Information To fully enable DNS, also specify one or more domain name servers with the ip name-server command.

FTOS does not support sending DNS queries over a VLAN. DNS queries are sent out all other interfaces, including the Management port.

To view current bindings, use the show hosts command.

Related Commands

ip name-server	Specify a DNS server.
show hosts	View current bindings.

ip domain-name

Configure one domain name for the E-Series.

Syntax **ip domain-name** *name*

To remove the domain name, enter **no ip domain-name**.

Parameters

name	Enter one domain name to be used to complete unqualified names (that is, incomplete domain names that cannot be resolved).

Defaults Not configured.

Command Modes CONFIGURATION

Usage Information You can only configure one domain name with the ip domain-name command. To configure more than one domain name, configure the ip domain-list command up to 6 times.

Use the following steps to enable dynamic resolution of hosts:

- specify a domain name server with the ip name-server command.
- enable DNS with the ip domain-lookup command.

To view current bindings, use the show hosts command.

Related Commands

ip domain-list	Configure additional names.

ip fib download-igp-only

C-Series	No
E-Series	✓

Configure the E-Series to download only IGP routes (for example, OSPF) on to line cards. When the command is configured or removed, it clears the routing table (similar to clear ip route command) and only IGP routes populate the table.

Syntax **ip fib download-igp-only** [**small-fib**]

To return to default setting, use the **no ip fib download-igp-only** [**small-fib**] command.

Parameters

small-fib	(OPTIONAL) Enter the keyword **small-fib** to download a smaller FIB table. This option is useful on line cards with a limited FIB size.

Defaults Disabled

Command Modes CONFIGURATION

ip helper-address

Specifies the destination broadcast or host address for DHCP server requests. FTOS supports DHCP-Relay services.

Syntax **ip helper-address** *ip-address*

To remove a DHCP server address, enter **no ip helper-address**.

Parameters

ip-address	Enter an IP address in dotted decimal format (A.B.C.D).

Defaults Not configured.

Command Modes INTERFACE

Usage Information You can add multiple DHCP servers by entering the ip helper-address command multiple times. If multiple servers are defined, an incoming request is sent simultaneously to all configured servers and the reply is forwarded to the DHCP client.

FTOS uses standard DHCP ports, that is UDP ports 67 (server) and 68 (client) for DHCP relay services. It listens on port 67 and if it receives a broadcast, the software converts it to unicast, and forwards to it to the DHCP-server with source port=68 and destination port=67.

The server replies with source port=67, destination port=67 and FTOS forwards to the client with source port=67, destination port=68.

ip helper-address hop-count disable

Disable the hop-count increment for the DHCP relay agent.

Syntax **ip helper-address hop-count disable**

To reenable the hop-count increment, use the **no ip helper-address hop-count disable** command.

Defaults Enabled; the hops field in the DHCP message header is incremented by default

Command Modes CONFIGURATION

Command History

Version 6.3.1.0	Introduced

Usage Information

This command disables the incrementing of the hops field when boot requests are relayed to a DHCP server through FTOS. If the incoming boot request already has a non-zero hops field, the message will be relayed with the same value for hops. However, the message will be discarded if the hops field exceeds 16, to comply with the relay agent behavior specified in RFC 1542.

Related Commands

ip helper-address	Specify the destination broadcast or host address for DHCP server requests.
show running-config	Display the current configuration and changes from default values.

ip host

Assign a name and IP address to be used by the host-to-IP address mapping table.

Syntax **ip host** *name ip-address*

To remove an IP host, use the **no ip host** *name* [*ip-address*] command.

Parameters

name	Enter a text string to associate with one IP address.
ip-address	Enter an IP address, in dotted decimal format, to be mapped to the name.

Defaults Not configured.

Command Modes CONFIGURATION

ip max-frag-count

Set the maximum number of fragments allowed in one packet for packet re-assembly.

Syntax **ip max-frag-count** *count*

To place no limit on the number of fragments allowed, enter **no ip max-frag-count**.

Parameters

count	Enter a number for the number of fragments allowed for re-assembly. Range: 2 to 256

Defaults No limit is set on number of fragments allowed.

Command Modes CONFIGURATION

Usage Information To avoid Denial of Service (DOS) attacks, keep the number of fragments allowed for re-assembly low.

ip mtu

Set the IP MTU (frame size) of the packet transmitted by the RPM for the line card interface. If the packet must be fragmented, FTOS sets the size of the fragmented packets to the size specified in this command.

Syntax **ip mtu** *value*

To return to the default IP MTU value, enter **no ip mtu**.

Parameters

value	Enter the maximum MTU size if the IP packet is fragmented. Default: 1500 bytes Range: 576 to 9234

Defaults 1500 bytes

Command Modes INTERFACE (Gigabit Ethernet and 10 Gigabit Ethernet interfaces)

Usage Information When you enter no mtu command, FTOS reduces the ip mtu value to 1536 bytes. To return the IP MTU value to the default, enter **no ip mtu**.

You must compensate for Layer 2 header when configuring link MTU on an Ethernet interface or FTOS may not fragment packets. If the packet includes a Layer 2 header, the difference between the link MTU and IP MTU (ip mtu command) must be enough bytes to include for the Layer 2 header.

Link MTU and IP MTU considerations for Port Channels and VLANs are as follows.

Port Channels:

- All members must have the same link MTU value and the same IP MTU value.
- The Port Channel link MTU and IP MTU must be less than or equal to the link MTU and IP MTU values configured on the channel members.

Example: if the members have a link MTU of 2100 and an IP MTU 2000, the Port Channel's MTU values cannot be higher than 2100 for link MTU or 2000 bytes for IP MTU.

VLANs:

- All members of a VLAN must have same IP MTU value.
- Members can have different Link MTU values. Tagged members must have a link MTU 4 bytes higher than untagged members to account for the packet tag.
- The VLAN link MTU and IP MTU must be less than or equal to the link MTU and IP MTU values configured on the VLAN members.

Example: The VLAN contains tagged members with Link MTU of 1522 and IP MTU of 1500 and untagged members with Link MTU of 1518 and IP MTU of 1500. The VLAN's Link MTU cannot be higher than 1518 bytes and its IP MTU cannot be higher than 1500 bytes.

Table 50 lists the various Layer 2 overheads found in FTOS and the number of bytes.

Table 50 Difference between Link MTU and IP MTU

Layer 2 Overhead	Difference between Link MTU and IP MTU
Ethernet (untagged)	18 bytes
VLAN Tag	22 bytes
Untagged Packet with VLAN-Stack Header	22 bytes
Tagged Packet with VLAN-Stack Header	26 bytes

For more information on MTU, refer to Appendix D, Configuring MTU Size.

Related Commands

mtu	Set the link MTU for an Ethernet interface.

ip name-server

Enter up to 6 IP addresses of name servers. The order you enter the addresses determines the order of their use.

Syntax **ip name-server** *ip-address* [*ip-address2...ip-address6*]

To remove a name server, use the **no ip name-server** *ip-address* command.

Parameters

ip-address	Enter the IP address, in dotted decimal format, of the name server to be used.
ip-address2 ... ip-address6	(OPTIONAL) Enter up five more IP addresses, in dotted decimal format, of name servers to be used. Separate the IP addresses with a space.

Defaults No name servers are configured.

Command Modes CONFIGURATION

Usage Information FTOS does not support sending DNS queries over a VLAN. DNS queries are sent out all other interfaces, including the Management port.

ip proxy-arp

Enable Proxy ARP on an interface.

Syntax **ip proxy-arp**

To disable Proxy ARP, enter **no ip proxy-arp**.

Defaults Enabled.

Command Modes INTERFACE

Related Commands

show ip interface	Displays the interface routing status and configuration.

ip redirects

Enable the interface to send ICMP redirect messages.

Syntax **ip redirects**

To return to default, enter **no ip redirects**.

Defaults Disabled

Command Modes INTERFACE

Usage Information This command is available for physical interfaces and port-channel interfaces. Additionally, this command supports VLANs only when the command chassis chassis-mode is set to TeraScale mode.

Note: This command is not supported on default VLAN (default vlan-id command).

ip route

Assign a static route to the E-Series.

Syntax **ip route** *destination mask* {*ip-address* | *interface* [*ip-address*]} [*distance*] [**permanent**] [**tag** *tag-value*]

To delete a specific static route, use the **no ip route** *destination mask* {*address* | *interface* [*ip-address*]} command.

To delete all routes matching a certain route, use the **no ip route** *destination mask* command.

Parameters

destination	Enter the IP address in dotted decimal format of the destination device.
mask	Enter the mask in slash prefix formation (/x) of the destination device's IP address.
ip-address	Enter the IP address in dotted decimal format of the forwarding router.
interface	Enter the following keywords and slot/port or number information: • For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For a loopback interface, enter the keyword **loopback** followed by a number from zero (0) to 16383. • For the null interface, enter the keyword **null** followed by zero (0). • For a Port Channel interface, enter the keyword **port-channel** followed by a number: C-Series Range: 1-128 E-Series Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale. • For a SONET interface, enter the keyword **sonet** followed by the sonet followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information. • For a VLAN, enter the keyword **vlan** followed by a number from 1 to 4094.
distance	(OPTIONAL) Enter a number as the distance metric assigned to the route. Range: 1 to 255
permanent	(OPTIONAL) Enter the keyword **permanent** to specify the route is not removed, even if the interface assigned to that route goes down. The route must be up initially to install it in the routing table. If you disable the interface with an IP address associated with the keyword **permanent**, the route disappears from the routing table.
tag *tag-value*	(OPTIONAL) Enter the keyword **tag** followed by a number to assign to the route. Range: 1 to 4294967295

Defaults Not configured.

Command Modes CONFIGURATION

Usage Information

Using the following example of a static route:
ip route 33.33.33.0 /24 gigabitethernet 0/0 172.31.5.43

- The software installs a next hop that is not on the directly connected subnet but which recursively resolves to a next hop on the interface's configured subnet. In the example, if gig 0/0 has ip address on subnet 2.2.2.0 and if 172.31.5.43 recursively resolves to 2.2.2.0, FTOS installs the static route.
- When interface goes down, FTOS withdraws the route.
- When interface comes up, FTOS re-installs the route.
- When recursive resolution is "broken," FTOS withdraws the route.
- When recursive resolution is satisfied, FTOS re-installs the route.

Related Commands

show ip route	View the E-Series routing table.

ip source-route

Enable the FTOS to forward IP packets with source route information in the header.

Syntax **ip source-route**

To drop packets with source route information, enter **no ip route-source**.

Defaults Enabled.

Command Modes CONFIGURATION

ip unreachables

Enable the generation of Internet Control Message Protocol (ICMP) unreachable messages.

Syntax **ip unreachables**

To disable the generation of ICMP messages, enter **no ip unreachables**.

Defaults Disabled

Command Modes INTERFACE

ip vlan-flooding

Enable unicast data traffic flooding on VLAN member ports.

Syntax **ip vlan-flooding**

To disable, use the **no ip vlan-flooding** command.

Defaults disabled

Command Modes CONFIGURATION

Command History

Version 7.4.1.0	Introduced

Usage Information By default this command is disabled. When enabled, all the Layer 3 unicast routed data traffic going through a VLAN member port is flooded across all the member ports of that VLAN. There might be some ARP table entries which are resolved through ARP packets which had Ethernet MAC SA different from MAC information inside the ARP packet. This unicast data traffic flooding occurs only for those packets which use these ARP entries.

load-balance (C-Series)

C-Series	✓
E-Series	No

By default for C-Series chassis, FTOS uses an IP 4-tuple (IP SA, IP DA, Source Port, and Destination Port) to distribute IP traffic over members of a Port Channel as well as equal-cost paths. To designate another method to balance traffic over Port Channel members, use the **load-balance** command.

Syntax **load-balance {ip-selection [dest-ip | source-ip]} | {mac [dest-mac | source-dest-mac | source-mac]} | {tcp-udp [enable]}**

To return to the default setting (IP 4-tuple), use the **no** version of the command.

Parameters

ip-selection {dest-ip | source-ip}	Enter the keywords to distribute IP traffic based on the following criteria: • **dest-ip**—Uses destination IP address and destination port fields to hash. The hashing mechanism returns a 3-bit index indicating which port the packet should be forwarded to. • **source-ip**—Uses source IP address and source port fields to hash. The hashing mechanism returns a 3-bit index indicating which port the packet should be forwarded to.
mac {dest-mac | source-dest-mac | source-mac}	Enter the keywords to distribute MAC traffic based on the following criteria: • **dest-mac**—Uses the destination MAC address, VLAN, Ethertype, source module ID and source port ID fields to hash. The hashing mechanism returns a 3-bit index indicating which port the packet should be forwarded to. • **source-dest-mac**—Uses the destination and source MAC address, VLAN, Ethertype, source module ID and source port ID fields to hash. The hashing mechanism returns a 3-bit index indicating which port the packet should be forwarded to. • **source-mac**—Uses the source MAC address, VLAN, Ethertype, source module ID and source port ID fields to hash. The hashing mechanism returns a 3-bit index indicating which port the packet should be forwarded to.
tcp-udp enable	Enter the keywords to distribute traffic based on the following: • **enable**—Takes the TCP/UDP source and destination ports into consideration when doing hash computations. (By default, this is **enabled**)

Defaults

IP 4-tuple (IP SA, IP DA, Source Port, Destination Port)

Command Modes

CONFIGURATION

Command History

Version 7.5.1.0	Introduced on C-Series

Usage Information

By default, FTOS distributes incoming traffic based on a hash algorithm using the following criteria:

- IP source address
- IP destination address
- TCP/UDP source port
- TCP/UDP destination port

Related Commands

hash-algorithm (C-Series)	Change the algorithm used to distribute traffic on a C-Series chassis.

load-balance (E-Series)

C-Series	No
E-Series	✓

By default, for E-Series chassis, FTOS uses an IP 5-tuple to distribute IP traffic over members of a Port Channel as well as equal cost paths. To designate another method to balance traffic over Port Channel members, use the **load-balance** command.

Syntax

load-balance [**ip-selection 3-tuple | ip-selection packet-based]** [**mac**]

To return to the default setting (IP 5-tuple), use one of the following commands:

- **no load-balance ip-selection 3-tuple**
- **no load-balance ip-selection packet-based**
- **no load-balance mac**

Parameters

ip-selection 3-tuple	Enter the keywords **ip-selection 3-tuple** to distribute IP traffic based on the following criteria: • IP source address • IP destination address • IP Protocol type **Note:** For IPV6, only the first 32 bits (LSB) of IP SA and IP DA are used for hash generation. Refer to Table 51 for more information.
ip-selection packet-based	Enter the keywords **ip-selection packet-based** to distribute IPV4 traffic based on the IP Identification field in the IPV4 header. This option does *not* affect IPV6 traffic; that is, IPV6 traffic is not distributed when this command is executed. Refer to Table 51 for more information.
mac	Enter the keyword **mac** to distribute traffic based on the following: • MAC source address, and • MAC destination address Refer to Table 51 for more information.

Defaults

IP 5-tuple (IP SA, IP DA, IP Protocol Type, Source Port and Destination Port)

Command Modes

CONFIGURATION

Command History

Version 6.1.1.0	Introduced

Usage Information

By default, FTOS distributes incoming traffic based on a hash algorithm using the following criteria:

- IP source address
- IP destination address
- IP Protocol type

- TCP/UDP source port
- TCP/UDP destination port

Note: For IPV6, only the first 32 bits (LSB) of IP Source Address and IP Destination Address are used for hash generation.

Table 51 lists the load balance command options and how the command combinations effect the distribution of traffic.

Table 51 Configurations of the load-balance Command

Configuration	Switched IP Traffic	Routed IP Traffic (IPV4 Only)	Switched Non-IP Traffic
Default (IP 5-tuple)	IP 5-tuple	IP 5-tuple	MAC based
ip-selection 3-tuple	IP 3-tuple	IP 3-tuple	MAC based
mac	MAC based	IP 5-tuple	MAC based
ip-selection 3-tuple and **mac**	MAC based	IP 3-tuple	MAC based
ip-selection packet-based	Packet based: IPV4 No distribution: IPV6	Packet based: IPV4	MAC based
ip-selection packet-based and mac	MAC based	Packet based: IPV4	MAC based

Related Commands

hash-algorithm (E-Series)	Change the algorithm used to distribute traffic on an E-Series chassis.

management route

Configure a static route that points to the Management interface or a forwarding router.

Syntax **management route** *ip-address mask* {*forwarding-router-address* | **managementEthernet**}

To remove a static route, use the **no management route** *ip-address mask* {*forwarding-router-address* | **managementEthernet**} command.

Parameters

ip-address mask	Enter an IP address (dotted decimal format) and mask (/ prefix format) as the IP address for the Management interface.

forwarding-router-address	Enter an IP address (dotted decimal format) of a forwarding router.
managementEthernet	Enter the keyword **managementEthernet** for the Management interface on the Primary RPM.

Defaults Not configured.

Command Modes CONFIGURATION

Usage Information When a Static (or a Protocol) route overlaps with Management static route, the Static (or Protocol) route is preferred over the Management Static route. Also, Management Static routes and the Management Connected prefix are not reflected in the hardware routing tables.

show arp

View the entries in the ARP table.

Syntax **show arp** [**interface** *interface* | **ip** *ip-address* [*mask*] | **macaddress** *mac-address* [*mac-address mask*]] [**cpu** {**cp** | **rp1** | **rp2**}] [**static** | **dynamic**] [**summary**]

Parameters

cpu	(OPTIONAL) Enter the keyword **cpu** with one of the following keywords to view ARP entries on that CPU: • **cp** - view ARP entries on the control process. • **rp1** - view ARP entries on Routing Processor 1. • **rp2** - view ARP entries on Routing Processor 2.
interface *interface*	(OPTIONAL) Enter the following keywords and slot/port or number information: • For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For the Management interface, enter the keyword **managementethernet** followed by the slot/port information. • For a Port Channel interface, enter the keyword **port-channel** followed by a number: C-Series Range: 1-128 E-Series Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale. • For a SONET interface, enter the keyword **sonet** followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information. • For a VLAN, enter the keyword **vlan** followed by a number from 1 to 4094.
ip *ip-address mask*	(OPTIONAL) Enter the keyword **ip** followed by an IP address in the dotted decimal format. Enter the optional IP address mask in the slash prefix format (/x).
macaddress *mac-address mask*	(OPTIONAL) Enter the keyword **macaddress** followed by a MAC address in nn:nn:nn:nn:nn:nn format. Enter the optional MAC address mask in nn:nn:nn:nn:nn format also.
static	(OPTIONAL) Enter the keyword **static** to view entries entered manually.
dynamic	(OPTIONAL) Enter the keyword **dynamic** to view dynamic entries.
summary	(OPTIONAL) Enter the keyword **summary** to view a summary of ARP entries.

Command Modes EXEC privilege

Example

```
Force10>show arp

Protocol    Address         Age(min)  Hardware Address    Interface  VLAN    CPU
-------------------------------------------------------------------------------
Internet    192.2.1.254           1   00:00:c0:02:01:02   Gi 9/13     -      CP
Internet    192.2.1.253           1   00:00:c0:02:01:02   Gi 9/13     -      CP
Internet    192.2.1.252           1   00:00:c0:02:01:02   Gi 9/13     -      CP
Internet    192.2.1.251           1   00:00:c0:02:01:02   Gi 9/13     -      CP
Internet    192.2.1.250           1   00:00:c0:02:01:02   Gi 9/13     -      CP
Internet    192.2.1.251           1   00:00:c0:02:01:02   Gi 9/13     -      CP
Internet    192.2.1.250           1   00:00:c0:02:01:02   Gi 9/13     -      CP
Internet    192.2.1.249           1   00:00:c0:02:01:02   Gi 9/13     -      CP
Internet    192.2.1.248           1   00:00:c0:02:01:02   Gi 9/13     -      CP
Internet    192.2.1.247           1   00:00:c0:02:01:02   Gi 9/13     -      CP
Internet    192.2.1.246           1   00:00:c0:02:01:02   Gi 9/13     -      CP
Internet    192.2.1.245           1   00:00:c0:02:01:02   Gi 9/13     -      CP
```

Figure 253 show arp Command Example (Partial)

```
Force10#sho arp cpu cp

Protocol    Address         Age(min)  Hardware Address    Interface  VLAN    CPU
-------------------------------------------------------------------------------
Internet    10.1.2.206            0   00:a0:80:00:15:b8   Ma 0/0      -      CP
Internet    182.16.1.20           0   00:30:19:24:2d:70   Gi 8/0      -      CP
Internet    100.10.10.10          0   00:30:19:4f:d3:80   Gi 8/12     -      CP
Internet    10.1.2.209           12   00:a0:80:00:12:6c   Ma 0/0      -      CP
Force10#
```

Figure 254 show arp cpu cp Command Example

Table 52 explains the fields in Figure 253 and Figure 254.

Table 52 show arp Command Example Fields

Row Heading	Description
Protocol	Displays the protocol type.
Address	Displays the IP address of the ARP entry.
Age(min)	Displays the age in minutes of the ARP entry.
Hardware Address	Displays the MAC address associated with the ARP entry.
Interface	Displays the first two letters of the interfaces type and the slot/port associated with the ARP entry.
VLAN	Displays the VLAN ID, if any, associated with the ARP entry.
CPU	Lists which CPU the entries are stored on.

```
Force10# show arp summary

Total Entries    Static Entries   Dynamic Entries  CPU
-------------------------------------------------------
83               0                83               CP
Force10
```

Figure 255 show arp summary Command Example

Table 53 explains the fields in Figure 255.

Table 53 show arp summary Command Example Fields

Row Heading	Description
Total Entries	Lists the total number of ARP entries in the ARP table.
Static Entries	Lists the total number of configured or static ARP entries.
Dynamic Entries	Lists the total number of learned or dynamic ARP entries.
CPU	Lists which CPU the entries are stored on.

show hosts

View the host table and DNS configuration.

Syntax **show hosts**

Command Modes EXEC

EXEC privilege

Example

```
Force10#show hosts
Default domain is not set
Name/address lookup uses static mappings
Name servers are not set
Host                    Flags      TTL    Type   Address
--------                -----      ----   ----   -------
ks                      (perm, OK) -       IP    2.2.2.2
4200-1                  (perm, OK) -       IP    192.68.69.2
1230-3                  (perm, OK) -       IP    192.68.99.2
ZZr                     (perm, OK) -       IP    192.71.18.2
Z10-3                   (perm, OK) -       IP    192.71.23.1
Force10#
```

Figure 256 show hosts Command Example

Table 54 defines the fields in the Figure 256.

Table 54 show hosts Command Example Fields

Field	Description
Default domain...	Displays the domain name (if configured).
Name/address lookup...	States if DNS is enabled on the system. If DNS is enabled, the Name/Address lookup is domain service. If DNS is not enabled, the Name/Address lookup is static mapping.

Table 54 show hosts Command Example Fields (continued)

Field	Description
Name servers are ...	Lists the name servers, if configured.
Host	Displays the host name assigned to the IP address.
Flags	Classifies the entry as one of the following: • perm - the entry was manually configured and will not time out • temp - the entry was learned and will time out after 72 hours of inactivity. Also included in the flag is an indication of the validity of the route: • ok - the entry is valid. • ex - the entry expired. • ?? - the entry is suspect.
TTL	Displays the amount of time until the entry ages out of the cache. For dynamically learnt entries only.
Type	Displays IP as the type of entry.
Address	Displays the IP address(es) assigned to the host.

Related Commands

traceroute	View DNS resolution
ip host	Configure a host.

show ip cam

View CAM entries for a port pipe on a line card.

Syntax **show ip cam linecard** *number* **port-set** *pipe-number* [*ip-address mask* [**longer-prefixes**] | **index** *index-number* | **summary**]

Parameters

number	Enter the number of the line card. Range: 0 to 13 on a E1200, 0 to 6 on a E600, and 0 to 5 on a E300.
pipe-number	Enter the number of the line card's port pipe. Range: 0 to 1
ip-address mask [**longer-prefix**]	(OPTIONAL) Enter the IP address and mask of a route to CAM entries for that route only. Enter the keyword **longer-prefixes** to view routes with a common prefix.
index *index-number*	(OPTIONAL) Enter the keyword **index** followed by the CAM index number. Range: depends on CAM size
summary	(OPTIONAL) Enter the keyword **summary** to view a table listing route prefixes and the total number routes which can be entered in to CAM.

Command Modes EXEC

EXEC privilege

Example 1

```
Force10#show ip cam linecard 13 port-set 0

 Index   Destination    EC CG V C       Next-Hop   VId      Mac-Addr      Port
------ --------------- -- -- - - --------------- ---- ---------------- -------
  3276       6.6.6.2  0  0 1 1       0.0.0.0    0 00:00:00:00:00:00 17c1 CP
  3277       5.5.5.2  0  0 1 1       0.0.0.0    0 00:00:00:00:00:00 17c1 CP
  3278       4.4.4.2  0  0 1 1       0.0.0.0    0 00:00:00:00:00:00 17c1 CP
  3279       3.3.3.2  0  0 1 1       0.0.0.0    0 00:00:00:00:00:00 17c1 CP
  3280       2.2.2.2  0  0 1 1       0.0.0.0    0 00:00:00:00:00:00 17c1 CP
 11144       6.6.6.0  0  0 1 1       0.0.0.0    6 00:00:00:00:00:00 17c5 RP2
 11145       5.5.5.0  0  0 1 1       0.0.0.0    5 00:00:00:00:00:00 17c5 RP2
 11146       4.4.4.0  0  0 1 1       0.0.0.0    4 00:00:00:00:00:00 17c5 RP2
 11147       3.3.3.0  0  0 1 1       0.0.0.0    3 00:00:00:00:00:00 17c5 RP2
 11148       2.2.2.0  0  0 1 1       0.0.0.0    2 00:00:00:00:00:00 17c5 RP2
 65535       0.0.0.0  0  0 1 1       0.0.0.0    0 00:00:00:00:00:00 17c5 RP2
Force10#
```

Figure 257 show ip cam Command Example

Table 55 defines the fields in Figure 257.

Table 55 show ip cam Command Example Fields

Field	Description
Index	Displays the CAM index number of the entry.
Destination	Displays the destination route of the index.
EC	Displays the number of equal cost multipaths (ECMP) available for the default route for non-Jumbo line cards. Displays 0,1 when ECMP is more than 8, for Jumbo line cards.
CG	Displays 0.
V	Displays a 1 if the entry is valid and a 0 if the entry is for a line card with Catalog number beginning with LC-EF.
C	Displays the CPU bit. 1 indicates that a packet hitting this entry is forwarded to the CP or RP2, depending on Egress port.
Next-Hop	Displays the next hop IP address of the entry.
VId	Displays the VLAN ID. If the entry is 0, the entry is not part of a VLAN.
Mac Addr	Displays the next-hop router's MAC address.
Port	Displays the egress interface. Use the second half of the entry to determine the interface. For example, in the entry 17cl CP, the CP is the pertinent portion. CP = control processor RP2 = route processor 2 Gi = Gigabit Ethernet interface So = SONET interface Te = 10 Gigabit Ethernet interface

Example 2

```
Force10#show ip cam linecard 4 port-set 0 summary
 Total Number of Routes in the CAM is 13
 Total Number of Routes which can be entered in CAM is 131072

 Prefix Len Current Use Initial Sz
 ---------- ----------- ----------
   32             7       37994
   31             0        1312
   30             0        3932
   29             0        1312
   28             0        1312
   27             0        1312
   26             0        1312
   25             0        1312
   24             6       40610
   23             0        3932
   22             0        2622
   21             0        2622
   20             0        2622
   19             0        2622
   18             0        1312
   17             0        1312
   16             0        3932
   15             0        1312
   14             0        1312
   13             0        1312
   12             0        1312
   11             0        1312
   10             0        1312
    9             0        1312
    8             0        1312
    7             0        1312
    6             0        1312
    5             0        1312
    4             0        1312
    3             0        1312
    2             0        1312
    1             0        1312
    0             0           8
Force10#
```

Figure 258 show ip cam summary Command Example

Table 56 defines the fields in Figure 258.

Table 56 show ip cam summary Command Example Fields

Field	Description
Prefix Length	Displays the prefix-length or mask for the IP address configured on the linecard 0 port-set 0.
Current Use	Displays the number of routes currently configured for the corresponding prefix or mask on the linecard 0 port-set 0.
Initial Size	Displays the CAM size allocated by FTOS for the corresponding mask. The CAM size is adjusted by FTOS if the number of routes for the mask exceeds the initial allocation.

show ip fib linecard

View all Forwarding Information Base entries.

Syntax **show ip fib linecard** *slot-number* [*ip-address mask* [**longer-prefixes**] | **summary**]

Parameters

slot-number	Enter the number of the line card slot. C-Series Range: 0-7 on the C300 E-Series Range: 0 to 13 on a E1200, 0 to 6 on a E600/E600i, and 0 to 5 on a E300
ip-address mask	(OPTIONAL) Enter the IP address of the network destination to view only information on that destination. You must enter the IP address is dotted decimal format (A.B.C.D). You must enter the mask in slash prefix format (/X).
longer-prefixes	(OPTIONAL) Enter the keyword **longer-prefixes** to view all routes with a common prefix.
summary	(OPTIONAL) Enter the keyword **summary** to view the total number of prefixes in the FIB.

Command Mode EXEC

EXEC privilege

Example

```
Force10>show ip fib linecard 12

 Destination         Gateway                      First-Hop      Mac-Addr          Port    VId  Index E
-------------------- ---------------------------- -------------  ----------------  ------- ---- ------
 3.0.0.0/8           via 100.10.10.10, So 2/8     100.10.10.10   00:01:e8:00:03:ff So 2/8   0   60260
 3.0.0.0/8           via 101.10.10.10, So 2/9
 100.10.10.0/24      Direct, So 2/8               0.0.0.0        00:01:e8:00:03:ff So 2/8   0   11144
 100.10.10.1/32      via 127.0.0.1                127.0.0.1      00:00:00:00:00:00 CP       0    3276
 100.10.10.10/32     via 100.10.10.10, So 2/8     100.10.10.10   00:01:e8:00:03:ff So 2/8   0       0
 101.10.10.0/24      Direct, So 2/9               0.0.0.0        00:00:00:00:00:00 RP2      0   11145
 101.10.10.1/32      via 127.0.0.1                127.0.0.1      00:00:00:00:00:00 CP       0    3277
 101.10.10.10/32     via 101.10.10.10, So 2/9     101.10.10.10   00:01:e8:01:62:32 So 2/9   0       1
Force10>
```

Figure 259 show ip fib linecard Command Example

Table 57 explains the information in Figure 259.

Table 57 show ip fib linecard Command Example Fields

Field	Description
Destination	Lists the destination IP address.
Gateway	Displays either the word `direct` and an interface for a directly connected route or the remote IP address to be used to forward the traffic.
First-Hop	Displays the first hop IP address.
Mac-Addr	Displays the MAC address.
Port	Displays the egress-port information.

Table 57 show ip fib linecard Command Example Fields

Field	Description
VId	Displays the VLAN ID. If no VLAN is assigned, zero (0) is listed.
Index	Displays the internal interface number.
EC	Displays the number of ECMP paths.

Related Commands

clear ip fib linecard	Clear FIB entries on a specified line card..

show ip flow

Show how a Layer 3 packet is forwarded when it arrives at a particular interface.

Syntax

show ip flow interface *interface* {**source-ip** *address* **destination-ip** *address*} {**protocol** [**tcp** | **udp**] | **icmp** | *number*} {**source-port** *number* **destination-port** *number*}

Parameters

interface *interface*	Enter the keyword **interface** followed by of the following interface keywords. • For a Fast Ethernet interface, enter the keyword **FastEthernet** followed by the slot/port information. • For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For a SONET interface, enter the keyword **sonet** followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information. (OPTIONAL) Enter an in or out parameter in conjunction with the optional interface:
source-ip *address*	Enter the keyword **source-ip** followed by the IP source address in IP address format.
destination-ip *address*	Enter the keyword **destination-ip** followed by the IP destination address in IP address format.
protocol [**tcp** | **udp** | **icmp**] | *number*	Enter the keyword **protocol** followed by one of the protocol type keywords: • **tcp** • **udp** • **icmp** *or* • Protocol number.

source-port *number*	Enter the keyword **source-port** followed by the source port number.
destination-port *number*	Enter the keyword **destination-port** followed by the destination port number.

Command Modes EXEC

Usage Information This command provides egress port information for a given IP flow. This is useful in identifying which interface the packet will follow in the case of Port-channel and Equal Cost Multi Paths. Use this command for routed packed only. For switched packets use the **show port-channel-flow** command

Example

```
Force10#show ip flow interface Gi 1/8 189.1.1.1 63.0.0.1 protocol tcp source-port 7898 destination-port\8

   flow: 189.1.1.1 63.0.0.1 protocol 6 7868 8976
   Ingress interface: Gi 1/20
   Egress interface: Gi 1/14 to 1.7.1.2[CAM hit 103710] unfragmented packet
                     Gi 1/10 to 1.2.1.2[CAM hit 103710] fragmented packet
```

Figure 260 show ip flow Command

show ip interface

View IP-related information on all interfaces.

Syntax **show ip interface** [*interface* | **brief** | **linecard** *slot-number*] [**configuration**]

Parameter

interface	(OPTIONAL) Enter the following keywords and slot/port or number information: • For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For a Loopback interface, enter the keyword **Loopback** followed by a number from 0 to 16383. • For the Management interface, enter the keyword **ManagementEthernet** followed by zero (0). • For the Null interface, enter the keyword **null** followed by zero (0). • For a Port Channel interface, enter the keyword **port-channel** followed by a number: C-Series Range: 1-128 E-Series Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale. • For a SONET interface, enter the keyword **sonet** followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information. • For a VLAN, enter the keyword **vlan** followed by a number from 1 to 4094.
brief	(OPTIONAL) Enter the keyword **brief** to view a brief summary of the interfaces and whether an IP address is assigned.

linecard *slot-number*	(OPTIONAL) Enter the keyword **linecard** followed by the number of the line card slot. C-Series Range: 0-7 on the C300 E-Series Range: 0 to 13 on a E1200, 0 to 6 on a E600/E600i, and 0 to 5 on a E300
configuration	(OPTIONAL) Enter the keyword **configuration** to display the physical interfaces with non-default configurations only.

Command Modes

EXEC

EXEC privilege

Example

```
Force10#show ip int te 0/0
TenGigabitEthernet 0/0 is down, line protocol is down
Internet address is not set
IP MTU is 1500 bytes
Inbound  access list is not set
Proxy ARP is enabled
Split Horizon is enabled
Poison Reverse is disabled
ICMP redirects are not sent
ICMP unreachables are not sent


Force10#
```

Figure 261 show ip interface Command Example

Table 58 explains the fields in Figure 262.

Table 58 show ip interface Command Example Items

Lines	Description
TenGigabitEthernet 0/0...	Displays the interface's type, slot/port and physical and line protocol status.
Internet address...	States whether an IP address is assigned to the interface. If one is, that address is displayed.
IP MTU is...	Displays IP MTU value.
Inbound access...	Displays the name of the any configured incoming access list. If none is configured, the phrase "not set" is displayed.
Proxy ARP...	States whether proxy ARP is enabled on the interface.
Split horizon...	States whether split horizon for RIP is enabled on the interface.
Poison Reverse...	States whether poison for RIP is enabled on the interface
ICMP redirects...	States if ICMP redirects are sent.
ICMP unreachables...	States if ICMP unreachable messages are sent.

```
Force10#show ip int brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet 1/0    unassigned      NO  Manual administratively down down
GigabitEthernet 1/1    unassigned      NO  Manual administratively down down
GigabitEthernet 1/2    unassigned      YES Manual up                    up
GigabitEthernet 1/3    unassigned      YES Manual up                    up
GigabitEthernet 1/4    unassigned      YES Manual up                    up
GigabitEthernet 1/5    10.10.10.1      YES Manual up                    up
GigabitEthernet 1/6    unassigned      NO  Manual administratively down down
```

Figure 262 show ip interface brief Command Example (Partial)

Table 59 explains the column headings in Figure 262.

Table 59 show ip interface brief Column Headings

Field	Description
Interface	Displays type of interface and the associated slot and port number.
IP-Address	Displays the IP address for the interface, if configured.
Ok?	Indicates if the hardware is functioning properly.
Method	Displays `Manual` if the configuration is read from the saved configuration.
Status	States whether the interface is enabled (`up`) or disabled (`administratively down`).
Protocol	States whether IP is enabled (`up`) or disabled (`down`) on the interface.

show ip management-route

View the IP addresses assigned to the Management interface.

Syntax **show ip management-route** [**all** | **connected** | **summary** | **static**]

Parameters

all	(OPTIONAL) Enter the keyword **all** to view all IP addresses assigned to all Management interfaces on the E-Series.
connected	(OPTIONAL) Enter the keyword **connected** to view only routes directly connected to the Management interface.
summary	(OPTIONAL) Enter the keyword **summary** to view a table listing the number of active and non-active routes and their sources.
static	(OPTIONAL) Enter the keyword **static** to view non-active routes also.

Command Modes EXEC

EXEC privilege

Example

```
Force10#show ip management-route

Destination         Gateway                      State
-----------         -------                      -----
10.1.2.0/24         ManagementEthernet 0/0       Connected
172.16.1.0/24       10.1.2.4                     Active

Force10#
```

Figure 263 show ip management route Command Example

show ip protocols

View information on all routing protocols enabled and active on the E-Series.

Syntax **show ip protocols**

Command Modes EXEC

EXEC privilege

Example

```
Force10>show ip prot
Routing Protocol is "ospf 1"
  Router ID is 192.68.130.1
  Area              Routing for Networks
  0.0.0.0           192.68.69.2    /24
  0.0.0.0           192.68.99.0    /24
  0.0.0.0           192.68.129.0   /24

Force10>
```

Figure 264 show ip protocols Command Example

show ip route

View information, including how they were learned, about the IP routes on the E-Series.

Syntax **show ip route** [*hostname* | *ip-address* [*mask*] [**longer-prefixes**]] [*protocol* [*process-id* | *routing-tag*]] [**all** | **connected** | **static**]

Parameter

ip-address	(OPTIONAL) Specify a name of a device or the IP address of the device to view more detailed information about the route.
mask	(OPTIONAL) Specify the network mask of the route. Use this parameter with the IP address parameter.

longer-prefixes	(OPTIONAL) Enter the keyword **longer-prefixes** to view all routes with a common prefix.
protocol	(OPTIONAL) Enter the name of a routing protocol (**bgp**, **isis**, **ospf**, **rip**) or the keywords **connected** or **static**. If you enter **bgp,** you can include the BGP *as-number*. If you enter **isis**, you can include the ISIS *routing-tag*. If you enter **ospf**, you can include the OSPF *process-id*.
process-id	(OPTIONAL) Specify that only OSPF routes with a certain process ID must be displayed.
routing-tag	(OPTIONAL) Specify that only ISIS routes with a certain routing tag must be displayed.
connected	(OPTIONAL) Enter the keyword **connected** to view only the directly connected routes.
all	(OPTIONAL) Enter the keyword **all** to view both active and non-active routes. To view a summary of active and non-active routes, use the show ip route summary command.
static	(OPTIONAL) Enter the keyword **static** to view only routes configured by the ip route command.

Command Modes

EXEC

EXEC privilege

Example

```
Force10#show ip route

Codes: C - connected, S - static, R - RIP
       B - BGP, IN - internal BGP, EX - external BGP, LO - Locally Originated
       O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1
       N2 - OSPF NSSA external type 2, E1 - OSPF external type 1
       E2 - OSPF external type 2, i - IS-IS, L1 - IS-IS level-1
       L2 - IS-IS level-2, IA - IS-IS inter area, * - candidate default
       > - non-active route + - summary route

Gateway of last resort is not set

       Destination        Gateway                      Dist/Metric Last Change
       -----------        -------                      ----------- -----------
  R    3.0.0.0/8          via 100.10.10.10, So 2/8           120/1    00:07:12
                          via 101.10.10.10, So 2/9
  C    100.10.10.0/24     Direct, So 2/8                       0/0    00:08:54
> R    100.10.10.0/24     Direct, So 2/8                     120/0    00:08:54
  C    101.10.10.0/24     Direct, So 2/9                       0/0    00:09:15
> R    101.10.10.0/24     Direct, So 2/9                     120/0    00:09:15
Force10>
```

Figure 265 show ip route all Command Example

Table 60 explains the fields in Figure 265.

Table 60 show ip route all Command Example Fields

Field	Description
(undefined)	Identifies the type of route: • C = connected • S = static • R = RIP • B = BGP • IN = internal BGP • EX = external BGP • LO = Locally Originated • O = OSPF • IA = OSPF inter area • N1 = OSPF NSSA external type 1 • N2 = OSPF NSSA external type 2 • E1 = OSPF external type 1 • E2 = OSPF external type 2 • i = IS-IS • L1 = IS-IS level-1 • L2 = IS-IS level-2 • IA = IS-IS inter-area • * = candidate default • > = non-active route • + = summary routes
Destination	Identifies the route's destination IP address.
Gateway	Identifies whether the route is directly connected and on which interface the route is configured.
Dist/Metric	Identifies if the route has a specified distance or metric.
Last Change	Identifies when the route was last changed or configured.

show ip route list

View IP routes in an IP prefix list.

Syntax **show ip route list** *prefix-list*

Parameters

prefix-list	Enter the name of a configured prefix list.

Command Modes EXEC

EXEC privilege

show ip route summary

View a table summarizing the IP routes in the E-Series.

Syntax **show ip route summary**

Command Modes EXEC

EXEC privilege

Example

```
Force10>show ip route summary

Route Source    Active Routes   Non-active Routes
connected       17              0
static          3               0
ospf 100        1368            2
  Intra-area: 762 Inter-area: 1 External-1: 600 External-2: 5
Total           1388            2
Total 1388 active route(s) using 222440 bytes
Total 2 non-active route(s) using 128 bytes
Force10>
```

Figure 266 show ip route summary Command Example

Table 61 explains the column headings in Figure 266.

Table 61 show ip route summary Column Headings

Column Heading	Description
Route Source	Identifies how the route is configured in FTOS.
Active Routes	Identifies the best route if a route is learned from two protocol sources.
Non-active Routes	Identifies the back-up routes when a route is learned by two different protocols. If the best route or active route goes down, the non-active route will become the best route.
ospf 100	If routing protocols (OSPF, RIP) are configured and routes are advertised, then information on those routes is displayed.
Total 1388 active ...	Displays the number of active and non-active routes and the memory usage of those routes. If there are no routes configured in the FTOS, this line does not appear.

Related Commands

show ip route	Display information about the routes found in E-Series.

show ip traffic

View IP, ICMP, UDP, TCP and ARP traffic statistics.

Syntax **show ip traffic** [**all** | **cp** | **rp1** | **rp2**]

Parameters

all	(OPTIONAL) Enter the keyword **all** to view statistics from all processors. If you do not enter a keyword, you also view all statistics from all processors.
cp	(OPTIONAL) Enter the **cp** to view only statistics from the Control Processor.
rp1	(OPTIONAL) Enter the keyword **rp1** to view only the statistics from Route Processor 1.
rp2	(OPTIONAL) Enter the keyword **rp2** to view only the statistics from Route Processor 2.

Command Modes EXEC privilege

Command History

Version 6.5.1.0	F10 Monitoring MIB available for ip traffic statistics

Example

```
Force10#Force10#show ip traffic
Control Processor IP Traffic:

IP statistics:
 Rcvd: 23857 total, 23829 local destination
    0 format errors, 0 checksum errors, 0 bad hop count
    0 unknown protocol, 0 not a gateway
    0 security failures, 0 bad options
 Frags: 0 reassembled, 0 timeouts, 0 too big
     0 fragmented, 0 couldn't fragment
 Bcast: 28 received, 0 sent; Mcast: 0 received, 0 sent
 Sent: 16048 generated, 0 forwarded
    21 encapsulation failed, 0 no route
ICMP statistics:
 Rcvd: 0 format errors, 0 checksum errors, 0 redirects, 0 unreachable
    0 echo, 0 echo reply, 0 mask requests, 0 mask replies, 0 quench
    0 parameter, 0 timestamp, 0 info request, 0 other
 Sent: 0 redirects, 0 unreachable, 0 echo, 0 echo reply
    0 mask requests, 0 mask replies, 0 quench, 0 timestamp
    0 info reply, 0 time exceeded, 0 parameter problem
UDP statistics:
 Rcvd: 0 total, 0 checksum errors, 0 no port
    0 short packets, 0 bad length, 0 no port broadcasts, 0 socket full
 Sent: 0 total, 0 forwarded broadcasts
TCP statistics:
 Rcvd: 23829 total, 0 checksum errors, 0 no port
 Sent: 16048 total
ARP statistics:
 Rcvd: 156 requests, 11 replies
 Sent: 21 requests, 10 replies (0 proxy)
Routing Processor1 IP Traffic:

...
```

Figure 267 show ip traffic Command Example (partial)

Table 61 defines some of the output in Figure 267.

Table 62 show ip traffic output definitions

Keyword	Definition
unknown protocol...	No receiver for these packets. Counts those packets whose protocol type field is not recognized by FTOS.
not a gateway...	Packets can not be routed; host/network is unreachable.
security failures...	Counts the number of received unicast/multicast packets that could not be forwarded due to: • route not found for unicast/multicast; ingress interfaces do not belong to the destination multicast group • destination IP address belongs to reserved prefixes; host/network unreachable
bad options...	Unrecognized IP option on a received packet.
Frags:	IP fragments received.
... reassembled	Number of IP fragments that were reassembled.
... timeouts	Number of times a timer expired on a reassembled queue.
... too big	Number of invalid IP fragments received.
... couldn't fragment	Number of packets that could not be fragmented and forwarded.
...encapsulation failed	Counts those packets which could not be forwarded due to ARP resolution failure. FTOS sends an arp request prior to forwarding an IP packet. If a reply is not received, FTOS repeats the request three times. These packets are counted in encapsulation failed.
Rcvd:	
...short packets	The number of bytes in the packet are too small.
...bad length	The length of the packet was not correct.
...no port broadcasts	The incoming broadcast/multicast packet did not have any listener.
...socket full	The applications buffer was full and the incoming packet had to be dropped.

Usage Information

The F10 Monitoring MIB provides access to the statistics described in Table 63.

Table 63 F10 Monitoring MIB

Command Display	Object	OIDs
IP statistics:		
Bcast:		
Received	f10BcastPktRecv	1.3.6.1.4.1.6027.3.3.5.1.1
Sent	f10BcastPktSent	1.3.6.1.4.1.6027.3.3.5.1.2
Mcast:		
Received	f10McastPktRecv	1.3.6.1.4.1.6027.3.3.5.1.3
Sent	f10McastPktSent	1.3.6.1.4.1.6027.3.3.5.1.4
ARP statistics:		
Rcvd:		

Table 63 F10 Monitoring MIB

Command Display	Object	OIDs
Request	f10ArpReqRecv	1.3.6.1.4.1.6027.3.3.5.2.1
Replies	f10ArpReplyRecv	1.3.6.1.4.1.6027.3.3.5.2.3
Sent:		
Request	f10ArpReqSent	1.3.6.1.4.1.6027.3.3.5.2.2
Replies	f10ArpReplySent	1.3.6.1.4.1.6027.3.3.5.2.4
Proxy	f10ArpProxySent	1.3.6.1.4.1.6027.3.3.5.2.5

show protocol-termination-table

C-Series	**No**
E-Series	✓

Display the IP Packet Termination Table (IPPTT).

Syntax **show protocol-termination-table linecard** *number* **port-set** *Port pipe-number*

Parameters

linecard *number*	Enter the keyword **linecard** followed by slot number of the line card. C-Series Range: 0-7 on the C300 E-Series Range: 0 to 13 on a E1200, 0 to 6 on a E600/E600i, and 0 to 5 on a E300
port-set *Port pipe-number*	Enter the keyword **port-set** followed by the line card's port pipe number. Range: 0 to 1

Defaults No default behavior or values

Command Modes EXEC

EXEC privilege

Command History

Version 6.4.1.0	Introduced

Example

```
Force10#show protocol-termination-table linecard 2 port-set 0
Index   Protocol   Src-Port   Dst-Port   Queue   DP   Blk-Hole   VlanCPU     EgPort
-----   --------   --------   --------   -----   --   --------   ----------  ------
0       ICMP       any        any        Q0      0    No         -           CP
1       UDP        any        1812       Q7      6    No         -           CP
2       UDP        any        68         Q7      6    No         -           CP
3       UDP        any        67         Q7      6    No         -           CP
4       TCP        any        22         Q7      6    No         -           CP
5       TCP        22         any        Q7      6    No         -           CP
6       TCP        639        any        Q7      6    No         -           RP2
7       TCP        any        639        Q7      6    No         -           RP2
8       TCP        646        any        Q7      6    No         -           RP1
9       TCP        any        646        Q7      6    No         -           RP1
10      UDP        646        any        Q7      6    No         -           RP1
11      UDP        any        646        Q7      6    No         -           RP1
12      TCP        23         any        Q7      6    No         -           CP
13      TCP        any        23         Q7      6    No         -           CP
14      UDP        any        123        Q7      6    No         -           CP
15      TCP        any        21         Q7      6    No         -           CP
16      TCP        any        20         Q7      6    No         -           CP
17      UDP        any        21         Q7      6    No         -           CP
18      UDP        any        20         Q7      6    No         -           CP
19      TCP        21         any        Q7      6    No         -           CP
20      TCP        20         any        Q7      6    No         -           CP
21      UDP        21         any        Q7      6    No         -           CP
22      UDP        20         any        Q7      6    No         -           CP
23      UDP        any        69         Q7      6    No         -           CP
24      UDP        69         any        Q7      6    No         -           CP
25      TCP        any        161        Q7      6    No         -           CP
26      TCP        161        any        Q7      6    No         -           CP
27      TCP        162        any        Q7      6    No         -           CP
28      TCP        any        162        Q7      6    No         -           CP
29      UDP        any        161        Q7      6    No         -           CP
30      UDP        161        any        Q7      6    No         -           CP
31      UDP        any        162        Q7      6    No         -           CP
32      UDP        162        any        Q7      6    No         -           CP
33      PIM-SM     any        any        Q6      0    No         -           RP2
34      IGMP       any        any        Q7      6    No         -           RP2
35      OSPF       any        any        Q7      6    No         -           RP1
```

Usage Information

The IPPTT table is used for looking up forwarding information for IP control traffic destined to the router. For the listed control traffic types, IPPTT contains the information for the following:

- Which CPU to send the traffic (CP, RP1, or RP2)
- What QoS parameters to set

Related Commands

show ip cam	Display the CAM table

show tcp statistics

View information on TCP traffic through the E-Series.

Syntax **show tcp statistics** {**all** | **cp** | **rp1** | **rp2**}

Parameters

all	Enter the keyword **all** to view all TCP information.
cp	Enter the keyword **cp** to view only TCP information from the Control Processor.
rp1	Enter the keyword **rp1** to view only TCP statistics from Route Processor 1.
rp2	Enter the keyword **rp2** to view only TCP statistics from Route Processor 2.

Command Modes EXEC privilege

Example

```
Force10#show tcp stat cp

Control Processor TCP:
Rcvd: 10585 Total, 0 no port
   0 checksum error, 0 bad offset, 0 too short
   329 packets (1263 bytes) in sequence
   17 dup packets (6 bytes)
   0 partially dup packets (0 bytes)
   7 out-of-order packets (0 bytes)
   0 packets ( 0 bytes) with data after window
   0 packets after close
   0 window probe packets, 41 window update packets
   41 dup ack packets, 0 ack packets with unsend data
   10184 ack packets (12439508 bytes)
Sent: 12007 Total, 0 urgent packets
   25 control packets (including 24 retransmitted)
   11603 data packets (12439677 bytes)
   24 data packets (7638 bytes) retransmitted
   355 ack only packets (41 delayed)
   0 window probe packets, 0 window update packets
7 Connections initiated, 8 connections accepted, 15 connections established
14 Connections closed (including 0 dropped, 0 embryonic dropped)
20 Total rxmt timeout, 0 connections dropped in rxmt timeout
0 Keepalive timeout, 0 keepalive probe, 0 Connections dropped in keepalive
Force10#
```

Figure 268 show tcp statistics cp Command Example

explains the fields in

Table 64 explains the fields in Figure 268.

Table 64 show tcp statistics cp Command Example Fields

Field	Description
Rcvd:	Displays the number and types of TCP packets received by the E-Series. • Total = total packets received • no port = number of packets received with no designated port.
0 checksum error...	Displays the number of packets received with the following: • checksum errors • bad offset to data • too short
329 packets ...	Displays the number of packets and bytes received in sequence.
17 dup ...	Displays the number of duplicate packets and bytes received.
0 partially ...	Displays the number of partially duplicated packets and bytes received.
7 out-of-order...	Displays the number of packets and bytes received out of order.
0 packets with data after window	Displays the number of packets and bytes received that exceed the E-Series's window size.

Table 64 show tcp statistics cp Command Example Fields (continued)

Field	Description
0 packets after close	Displays the number of packet received after the TCP connection was closed.
0 window probe packets ...	Displays the number of window probe and update packets received.
41 dup ack...	Displays the number of duplicate acknowledgement packets and acknowledgement packets with data received.
10184 ack ...	Displays the number of acknowledgement packets and bytes received.
Sent:	Displays the total number of TCP packets sent and the number of urgent packets sent.
25 control packets...	Displays the number of control packets sent and the number retransmitted.
11603 data packets...	Displays the number of data packets sent.
24 data packets retransmitted	Displays the number of data packets resent.
355 ack...	Displays the number of acknowledgement packets sent and the number of packet delayed.
0 window probe...	Displays the number of window probe and update packets sent.
7 Connections initiated ...	Displays the number of TCP connections initiated, accepted, and established.
14 Connections closed ...	Displays the number of TCP connections closed, dropped.
20 Total rxmt...	Displays the number of times the E-Series tried to resend data and the number of connections dropped during the TCP retransmit timeout period.
0 Keepalive	Lists the number of keepalive packets in timeout, the number keepalive probes and the number of TCP connections dropped during keepalive.

Chapter 29 Policy-based Routing

C-Series	NO
E-Series	✓

Platform Specific Feature: Policy-based Routing is supported on the E-Series only.

Policy-based Routing (PBR) enables you to apply routing policies to specific interfaces. To enable PBR, a redirect list is created and then applied to the interface. Once the redirect list is applied to the interface, all traffic passing through is subject to the rules defined in the redirect list.

PBR can be applied to physical interfaces and logical interfaces (such as LAG or VLAN). Trace lists and Redirect lists do not function correctly when both are configured in the same configuration.

Note: Apply Policy-based Routing to Layer 3 interfaces only.

Policy-based routing includes the following commands:

- ip redirect-group on page 770
- ip redirect-list on page 771
- permit on page 771
- redirect on page 773
- seq on page 774
- show cam pbr on page 775
- show ip redirect-list on page 777

ip redirect-group

C-Series	No
E-Series	✓

Apply a redirect list (policy-based routing) on an interface. You can apply multiple redirect lists to an interface by entering this command multiple times.

Syntax

ip redirect-group *redirect-list-name*

To remove a redirect list from an interface, use the **no ip redirect-group** *name* command.

Parameters

redirect-list-name	Enter the name of a configured Redirect list.

Defaults

No default behavior or values

Command Modes

INTERFACE (conf-if-vl-)

Command History

Version 7.4.2.0	Added support for LAG and VLAN interfaces
Version 6.5.3.0	Introduced

Usage Information

Any number of redirect-groups can be applied to an interface. A redirect list can contain any number of configured rules. These rules includes the next-hop IP address where the incoming traffic is to be redirected.

If the next hop address is reachable, traffic is forwarded to the specified next hop. Otherwise the normal routing table is used to forward traffic. When a redirect-group is applied to an interface and the next-hop is reachable, the rules are added into the PBR CAM region. When incoming traffic hits an entry in the CAM, the traffic is redirected to the corresponding next-hop IP address specified in the rule.

Note: Apply redirect list to Physical, VLAN, or LAG interfaces only.

Related Commands

show cam pbr	Display the content of the PBR CAM.
show ip redirect-list	Display the redirect-list configuration.

ip redirect-list

C-Series	No
E-Series	✓

Configure a redirect list and enter the REDIRECT-LIST mode.

Syntax **ip-redirect-list** *redirect-list-name*

To remove a redirect list, enter **no ip redirect-list**.

Parameters

redirect-list-name	Enter the name of a redirect list.

Defaults No default behavior or values

Command Modes CONFIGURATION

Command History

Version 6.5.3.0	Introduced

permit

C-Series	No
E-Series	✓

Configure a rule for the redirect list.

Syntax **permit** {*ip-protocol-number* | *protocol-type* } {*source mask* | **any** | **host** *ip-address*} {*destination mask* | **any** | **host** *ip-address*} [*bit*] [*operators*]

To remove the rule, use one of the following:

- use the **no seq** *sequence-number* command syntax if you know the filter sequence number.
- use the no **permit** {*ip-protocol-number* | *protocol-type* } {*source mask* | **any** | **host** *ip-address*} {*destination mask* | **any** | **host** *ip-address*} [*bit*] [*operators*]

Parameters

ip-protocol-number	Enter a number from 0 to 255 for the protocol identified in the IP protocol header.
protocol-type	Enter one of the following keywords as the protocol type: • **icmp** for Internet Control Message Protocol • **ip** for Any Internet Protocol • **tcp** for Transmission Control Protocol • **udp** for User Datagram Protocol
source	Enter the IP address of the network or host from which the packets were sent.
mask	Enter a network mask in /prefix format (/x).
any	Enter the keyword **any** to specify that all traffic is subject to the filter.
host *ip-address*	Enter the keyword **host** followed by the IP address to specify a host IP address.
destination	Enter the IP address of the network or host to which the packets are sent.
bit	(OPTIONAL) For TCP protocol type only, enter one or a combination of the following TCP flags: • **ack** = acknowledgement • **fin** = finish (no more data from the user) • **psh** = push function • **rst** = reset the connection • **syn** = synchronize sequence number • **urg** = urgent field
operator	(OPTIONAL) For TCP and UDP parameters only. Enter one of the following logical operand: • **eq** = equal to • **neq** = not equal to • **gt** = greater than • **lt** = less than • **range** = inclusive range of ports (you must specify two ports for the *port* command parameter.)

Defaults No default behavior or values

Command Modes REDIRECT-LIST

Command History

Version 7.5.1.0	Introduced

redirect

C-Series	No
E-Series	✓

Configure a rule for the redirect list.

Syntax

redirect {*ip-address* | **sonet** *slot/port*} {*ip-protocol-number* | *protocol-type* [*bit*]} {*source mask* | **any** | **host** *ip-address*} {*destination mask* | **any** | **host** *ip-address*} [*operator*]

To remove this filter, use one of the following:

- use the **no seq** *sequence-number* command syntax if you know the filter's sequence number.
- use the **no redirect** {*ip-address* | **sonet** *slot/port*} {*ip-protocol-number* [*bit*] | *protocol-type*} {*source mask* | **any** | **host** *ip-address*} {*destination mask* | **any** | **host** *ip-address*} [*operator*]

Parameters

ip-address	Enter the IP address of the forwarding router.
sonet *slot/port*	Enter the keyword **sonet** followed by the slot/port information.
ip-protocol-number	Enter a number from 0 to 255 for the protocol identified in the IP protocol header.
protocol-type	Enter one of the following keywords as the protocol type: • **icmp** for Internet Control Message Protocol • **ip** for Any Internet Protocol • **tcp** for Transmission Control Protocol • **udp** for User Datagram Protocol
bit	(OPTIONAL) For TCP protocol type only, enter one or a combination of the following TCP flags: • **ack** = acknowledgement • **fin** = finish (no more data from the user) • **psh** = push function • **rst** = reset the connection • **syn** = synchronize sequence number • **urg** = urgent field
source	Enter the IP address of the network or host from which the packets were sent.
mask	Enter a network mask in /prefix format (/x).
any	Enter the keyword **any** to specify that all traffic is subject to the filter.
host *ip-address*	Enter the keyword **host** followed by the IP address to specify a host IP address.

destination	Enter the IP address of the network or host to which the packets are sent.
operator	(OPTIONAL) For TCP and UDP parameters only. Enter one of the following logical operand: • **eq** = equal to • **neq** = not equal to • **gt** = greater than • **lt** = less than • **range** = inclusive range of ports (you must specify two ports for the *port* command parameter.)

Defaults No default behavior or values

Command Modes REDIRECT-LIST

Command History

Version 7.4.1.0	Added the bit variable for TCP protocols only

seq

C-Series	No
E-Series	✓

Configure a filter with an assigned sequence number for the redirect list.

Syntax **seq** *sequence-number* {**permit** | **redirect** {*ip-address* | **sonet** *slot/port*}} {*ip-protocol-number* | *protocol-type*} {*source mask* | **any** | **host** *ip-address*} {*destination mask* | **any** | **host** *ip-address*}[bit] [*operator*]

To delete a filter, use the **no seq** *sequence-number* command.

Parameters

sequence-number	Enter a number from 1 to 65535.
permit	Enter the keyword **permit** assign the sequence to the permit list.
redirect	Enter the keyword **redirect** to assign the sequence to the redirect list.
ip-address	Enter the IP address of the forwarding router.
sonet *slot/port*	Enter the keyword **sonet** followed by the slot/port information.
ip-protocol-number	Enter a number from 0 to 255 for the protocol identified in the IP protocol header.
protocol-type	Enter one of the following keywords as the protocol type: • **icmp** for Internet Control Message Protocol • **ip** for Any Internet Protocol • **tcp** for Transmission Control Protocol • **udp** for User Datagram Protocol

source	Enter the IP address of the network or host from which the packets were sent.
mask	Enter a network mask in /prefix format (/x).
any	Enter the keyword **any** to specify that all traffic is subject to the filter.
host *ip-address*	Enter the keyword **host** followed by the IP address to specify a host IP address.
destination	Enter the IP address of the network or host to which the packets are sent.
bit	(OPTIONAL) For TCP protocol type only, enter one or a combination of the following TCP flags: • **ack** = acknowledgement • **fin** = finish (no more data from the user) • **psh** = push function • **rst** = reset the connection • **syn** = synchronize sequence number • **urg** = urgent field
operator	(OPTIONAL) For TCP and UDP parameters only. Enter one of the following logical operand: • **eq** = equal to • **neq** = not equal to • **gt** = greater than • **lt** = less than • **range** = inclusive range of ports (you must specify two ports for the *port* command parameter.)

Defaults No default behavior or values

Command Modes REDIRECT-LIST

Command History

Version 7.5.1.0	Added the bit variable and Permit and Redirect

show cam pbr

C-Series	No
E-Series	✓

Display the PBR CAM content.

Syntax **show cam pbr** {[**interface** *interface*] | **linecard** *slot-number* **port-set** *number*]} [**summary**]

Parameters

interface *interface*	Enter the keyword **interface** followed by the name of the interface. The interface can be a physical interface or VLAN interface with *vlan-id*.
linecard *slot-number*	Enter the keyword **linecard** followed the slot number. Range: 0 to 13 for the E1200, 0 to 6 for the E600/E600i, 0 to 5 for the E300
port-set *number*	Enter the keyword **port-set** followed the port-pipe number. Range: 0 to 1
summary	Enter the keyword **summary** to view only the total number of CAM entries.

Defaults

No default values or behavior

Command Modes

EXEC

Command History

Version 7.4.1.0	Introduced

Example

```
Force10#show cam pbr interface vlan 10

 Cam    Port VlanID Proto Tcp   Src   Dst   SrcIp           DstIp     Next-hop          Egress
Index                    Flag  Port  Port                            MAC               Port
-------------------------------------------------------------------------------------------
15296 -     10     TCP   0x10  0     0     155.55.1.0/24   0.0.0.0/0 00:00:00:00:01:02 5/4
15297 -     10     TCP   0x11  0     0     155.55.1.0/24   0.0.0.0/0 00:00:00:00:01:03 Po 5
15298 -     10     TCP   0x11  0     0     144.44.1.0/24   0.0.0.0/0 00:00:00:00:01:04 Vl 10(10/2)
15299 -     10     TCP   0x10  0     0     111.55.1.0/24   1.1.1.1/8 00:00:00:00:01:05 Vl 11(Po 5)
Force10#
```

Figure 269 show cam pbr interface vlan Command

Example

```
Force10#Force10#show cam pbr linecard 2 p 0

TCP Flag: Bit 5 - URG, Bit 4 - ACK, Bit 3 - PSH, Bit 2 - RST, Bit 1 - SYN, Bit 0 - FIN

Cam    Port VlanID Proto Tcp   Src   Dst   SrcIp             DstIp             Next-hop          Egress
Index                    Flag  Port  Port                                      MAC               Port
-------------------------------------------------------------------------------------------------------
.
.
.
15230 _     10     TCP   0x10  0     0     100.55.1.0/24     182.16.1.1/24     N/A               N/A

Force10#
```

Figure 270 show cam pbr linecard 2 port-set 0 Command

Note: In Figure 270, the rule with 15230 Cam Index is the Permit rule. The Next-hop MAC and Egress Port are always N/A for permit rules.

Usage Information

The **show cam pbr** command displays the PBR CAM content. The "VlanID" column displays the corresponding VLAN ID to which the redirect-group is applied.

Related Commands

ip redirect-group	Apply a redirect group to an interface.
show ip redirect-list	Display the redirect-list configuration.
show cam-usage	Display the CAM usage on ACL, router, or switch.

show ip redirect-list

C-Series	No
E-Series	✓

View the redirect list configuration and the interfaces it is applied to.

Syntax **show ip redirect-list** *redirect-list-name*

Parameters

redirect-list-name	Enter the name of a configured Redirect list.

Command Modes EXEC

EXEC privilege

Example

```
Force10#show ip redirect-list test_sonet

IP redirect-list rcl0:
 Defined as:
  seq 5 permit ip any host 182.16.2.10
  seq 10 redirect 182.16.1.2 ip any any, Next-hop un-reachable, ARP un-resolved
 Applied interfaces:
  Gi 9/0
  So 8/2
  Vl 10
  Po 3
Force10#
```

Figure 271 show ip redirect-list Command Example

Chapter 30 Far-End Failure Detection

C-Series	NO
E-Series	✓

Platform Specific Feature: Policy-based Routing is supported on the E-Series only.

The FTOS supports Far-End Failure Detection (FEFD) on Ethernet interfaces. This feature detects and reports far-end link failures.

- FEFD is not supported on the Management interface.
- By default, FEFD is disabled.

The FEFD commands are:

- debug fefd on page 779
- fefd on page 780
- fefd-global on page 781
- fefd disable on page 781
- fefd interval on page 782
- fefd-global interval on page 782
- fefd reset on page 783
- show fefd on page 783

debug fefd

C-Series	No
E-Series	✓

Enable debugging of FEFD.

Syntax **debug fefd** {**events** | **packets**} [*interface*]

To disable debugging of FEFD, use the **no debug fefd** {**events** | **packets**} [*interface*] command syntax.

Parameters

events	Enter the keyword **events** to enable debugging of FEFD state changes.
packets	Enter the keyword **packets** to enable debugging of FEFD to view information on packets sent and received.
interface	(OPTIONAL) Enter the following keywords and slot/port or number information: • For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For a SONET interface, enter the keyword **sonet** followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information.

Command Modes EXEC privilege

fefd

C-Series	**No**
E-Series	✓

Enable Far-End Failure Detection on an interface.

Syntax **fefd** [**mode** {**normal** | **aggresive**}]

To disable FEFD on an interface, enter **no fefd mode**.

Parameters

mode normal	(OPTIONAL) Enter the keywords **mode normal** to change the link state to "unknown" when a far-end failure is detected by the software on that interface. When the interface is placed in "unknown" state, the software brings down the line protocol. Default: mode normal
mode aggressive	(OPTIONAL) Enter the keyword **mode aggressive** to change the link state to "error-disabled" when a far-end failure is detected by the software on that interface. When an interface is placed in "error-disabled" state, you must enter the fefd reset command to reset the interface state.

Defaults Disabled.

Command Modes INTERFACE

Usage Information When you enter no fefd mode for an interface and fefd-global, FEFD is enabled on the interface because the no fefd mode command is not retained in the configuration file. To keep the interface FEFD disabled when the global configuration changes, use the fefd disable command.

fefd-global

C-Series	No
E-Series	✓

Enable FEFD globally on the system.

Syntax **fefd-global** [**mode** {**normal** | **aggresive**}]

To disable FEFD globally, use the **no fefd-global** [**mode** {**normal** | **aggresive**}] command syntax.

Parameters

mode normal	(OPTIONAL) Enter the keywords **mode normal** to change the link state to "unknown" when a far-end failure is detected by the software on that interface. When the interface is placed in "unknown" state, the software brings down the line protocol. Normal mode is the default.
mode aggressive	(OPTIONAL) Enter the keyword **mode aggressive** to change the link state to "error-disabled" when a far-end failure is detected by the software on that interface. When an interface is placed in "error-disabled" state, you must enter the fefd reset command to reset the interface state.

Defaults Disabled.

Command Modes CONFIGURATION

Usage Information If you enter only the **fefd-global** syntax, the mode is normal and the default interval is 15 seconds.

If you disable FEFD globally (**no fefd-global**), the system does not remove the FEFD interface configuration.

fefd disable

C-Series	No
E-Series	✓

Disable FEFD on an interface only. This command overrides the fefd-global command for the interface.

Syntax **fefd disable**

To re-enable FEFD on an interface, enter **no fefd disable**.

Default Not configured.

Command Modes INTERFACE

fefd interval

C-Series	No
E-Series	✓

Set an interval between control packets.

Syntax **fefd interval** *seconds*

To return to the default value, enter **no fefd interval**.

Parameters

seconds	Enter a number as the time between FEFD control packets. Range: 3 to 300 seconds Default: 15 seconds

Defaults 15 seconds

Command Modes INTERFACE

fefd-global interval

C-Series	No
E-Series	✓

Configure an interval between FEFD control packets.

Syntax **fefd-global interval** *seconds*

To return to the default value, enter **no fefd-global interval**.

Parameters

seconds	Enter a number as the time between FEFD control packets. Range: 3 to 300 seconds Default: 15 seconds

Defaults 15 seconds

Command Modes CONFIGURATION

fefd reset

C-Series	No
E-Series	✓

Reset all interfaces or a singe interface that was in “error-disabled” mode.

Syntax **fefd reset** [*interface*]

Parameters

interface	(OPTIONAL) Enter the following keywords and slot/port or number information: • For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For a SONET interface, enter the keyword **sonet** followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information.

Defaults Not configured.

Command Modes EXEC privilege

show fefd

C-Series	No
E-Series	✓

View FEFD status globally or on a specific interface.

Syntax **show fefd** [*interface*]

Parameters

interface	(OPTIONAL) Enter the following keywords and slot/port or number information: • For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For a SONET interface, enter the keyword **sonet** followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information.

Command Modes

EXEC

EXEC privilege

Example

```
Force10#sh fefd
FEFD is globally 'ON', interval is 10 seconds, mode is 'Aggressive'.

INTERFACE      MODE           INTERVAL       STATE
                              (second)
Gi 5/0         Aggressive     10             Admin Shutdown
Gi 5/1         Aggressive     10             Admin Shutdown
Gi 5/2         Aggressive     10             Admin Shutdown
Gi 5/3         Aggressive     10             Admin Shutdown
Gi 5/4         Aggressive     10             Admin Shutdown
Gi 5/5         Aggressive     10             Admin Shutdown
Gi 5/6         Aggressive     10             Admin Shutdown
Gi 5/7         Aggressive     10             Admin Shutdown
Gi 5/8         Aggressive     10             Admin Shutdown
Gi 5/9         Aggressive     10             Admin Shutdown
Gi 5/10        NA             NA             Locally disabled
Gi 5/11        Aggressive     10             Err-disabled
Force10#
```

Figure 272 show fefd Command Example

Table 65 describes the information in Figure 272.

Table 65 show fefd display details

Field	Description
Interface	Displays the interfaces type and number.
Mode	Displays the mode (aggressive or normal) or NA if the interface contains fefd disable in its configuration.
Interval	Displays the interval between FEFD packets.
State	Displays the the state of the interface and can be one of the following: • bi-directional (interface is up and connected and seeing neighbor's echos) • err-disabled (only found when the FEFD mode is aggressive and when the interface has not seen its neighbor's echos for 3 times the message interval. To reset an interface in this state, use the fefd reset command.) • unknown (only found when FEFD mode is normal • locally disabled (interface contains the fefd disable command in its configuration) • Admin Shutdown (interface is disabled with the shutdown command)

Chapter 31 VRRP Commands

Use the commands in this chapter to configure and enable Virtual Router Redundany Protocol ((VRRP).

To enter the VRRP mode on an interface, use the vrrp-group command at the INTERFACE mode. The interface must be in Layer 3 mode (that is, you cannot have the switchport command configured on the interface). You can configure up to 12 VRRP groups on one interface.

- advertise-interval on page 785
- authentication-type on page 786
- clear counters vrrp on page 787
- debug vrrp on page 787
- description on page 788
- disable on page 788
- hold-time on page 789
- preempt on page 789
- priority on page 790
- show config on page 790
- show vrrp on page 791
- track on page 793
- virtual-address on page 794
- vrrp-group on page 795

advertise-interval

Set the time interval between VRRP advertisements.

Syntax **advertise-interval** *seconds*

To return to the default settings, enter **no advertise-interval**.

Parameters

seconds	Enter a number of seconds. Range: 1 to 255. Default: 1 second.

Defaults 1 second.

Command Modes VRRP

Usage Information Force10 Networks recommends that you keep the default setting for this command. If you do change the time interval between VRRP advertisements on one router, you must change it on all routers.

authentication-type

Enable authentication of VRRP data exchanges.

Syntax **authentication-type simple** [*encryption-type*] *password*

To delete an authentication type and password, enter **no authentication-type**.

Parameters

simple	Enter the keyword **simple** to specify simple authentication.
encryption-type	(OPTIONAL) Enter one of the following numbers: • 0 (zero) for an unecrypted (clear text) password • 7 (seven) for hidden text password.
password	Enter a character string up to 8 characters long as a password. If you do not enter an encryption-type, the password is stored as clear text.

Defaults Not configured.

Command Modes VRRP

Usage Information The password is displayed in the show config output if the encryption-type is unencrypted or clear text. If you choose to encrypt the password, the show config displays an encrypted text string.

clear counters vrrp

Clear the counters maintained on VRRP operations.

Syntax **clear counters vrrp** [*vrrp-id*]

Parameters

vrrp-id	(OPTIONAL) Enter the number of the VRRP group ID. Range: 1 to 255

Command Modes EXEC privilege

debug vrrp

Allows you to enable debugging of VRRP.

Syntax **debug vrrp** *interface* [*vrrp-id*] {**all** | **packets** | **state** | **timer**}

To disable debugging, use the **no debug vrrp** *interface* [*vrrp-id*] {**all** | **packets** | **state** | **timer**} command.

Parameters

interface	Enter the following keywords and slot/port or number information: • For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For Port Channel interface types, enter the keyword **port-channel** followed by the number: C-Series Range: 1-128 on the C300 E-Series Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information. • For a VLAN interface, enter the keyword **vlan** followed by the VLAN ID. The VLAN ID range is from 1 to 4094.
vrrp-id	(OPTIONAL) Enter a number from 1 to 255 as the VRRP group ID.
all	Enter the keyword **all** to enable debugging of all VRRP groups.
packets	Enter the keyword **packets** to enable debugging of VRRP control packets.
state	Enter the keyword **state** to enable debugging of VRRP state changes.
timer	Enter the keyword **timer** to enable debugging of the VRRP timer.

Command Modes EXEC privilege

Usage Information If no options are specified, debug is active on all interfaces and all VRRP groups.

description

Configure a short text string describing the VRRP group.

Syntax **description** *text*

To delete a VRRP group description, enter **no description**.

Parameters

text	Enter a text string up to 80 characters long.

Defaults Not enabled.

Command Modes VRRP

disable

Disable a VRRP group.

Syntax **disable**

To re-enable a disabled VRRP group, enter **no disable**.

Defaults VRRP is enabled.

Command Modes VRRP

Usage Information To enable VRRP traffic, assign an IP address to the VRRP group using the virtual-address command and enter **no disable**.

Related Commands

virtual-address	Specify the IP address of the Virtual Router.

hold-time

Specify a delay (in seconds) before a switch becomes the MASTER virtual router. By delaying the initialization of the VRRP MASTER, the new switch can stabilize its routing tables.

Syntax **hold-time** *seconds*

To return to the default value, enter **no hold-time**.

Parameters

seconds	Enter a number of seconds. Range: 0 to 65535. Default: zero (0) seconds.

Defaults zero (0) seconds

Command Modes VRRP

Usage Information If a switch is a MASTER and you change the hold timer, you must disable and re-enable VRRP for the new hold timer value to take effect.

Related Commands

disable	Disable a VRRP group.

preempt

Permit a BACKUP router with a higher priority value to preempt or become the MASTER router.

Syntax **preempt**

To prohibit preemption, enter **no preempt**.

Defaults Enabled (that is, a BACKUP router can preempt the MASTER router).

Command Modes VRRP

priority

Specify a VRRP priority value for the VRRP group. This value is used by the VRRP protocol during the MASTER election process.

Syntax **priority** *priority*

To return to the default value, enter **no priority**.

Parameters

priority	Enter a number as the priority. Enter 255 only if the router's virtual address is the same as the interface's primary IP address (that is, the router is the OWNER). Range: 1 to 255. Default: 100.

Defaults 100

Command Modes VRRP

Usage Information To guarantee that a VRRP group becomes MASTER, configure the VRRP group's virtual address with same IP address as the interface's primary IP address and change the priority of the VRRP group to 255.

If you set the priority to 255 and the virtual-address is not equal to the interface's primary IP address, an error message appears.

show config

View the non default VRRP configuration.

Syntax **show config** [**verbose**]

Parameters

verbose	(OPTIONAL) Enter the keyword **verbose** to view all VRRP group configuration information, including defaults.

Command Modes VRRP

Example

```
Force10(conf-if-vrid-4)#show con
 vrrp-group 4
  virtual-address 119.192.182.124
 !
```

Figure 273 show config Command Example

show vrrp

View the VRRP groups that are active. If no VRRP groups are active, the FTOS returns "`No Active VRRP group`."

Syntax **show vrrp** [*vrrp-id*] [*interface*] [**brief**]

Parameters

vrrp-id	(OPTIONAL) Enter the Virtual Router Identifier for the VRRP group to view only that group. Range: 1 to 255.
interface	(OPTIONAL) Enter the following keywords and slot/port or number information: • For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For Port Channel interface types, enter the keyword **port-channel** followed by the number: C-Series Range: 1-128 on the C300 E-Series Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale • For SONET interfaces, enter the keyword **sonet** followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information. • For a VLAN interface, enter the keyword **vlan** followed by the VLAN ID. The VLAN ID range is from 1 to 4094.
brief	(OPTIONAL) Enter the keyword **brief** to view a table of information on the VRRP groups on the E-Series.

Command Modes EXEC

EXEC privilege

Example

```
Force10>Interface Grp Pri  Pre State  Master addr     Virtual addr(s)
Description
-------------------------------------------------------------------------------------------
Gi 10/37  1   100  Y   Master 200.200.200.200 200.200.200.201
Gi 10/37  2   100  Y   Master 200.200.200.200 200.200.200.202 200.200.200.203     Description
Gi 10/37  3   100  Y   Master 1.1.1.1         1.1.1.2
Gi 10/37  4   100  Y   Master 200.200.200.200 200.200.200.206 200.200.200.207 ... short desc
Gi 10/37  254 254  Y   Master 200.200.200.200 200.200.200.204 200.200.200.205
Force10>
```

Figure 274 show vrrp brief Command Example

Table 66 describes the items displayed in Figure 274

Table 66 show vrrp brief Command Example Items

Item	Description
Interface	Lists the interface type, slot and port on which the VRRP group is configured.
Grp	Displays the VRRP group ID.

Table 66 show vrrp brief Command Example Items

Item	Description
Pri	Displays the priority value assigned to the interface. If the track command is configured to track that interface and the interface is disabled, the *cost* is subtracted from the priority value assigned to the interface.
Pre	States whether preempt is enabled on the interface. • Y = Preempt is enabled. • N = Preempt is not enabled.
State	Displays the operational state of the interface by using one of the following: • NA/IF (the interface is not available). • MASTER (the interface associated with the MASTER router). • BACKUP (the interface associated with the BACKUP router).
Master addr	Displays the IP address of the MASTER router.
Virtual addr(s)	Displays the virtual IP addresses of the VRRP routers associated with the interface.

```
Force10>show vrrp
------------------
GigabitEthernet 12/3, VRID: 1, Net: 10.1.1.253
State: Master, Priority: 105, Master: 10.1.1.253 (local)
Hold Down: 0 sec, Preempt: TRUE, AdvInt: 1 sec
Adv rcvd: 0, Adv sent: 1862, Gratuitous ARP sent: 0
Virtual MAC address:
 00:00:5e:00:01:01
Virtual IP address:
 10.1.1.252
Authentication: (none)
Tracking states for 1 interfaces:
 Up  GigabitEthernet 12/17 priority-cost 10
------------------
GigabitEthernet 12/4, VRID: 2, Net: 10.1.2.253
State: Master, Priority: 110, Master: 10.1.2.253 (local)
Hold Down: 10 sec, Preempt: TRUE, AdvInt: 1 sec
Adv rcvd: 0, Adv sent: 1862, Gratuitous ARP sent: 0
Virtual MAC address:
 00:00:5e:00:01:02
Virtual IP address:
 10.1.2.252
Authentication: (none)
Tracking states for 2 interfaces:
 Up  GigabitEthernet 2/1 priority-cost 10
 Up  GigabitEthernet 12/17 priority-cost 10
Force10>
```

Figure 275 show vrrp Command Example

Table 67 describes the information displayed in Figure 275.

Table 67 show vrrp Command Example Items

Line Beginning with	Description
GigabitEthernet 12/3...	Displays the Interface, the VRRP group ID, and the network address. If the interface is no sending VRRP packets, 0.0.0.0 appears as the network address.

Table 67 show vrrp Command Example Items (continued)

State: master...	Displays the interface's state: • `Na/If` (not available), • `master` (MASTER virtual router) • `backup` (BACKUP virtual router) the interface's priority and the IP address of the MASTER.
Hold Down:...	This line displays additional VRRP configuration information: • `Hold Down` displays the hold down timer interval in seconds. • `Preempt` displays TRUE if preempt is configured and FALSE if preempt is not configured. • `AdvInt` displays the Advertise Interval in seconds.
Adv rcvd:...	This line displays counters for the following: • `Adv rcvd` displays the number of VRRP advertisements received on the interface. • `Adv sent` displays the number of VRRP advertisements sent on the interface. • `Gratuitous ARP` sent displays the number of gratuitous ARPs sent.
Virtual MAC address	Displays the virtual MAC address of the VRRP group.
Virtual IP address	Displays the virtual IP address of the VRRP router to which the interface is connected.
Authentication:...	States whether authentication is configured for the VRRP group. If it is, the authentication type and the password are listed.
Tracking states...	This line is displayed if the track command is configured on an interface. Below this line, the following information on the tracked interface is displayed: • `Dn` or `Up` states whether the interface is down or up. • the interface type slot/port information

track

Monitor an interface and lower the priority value of the VRRP group on that interface if it is disabled.

Syntax **track** *interface* [**priority-cost** *cost*]

To disable monitoring, use the **no track** *interface* command.

Parameters

interface	Enter the following keywords and slot/port or number information: • For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For a Loopback interface, enter the keyword **loopback** followed by a number from 0 to 16383. • For Port Channel interface types, enter the keyword **port-channel** followed by the number: C-Series Range: 1-128 on the C300 E-Series Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale • For SONET interfaces, enter the keyword **sonet** followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information. • For a VLAN interface, enter the keyword **vlan** followed by a number from 1 to 4094.
cost	(OPTIONAL) Enter a number as the amount to be subtracted from the priority value. Range: 1 to 254. Default: 10.

Defaults *cost* = 10

Command Modes VRRP

Usage Information If the interface is disabled, the cost value is subtracted from the priority value and forces a new MASTER election if the priority value is lower than the priority value in the BACKUP virtual routers.

virtual-address

Configure up to 12 IP addresses of virtual routers on the interface. You must set at least one virtual address for the VRRP group to start sending VRRP packets.

Syntax **virtual-address** *ip-address1* [... *ip-address12*]

To delete one or more virtual IP addresses, use the **no virtual-address** *ip-address1* [... *ip-address12*] command.

Parameters

ip-address1	Enter an IP address of the virtual router in dotted decimal format. The IP address must be on the same subnet as the interface's primary IP address.
... *ip-address12*	(OPTIONAL) Enter up 11 additional IP addresses of virtual routers in dotted decimal format. Separate the IP addresses with a space. The IP addresses must be on the same subnet as the interface's primary IP address.

Defaults Not configured.

Command Modes VRRP

Command History

Version 7.4.1.0	Introduced support for telnetting to the VRRP group IP address assigned using this command

Usage Information The VRRP group only becomes active and sends VRRP packets when a virtual IP address is configured. When you delete the virtual address, the VRRP group stops sending VRRP packets.

A system message appears after you enter or delete the virtual-address command.

To guarantee that a VRRP group becomes MASTER, configure the VRRP group's virtual address with the same IP address as the interface's primary IP address and change the priority of the VRRP group to 255.

You can ping the virtual addresses configured in all VRRP groups.

vrrp-group

Assign a VRRP ID to an interface. You can configure up to 12 VRRP groups per interface.

Syntax **vrrp-group** *vrrp-id*

Parameters

vrrp-id	Enter a number as the group ID. Range: 1 to 255.

Defaults Not configured.

Command Modes INTERFACE

Usage Information The VRRP group only becomes active and sends VRRP packets when a virtual IP address is configured. When you delete the virtual address, the VRRP group stops sending VRRP packets.

Related Commands

virtual-address	Assign up to 12 virtual IP addresses.

Chapter 32 Spanning Tree Protocol

The following commands configure and monitor the IEEE 802.1d Spanning Tree Protocol.

- bridge-priority on page 797
- debug spanning-tree on page 798
- disable on page 798
- forward-delay on page 799
- hello-time on page 799
- max-age on page 800
- protocol spanning-tree on page 800
- show config on page 801
- show spanning-tree 0 on page 801
- spanning-tree on page 803

bridge-priority

Set the bridge priority of the E-Series in an IEEE 802.1D Spanning Tree.

Syntax **bridge-priority** {*priority-value* | **primary** | **secondary**}

To return to the default value, enter **no bridge-priority**.

Parameters

priority-value	Enter a number as the bridge priority value. Range: 0 to 65535. Default: 32768.
primary	Enter the keyword **primary** to designate the bridge as the root bridge.
secondary	Enter the keyword **secondary** to designate the bridge as a secondary root bridge.

Defaults *priority-value* = 32768

Command Modes SPANNING TREE

Related Commands

protocol spanning-tree	Enter SPANNING TREE mode on the E-Series.

debug spanning-tree

Enable debugging of Spanning Tree Protocol and view information on the protocol.

Syntax **debug spanning-tree** *stp-id* [**all** | **bpdu** | **config** | **events** | **exceptions** | **general** | **root**]

To disable debugging, enter **no debug spanning-tree**.

Parameters

stp-id	Enter zero (0). The E-Series supports on Spanning Tree group with a group ID of 0.
all	(OPTIONAL) Enter the keyword **all** to debug all spanning tree operations.
bpdu	(OPTIONAL) Enter the keyword **bpdu** to debug Bridge Protocol Data Units.
config	(OPTIONAL) Enter the keyword **config** to debug configuration information.
events	(OPTIONAL) Enter the keyword **events** to debug STP events.
exceptions	(OPTIONAL) Enter the keyword **exceptions** to debug STP exceptions.
general	(OPTIONAL) Enter the keyword **general** to debug general STP operations.
root	(OPTIONAL) Enter the keyword **root** to debug STP root transactions.

Command Modes EXEC privilege

Usage Information When you enable **debug spanning-tree bpdu** for multiple interfaces, the software only sends information on BPDUs for the last interface specified.

disable

Disable Spanning Tree Protocol globally on the E-Series.

Syntax **disable**

To enable Spanning Tree Protocol, enter **no disable**.

Defaults Enabled (that is, Spanning Tree Protocol is disabled.)

Command Modes SPANNING TREE

Related Commands

protocol spanning-tree	Enter SPANNING TREE mode.

forward-delay

The amount of time the interface waits in the Listening State and the Learning State before transitioning to the Forwarding State.

Syntax **forward-delay** *seconds*

To return to the default setting, enter **no forward-delay.**

Parameters

seconds	Enter the number of seconds the FTOS waits before transitioning STP to the forwarding state. Range: 4 to 30 Default: 15 seconds.

Defaults 15 seconds

Command Modes SPANNING TREE

Related Commands

max-age	Change the wait time before STP refreshes protocol configuration information.
hello-time	Change the time interval between BPDUs.

hello-time

Set the time interval between generation of Spanning Tree Bridge Protocol Data Units (BPDUs).

Syntax **hello-time** *seconds*

To return to the default value, enter **no hello-time**.

Parameters

seconds	Enter a number as the time interval between transmission of BPDUs. Range: 1 to 10. Default: 2 seconds.

Defaults 2 seconds

Command Modes SPANNING TREE

Related Commands

forward-delay	Change the wait time before STP transitions to the Forwarding state.
max-age	Change the wait time before STP refreshes protocol configuration information.

max-age

Set the time interval for the Spanning Tree bridge to maintain configuration information before refreshing that information.

Syntax **max-age** *seconds*

To return to the default values, enter **no max-age**.

Parameters

max-age	Enter a number of seconds the FTOS waits before refreshing configuration information. Range: 6 to 40 Default: 20 seconds.

Defaults 20 seconds

Command Modes SPANNING TREE

Related Commands

forward-delay	Change the wait time before STP transitions to the Forwarding state.
hello-time	Change the time interval between BPDUs.

protocol spanning-tree

Enter the SPANNING TREE mode to enable and configure the Spanning Tree group.

Syntax **protocol spanning-tree** *stp-id*

To disable the Spanning Tree group, enter **no protocol spanning-tree** *stp-id* command.

Parameters

stp-id	Enter zero (0). FTOS supports one Spanning Tree group with a group ID of 0.

Defaults Not configured.

Command Modes CONFIGURATION

Example

```
Force10(conf)#protocol spanning-tree 0
Force10(config-span)#
```

Figure 276 protocol spanning-tree

Usage Information

STP is not enabled when you enter the SPANNING TREE mode. To enable STP globally on the E-Series, enter no disable from the SPANNING TREE mode.

Refer to the *FTOS Configuration Guide* for more information on Spanning Tree Protocol and Spanning Tree groups.

Related Commands

disable	Disable Spanning Tree group 0. To enable Spanning Tree group 0, enter **no disable**.

show config

View the current configuration for the mode. Only non-default values are shown.

Syntax **show config**

Command Modes SPANNING TREE

Example

```
Force10(config-span)#show config
protocol spanning-tree 0
 no disable
Force10(config-span)#
```

Figure 277 show config command for the SPANNING TREE mode

show spanning-tree 0

View the Spanning Tree group configuration and status of interfaces in the Spanning Tree group.

Syntax **show spanning-tree 0** [**active** | **brief** | **interface** *interface* | **root** | **summary**]

Parameters

0	Enter **0** (zero) to view information about that specific Spanning Tree group.
active	(OPTIONAL) Enter the keyword **active** to view only active interfaces in Spanning Tree group 0.
brief	(OPTIONAL) Enter the keyword **brief** to view a synopsis of the Spanning Tree group configuration information (Figure 279).

interface *interface*	(OPTIONAL) Enter the keyword **interface** and the type slot/port of the interface you want displayed. Type slot/port options are the following: • For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For a SONET interface, enter the keyword **sonet** followed by the slot/port information. • For Port Channel groups, enter the keyword **port-channel** followed by a number: C-Series Range: 1-128 E-Series Range: 1-32 for EtherScale, 1-255 for TeraScale • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information.
root	(OPTIONAL) Enter the keyword **root** to view configuration information on the Spanning Tree group root.
summary	(OPTIONAL) Enter the keyword **summary** to only the number of ports in the Spanning Tree group and their state.

Command Modes

EXEC

EXEC privilege

Example

```
Force10#show spann 0
     Executing IEEE compatible Spanning Tree Protocol
          Bridge Identifier has priority 32768, Address 0001.e800.0a56
          Configured hello time 2, max age 20, forward delay 15
          We are the root of the spanning tree
          Current root has priority 32768 address  0001.e800.0a56
          Topology change flag set, detected flag set
          Number of topology changes 1 last change occurred 0:00:05 ago
                  from GigabitEthernet 1/3
          Timers: hold 1, topology change 35
                  hello 2, max age 20, forward_delay 15
          Times:  hello 1, topology change 1, notification 0, aging 2

     Port 26 (GigabitEthernet 1/1) is Forwarding
          Port path cost 4, Port priority 8, Port Identifier 8.26
          Designated root has priority 32768, address 0001.e800.0a56
          Designated bridge has priority 32768, address 0001.e800.0a56
          Designated port id is 8.26, designated path cost 0
          Timers: message age 0, forward_delay 0, hold 0
          Number of transitions to forwarding state 1
          BPDU: sent:18, received 0
          The port is not in the portfast mode

     Port 27 (GigabitEthernet 1/2) is Forwarding
          Port path cost 4, Port priority 8, Port Identifier 8.27
          Designated root has priority 32768, address 0001.e800.0a56
          Designated bridge has priority 32768, address 0001.e800.0a56
          Designated port id is 8.27, designated path cost 0
          Timers: message age 0, forward_delay 0, hold 0
          Number of transitions to forwarding state 1
          BPDU: sent:18, received 0
          The port is not in the portfast mode

     Port 28 (GigabitEthernet 1/3) is Forwarding
          Port path cost 4, Port priority 8, Port Identifier 8.28
          Designated root has priority 32768, address 0001.e800.0a56
          Designated bridge has priority 32768, address 0001.e800.0a56
          Designated port id is 8.28, designated path cost 0
          Timers: message age 0, forward_delay 0, hold 0
          Number of transitions to forwarding state 1
          BPDU: sent:31, received 0
          The port is not in the portfast mode

Force10#
```

Figure 278 show spanning-tree

```
Force10#show span 0 brief
     Executing IEEE compatible Spanning Tree Protocol
          Root ID      Priority 32768
             Address 0001.e800.0a56
          Root Bridge hello time 2, max age 20, forward delay 15
          Bridge ID      Priority 32768,
             Address 0001.e800.0a56
          Configured hello time 2, max age 20, forward delay 15
Interface                                      Designated
 Name          PortID Prio Cost Sts Cost     Bridge ID             PortID
-------------- ------ ---- ---- --- -----    -----------------     ------
Gi 1/1          8.26     8    4 FWD     0    32768 0001.e800.0a56  8.26
Gi 1/2          8.27     8    4 FWD     0    32768 0001.e800.0a56  8.27
Gi 1/3          8.28     8    4 FWD     0    32768 0001.e800.0a56  8.28
Force10#
```

Figure 279 show spanning-tree brief

Usage Information You must enable Spanning Tree group 0 prior to using this command.

spanning-tree

Configure Spanning Tree group id, cost, priority, and Portfast for an interface.

Syntax **spanning-tree** *stp-id* [**cost** *cost*] [**portfast** [**bpduguard**]] [**priority** *priority*]

To disable Spanning Tree group on an interface, use the **no spanning-tree** *stp-id* [**cost** *cost*] [**portfast**] [**priority** *priority*] command.

Parameters

stp-id	Enter the Spanning Tree Protocol group ID. Range: 0
cost *cost*	(OPTIONAL) Enter the keyword **cost** followed by a number as the cost. Range: 1 to 65535 Defaults: 100 Mb/s Ethernet interface = 19 1-Gigabit Ethernet interface = 4 10-Gigabit Ethernet interface = 2 Port Channel interface with 100 Mb/s Ethernet = 18 Port Channel interface with 1-Gigabit Ethernet = 3 Port Channel interface with 10-Gigabit Ethernet = 1
priority *priority*	(OPTIONAL) Enter keyword **priority** followed by a number as the priority. Range: zero (0) to 15. Default: 8
portfast [**bpduguard**]	(OPTIONAL) Enter the keyword **portfast** to enable Portfast to move the interface into forwarding mode immediately after the root fails. Enter the keyword **bpduguard** to disable the port when it receives a BPDU.

Defaults *cost* = depends on the interface type; *priority* = 8

Command Modes INTERFACE

Usage Information If you enable **portfast bpduguard** on an interface and the interface receives a BPDU, the software disables the interface and sends a message stating that fact. The port is in ERR_DISABLE mode, yet appears in the **show interface** commands as enabled.

Chapter 33 PVST+

Force10's implementation of PVST+ (Per-VLAN Spanning Tree plus) is based on the IEEE 802.1d standard spanning-tree protocol but it creates a separate spanning-tree for each VLAN configured.

Note: For easier command line entry, the plus (+) sign is not used at the command line.

The FTOS PVST+ commands are:

- disable on page 805
- protocol spanning-tree pvst on page 806
- show spanning-tree pvst on page 806
- spanning-tree pvst on page 809
- tc-flush-standard on page 811
- vlan bridge-priority on page 811
- vlan forward-delay on page 812
- vlan hello-time on page 812
- vlan max-age on page 813

disable

Disable PVST+ globally.

Syntax **disable**

To enable PVST+, enter **no disable**.

Defaults PVST+ is disabled

Command Modes CONFIGURATION (conf-pvst)

Command History

Version 6.2.1.1	Introduced

Related Commands		
	protocol spanning-tree pvst	Enter PVST+ mode.

protocol spanning-tree pvst

Enter the PVST+ mode to enable PVST+ on a device.

Syntax **protocol spanning-tree pvst**

To disable PVST+, use the disable command.

Defaults This command has no default value or behavior.

Command Modes CONFIGURATION

Command History		
	Version 6.2.1.1	Introduced

Example

```
Force10#conf
Force10(conf)#protocol spanning-tree pvst
Force10(conf-pvst)#no disable
Force10(conf-pvst)#vlan 2 bridge-priority 4096
Force10(conf-pvst)#vlan 3 bridge-priority 16384
Force10(conf-pvst)#
Force10(conf-pvst)#show config
!
protocol spanning-tree pvst
 no disable
 vlan 2 bridge-priority 4096
 vlan 3 bridge-priority 16384
Force10#
```

Usage Information Once PVST+ is enabled, the device runs an STP instance for each VLAN it supports.

Related Commands		
	disable	Disable PVST+.
	show spanning-tree pvst	Display the PVST+ configuration.

show spanning-tree pvst

View the Per-VLAN Spanning Tree configuration.

Syntax **show spanning-tree pvst [vlan** *vlan-id*] [**brief**] [*Interface*]

vlan *vlan-id*	(OPTIONAL) Enter the keyword **vlan** followed by the VLAN ID. Range: 1 to 4094
brief	(OPTIONAL) Enter the keyword **brief** to view a synopsis of the PVST+ configuration information.
Interface	(OPTIONAL) Enter one of the interface keywords along with the slot/port information: • For a Fast Ethernet interface, enter the keyword **FastEthernet** followed by the slot/port information. • For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For Port Channel groups, enter the keyword **port-channel** followed by a number: C-Series Range: 1-128 E-Series Range: 1-32 for EtherScale, 1-255 for TeraScale • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information.

Defaults No default behavior or values

Command Modes EXEC

EXEC Privilege

Command History

Version 6.2.1.1	Introduced
Version 6.4.1.0	Expanded to display port error disable state (EDS) caused by loopback BPDU inconsistency (see Figure 282) and Port VLAN ID inconsistency (see Figure 283)

Example 1

```
Force10#show spanning-tree pvst vlan 3 brief
VLAN 3
Executing IEEE compatible Spanning Tree Protocol
Root ID    Priority 4096, Address 0001.e801.6aa8
Root Bridge hello time 2, max age 20, forward delay 15
Bridge ID    Priority 16384, Address 0001.e805.e306
Configured hello time 2, max age 20, forward delay 15

Interface                                        Designated
 Name      PortID   Prio Cost    Sts Cost       Bridge ID         PortID
---------- -------- ---- ------  --- ------- -------------------- --------
Gi 1/0     128.130  128  20000   FWD 20000   4096  0001.e801.6aa8  128.426
Gi 1/1     128.131  128  20000   BLK 20000   4096  0001.e801.6aa8  128.427
Gi 1/16    128.146  128  20000   FWD 20000   16384 0001.e805.e306  128.146
Gi 1/17    128.147  128  20000   FWD 20000   16384 0001.e805.e306  128.147

Interface
 Name      Role   PortID   Prio Cost    Sts Cost    Link-type Edge
---------- ------ -------- ---- ------- --- ------- --------- ----
Gi 1/0     Root   128.130  128  20000   FWD 20000   P2P       No
Gi 1/1     Altr   128.131  128  20000   BLK 20000   P2P       No
Gi 1/16    Desg   128.146  128  20000   FWD 20000   P2P       Yes
Gi 1/17    Desg   128.147  128  20000   FWD 20000   P2P       Yes
```

Figure 280 show spanning-tree pvst brief command

Example 2

```
Force10#show spanning-tree pvst vlan 2
VLAN 2
Root Identifier has priority 4096, Address 0001.e805.e306
Root Bridge hello time 2, max age 20, forward delay 15
Bridge Identifier has priority 4096, Address 0001.e805.e306
Configured hello time 2, max age 20, forward delay 15
We are the root of VLAN 2
Current root has priority 4096, Address 0001.e805.e306
Number of topology changes 3, last change occured 00:57:00

Port 130 (GigabitEthernet 1/0) is designated Forwarding
Port path cost 20000, Port priority 128, Port Identifier 128.130
Designated root has priority 4096, address 0001.e805.e3:06
Designated bridge has priority 4096, address 0001.e805.e3:06
Designated port id is 128.130, designated path cost 0
Number of transitions to forwarding state 1
BPDU sent 1567, received 3
The port is not in the Edge port mode

Port 131 (GigabitEthernet 1/1) is designated Forwarding
Port path cost 20000, Port priority 128, Port Identifier 128.131
Designated root has priority 4096, address 0001.e805.e3:06
Designated bridge has priority 4096, address 0001.e805.e3:06
Designated port id is 128.131, designated path cost 0
Number of transitions to forwarding state 1
BPDU sent 1567, received 0
The port is not in the Edge port mode

Port 146 (GigabitEthernet 1/16) is designated Forwarding
Port path cost 20000, Port priority 128, Port Identifier 128.146
Designated root has priority 4096, address 0001.e805.e3:06
Designated bridge has priority 4096, address 0001.e805.e3:06
Designated port id is 128.146, designated path cost 0
Number of transitions to forwarding state 1
BPDU sent 1578, received 0
The port is in the Edge port mode

Port 147 (GigabitEthernet 1/17) is designated Forwarding
Port path cost 20000, Port priority 128, Port Identifier 128.147
Designated root has priority 4096, address 0001.e805.e3:06
Designated bridge has priority 4096, address 0001.e805.e3:06
Designated port id is 128.147, designated path cost 0
Number of transitions to forwarding state 1
BPDU sent 1579, received 0
The port is in the Edge port mode
```

Figure 281 show spanning-tree pvst vlan command

Example 3

```
Force10#show spanning-tree pvst vlan 2 interface gigabitethernet 1/0

GigabitEthernet 1/0 of VLAN 2 is LBK_INC discarding

Edge port:no (default) port guard :none (default)
Link type: point-to-point (auto) bpdu filter:disable (default)
Bpdu guard :disable (default)
Bpdus sent 152, received 27562

Interface                                    Designated
 Name     PortID   Prio Cost    Sts Cost       Bridge ID          PortID
--------- -------- ---- ------- --- ------- -------------------- --------
Gi 1/0    128.1223 128  20000   EDS 0       32768 0001.e800.a12b  128.1223
```

Loopback BPDU Inconsistency (LBK_INC)

Figure 282 show spanning-tree pvst command with EDS and LBK

Example 4

```
Force10#show spanning-tree pvst vlan 2 interface gigabitethernet 1/0

GigabitEthernet 1/0 of VLAN 2 is PVID_INC discarding

Edge port:no (default) port guard :none (default)
Link type: point-to-point (auto) bpdu filter:disable (default)
Bpdu guard :disable (default)
Bpdus sent 1, received 0

Interface                                    Designated
 Name     PortID   Prio Cost    Sts Cost      Bridge ID         PortID
--------- -------- ---- ------- --- ------- -------------------- --------
Gi 1/0     128.1223 128  20000   EDS 0       32768 0001.e800.a12b  128.1223
```

Port VLAN ID (PVID) Inconsistency

Figure 283 show spanning-tree pvst with EDS and PVID

Related Commands

spanning-tree pvst	Configure PVST+ on an interface.

spanning-tree pvst

Configure PVST+ Edge port with optional Bridge Port Data Unit (BPDU) guard, VLAN, Port priority, and Port cost on an interface.

Syntax **spanning-tree pvst** [**edge-port** [**bpduguard**]] | **vlan** *vlan-range* {**cost** *number* | **priority** *value*}]

To disable PVST+ on an interface, use the **no spanning-tree pvst** [**edge-port** [**bpduguard**]] | **vlan** *vlan-range* {**cost** *number* | **priority** *value*}] command.

Parameters

edge-port	(OPTIONAL) Enter the keyword **edge-port** to configure the interface as a PVST+ edge port.
bpduguard	(OPTIONAL) Enter the keyword **bpduguard** to configure a Bridge Port Data Unit guard on the edge-port.
vlan *vlan-range*	(OPTIONAL) Enter the keyword **vlan** followed by the VLAN number(s). Range: 1 to 4094

cost *number*	(OPTIONAL) Enter the keyword **cost** followed by the port cost value. Range: 1 to 200000 Defaults: 100 Mb/s Ethernet interface = 200000 1-Gigabit Ethernet interface = 20000 10-Gigabit Ethernet interface = 2000 Port Channel interface with one 100 Mb/s Ethernet = 200000 Port Channel interface with one 1-Gigabit Ethernet = 20000 Port Channel interface with one 10-Gigabit Ethernet = 2000 Port Channel with two 1-Gigabit Ethernet = 18000 Port Channel with two 10-Gigabit Ethernet = 1800 Port Channel with two 100-Mbps Ethernet = 180000
priority *value*	(OPTIONAL) Enter the keyword **priority** followed the Port priority value in increments of 16. Range: 0 to 240 Default: 128

Defaults Not Configured

Command Modes INTERFACE

Command History

Version 7.4.1.0	Added the optional Bridge Port Data Unit (BPDU) guard
Version 6.2.1.1	Introduced

Usage Information The BPDU guard option prevents the port from participating in an active STP topology in case a BPDU appears on a port unintentionally, or is misconfigured, or is subject to a DOS attack. This option places the port into an error disable state if a BPDU appears, and a message is logged so that the administrator can take corrective action.

Note: A port configured as an edge port, on a PVST switch, will immediately transition to the forwarding state. Only ports connected to end-hosts should be configured as an edge port. Consider an edge port similar to a port with a spanning-tree portfast enabled.

Example

```
Force10(conf-if-gi-1/1)#spanning-tree pvst vlan 3 cost 18000
Force10(conf-if-gi-1/1)#end
Force10(conf-if-gi-1/1)#show config
!
interface GigabitEthernet 1/1
 no ip address
 switchport
 spanning-tree pvst vlan 3 cost 18000
 no shutdown
Force10(conf-if-gi-1/1)#end

Force10#
```

Figure 284 spanning-tree pvst command

Related Commands

show spanning-tree pvst	View PVST+ configuration

tc-flush-standard

Enable the MAC address flushing upon receiving every topology change notification.

Syntax **tc-flush-standard**

To disable, use the **no tc-flush-standard** command.

Defaults Disabled

Command Modes CONFIGURATION

Command History

Version 6.5.1.0	Introduced

Usage Information By default FTOS implements an optimized flush mechanism for PVST+. This helps in flushing the MAC addresses only when necessary (and less often) allowing for faster convergence during topology changes. However, if a standards-based flush mechanism is needed, this *knob* command can be turned on to enable flushing MAC addresses upon receiving every topology change notification.

vlan bridge-priority

Set the PVST+ bridge-priority for a VLAN or a set of VLANs.

Syntax **vlan** *vlan-range* **bridge-priority** *value*

To return to the default value, enter **no vlan bridge-priority** command.

Parameters

vlan *vlan-range*	Enter the keyword **vlan** followed by the VLAN number(s). Range: 1 to 4094
bridge-priority *value*	Enter the keyword **bridge-priority** followed by the bridge priority value in increments of 4096. Range: 0 to 61440 Default: 32768

Defaults 32768

Command Modes CONFIGURATION (conf-pvst)

Command History

Version 6.2.1.1	Introduced

Related Commands

vlan forward-delay	Change the time interval before FTOS transitions to the forwarding state
vlan hello-time	Change the time interval between BPDUs

vlan max-age	Change the time interval before PVST+ refreshes
show spanning-tree pvst	Display the PVST+ configuration

vlan forward-delay

The amount of time the interface waits in the Listening State and the Learning State before transitioning to the Forwarding State.

Syntax **vlan** *vlan-range* **forward-delay** *seconds*

To return to the default setting, enter **no vlan forward-delay** command.

Parameters

vlan *vlan-range*	Enter the keyword **vlan** followed by the VLAN number(s). Range: 1 to 4094
forward-delay *seconds*	Enter the keyword **forward-delay** followed by the time interval, in seconds, that FTOS waits before transitioning PVST+ to the forwarding state. Range: 4 to 30 seconds Default: 15 seconds

Defaults 15 seconds

Command Modes CONFIGURATION (conf-pvst)

Command History

Version 6.2.1.1	Introduced

Related Commands

vlan bridge-priority	Set the bridge-priority value
vlan hello-time	Change the time interval between BPDUs
vlan max-age	Change the time interval before PVST+ refreshes
show spanning-tree pvst	Display the PVST+ configuration

vlan hello-time

Set the time interval between generation of PVST+ Bridge Protocol Data Units (BPDUs).

Syntax **vlan** *vlan-range* **hello-time** *seconds*

To return to the default value, enter **no vlan hello-time** command.

Parameters

vlan *vlan-range*	Enter the keyword **vlan** followed by the VLAN number(s). Range: 1 to 4094
hello-time *seconds*	Enter the keyword **hello-time** followed by the time interval, in seconds, between transmission of BPDUs. Range: 1 to 10 seconds Default: 2 seconds

Defaults 2 seconds

Command Modes CONFIGURATION (conf-pvst)

Command History

Version 6.2.1.1	Introduced

Related Commands

vlan bridge-priority	Set the bridge-priority value
vlan forward-delay	Change the time interval before FTOS transitions to the forwarding state
vlan max-age	Change the time interval before PVST+ refreshes
show spanning-tree pvst	Display the PVST+ configuration

vlan max-age

Set the time interval for the PVST+ bridge to maintain configuration information before refreshing that information.

Syntax **vlan** *vlan-range* **max-age** *seconds*

To return to the default, use the **no vlan max-age** command.

Parameters

vlan *vlan-range*	Enter the keyword **vlan** followed by the VLAN number(s). Range: 1 to 4094
max-age *seconds*	Enter the keyword **max-age** followed by the time interval, in seconds, that FTOS waits before refreshing configuration information. Range: 6 to 40 seconds Default: 20 seconds

Defaults 20 seconds

Command Modes CONFIGURATION (conf-pvst)

Command History

Version 6.2.1.1	Introduced

Related Commands

vlan bridge-priority	Set the bridge-priority value
vlan forward-delay	Change the time interval before FTOS transitions to the forwarding state
vlan hello-time	Change the time interval between BPDUs
show spanning-tree pvst	Display the PVST+ configuration

Chapter 34 RSTP

Force10's implementation of RSTP (Rapid Spanning Tree Protocol) is based on the IEEE 802.1w standard spanning-tree protocol. The RSTP algorithm configures connectivity throughout a Bridged LAN that is comprised of LANs interconnected by Bridges.

The FTOS RSTP commands are:

- bridge-priority on page 815
- debug spanning-tree rstp on page 816
- disable on page 817
- forward-delay on page 817
- hello-time on page 818
- max-age on page 818
- protocol spanning-tree rstp on page 819
- show config on page 820
- show spanning-tree rstp on page 820
- spanning-tree rstp on page 822
- tc-flush-standard on page 823

bridge-priority

Set the bridge priority for RSTP.

Syntax **bridge-priority** *priority-value*

To return to the default value, enter **no bridge-priority**.

Parameters

priority-value	Enter a number as the bridge priority value in increments of 4096. Range: 0 to 61440. Default: 32768

Defaults 32768

Command Modes CONFIGURATION RSTP (conf-rstp)

Command History

Version 6.2.1.1	Introduced

Related Commands

protocol spanning-tree rstp	Enter the Rapid Spanning Tree mode

debug spanning-tree rstp

Enable debugging of RSTP and view information on the protocol.

Syntax **debug spanning-tree rstp [all | bpdu** *interface* **{in | out} | events]**

To disable debugging, enter **no debug spanning-tree rstp**.

Parameters

all	(OPTIONAL) Enter the keyword **all** to debug all spanning tree operations.
bpdu *interface* **{in | out}**	(OPTIONAL) Enter the keyword **bpdu** to debug Bridge Protocol Data Units. (OPTIONAL) Enter the interface keyword along with the type slot/port of the interface you want displayed. Type slot/port options are the following: • For a Fast Ethernet interface, enter the keyword **FastEthernet** followed by the slot/port information. • For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For Port Channel groups, enter the keyword **port-channel** followed by a number: C-Series Range: 1-128 E-Series Range: 1-32 for EtherScale, 1-255 for TeraScale • For a SONET interface, enter the keyword **sonet** followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information. Optionally, enter an in or out parameter in conjunction with the optional interface: • For Receive, enter **in** • For Transmit, enter **out**
events	(OPTIONAL) Enter the keyword **events**to debug RSTP events.

Command Modes EXEC privilege

Command History

Version 6.2.1.1	Introduced

Example

```
Force10#debug spanning-tree rstp bpdu gigabitethernet 2/0 ?
in Receive (in)
out Transmit (out)
```

disable

Disable RSTP globally on the system.

Syntax **disable**

To enable Rapid Spanning Tree Protocol, enter **no disable**.

Defaults RSTP is disabled

Command Modes CONFIGURATION RSTP (conf-rstp)

Command History

Version 6.2.1.1	Introduced

Related Commands

protocol spanning-tree rstp	Enter the Rapid Spanning Tree mode

forward-delay

Configure the amount of time the interface waits in the Listening State and the Learning State before transitioning to the Forwarding State.

Syntax **forward-delay** *seconds*

To return to the default setting, enter **no forward-delay.**

Parameters

seconds	Enter the number of seconds that FTOS waits before transitioning RSTP to the forwarding state. Range: 4 to 30 Default: 15 seconds

Defaults 15 seconds

Command Modes CONFIGURATION RSTP (conf-rstp)

Command History

Version 6.2.1.1	Introduced

Related Commands

hello-time	Change the time interval between BPDUs.
max-age	Change the wait time before RSTP refreshes protocol configuration information.

hello-time

Set the time interval between generation of RSTP Data Units (BPDUs).

Syntax **hello-time** *seconds*

To return to the default value, enter **no hello-time**.

Parameters

seconds	Enter a number as the time interval between transmission of BPDUs. Range: 1 to 10 seconds Default: 2 seconds.

Defaults 2 seconds

Command Modes CONFIGURATION RSTP (conf-rstp)

Command History

Version 6.2.1.1	Introduced

Related Commands

forward-delay	Change the wait time before RSTP transitions to the Forwarding state.
max-age	Change the wait time before RSTP refreshes protocol configuration information.

max-age

Set the time interval for the RSTP bridge to maintain configuration information before refreshing that information.

Syntax **max-age** *seconds*

To return to the default values, enter **no max-age**.

Parameters

max-age	Enter a number of seconds the FTOS waits before refreshing configuration information. Range: 6 to 40 seconds Default: 20 seconds

Defaults 20 seconds

Command Modes CONFIGURATION RSTP (conf-rstp)

Command History

Version 6.2.1.1	Introduced

Related Commands

max-age	Change the wait time before RSTP transitions to the Forwarding state.
hello-time	Change the time interval between BPDUs.

protocol spanning-tree rstp

Enter the RSTP mode to configure RSTP.

Syntax **protocol spanning-tree rstp**

To exit the RSTP mode, enter **exit**

Defaults Not configured

Command Modes CONFIGURATION RSTP (conf-rstp)

Command History

Version 6.2.1.1	Introduced

Example

```
Force10(conf)#protocol spanning-tree rstp
Force10(config-rstp)##no disable
```

Figure 285 protocol spanning-tree rstp command

Usage Information RSTP is not enabled when you enter the RSTP mode. To enable RSTP globally on the system, enter no disable from the RSTP mode.

Related Commands

disable	Disable RSTP globally on the system.

show config

View the current configuration for the mode. Only non-default values are displayed.

Syntax **show config**

Command Modes CONFIGURATION RSTP (conf-rstp)

Command History

Version 6.2.1.1	Introduced

Example

```
Force10(conf-rstp)#show config
!
protocol spanning-tree rstp
 no disable
 bridge-priority 16384
Force10(conf-rstp)#
```

Figure 286 show config command for the RSTP mode

show spanning-tree rstp

Display the RSTP configuration.

Syntax **show spanning-tree rstp** [**brief**]

Parameters

brief

Command Modes EXEC

EXEC privilege

Command History

Version 6.2.1.1	Introduced
Version 6.4.1.0	Expanded to display port error disable state (EDS) caused by loopback BPDU inconsistency (see Figure 288)

Example 1

```
Force10#show spanning-tree rstp brief
Executing IEEE compatible Spanning Tree Protocol
Root ID    Priority 8192, Address 0001.e805.e306
Root Bridge hello time 4, max age 20, forward delay 15
Bridge ID    Priority 16384, Address 0001.e801.6aa8
Configured hello time 2, max age 20, forward delay 15

Interface                                          Designated
 Name      PortID   Prio Cost    Sts Cost        Bridge ID         PortID
---------- -------- ---- ------- --- ------- -------------------- --------
Gi 4/0     128.418  128  20000   FWD 20000   16384 0001.e801.6aa8 128.418
Gi 4/1     128.419  128  20000   FWD 20000   16384 0001.e801.6aa8 128.419
Gi 4/8     128.426  128  20000   FWD 20000   8192  0001.e805.e306 128.130
Gi 4/9     128.427  128  20000   BLK 20000   8192  0001.e805.e306 128.131

Interface
 Name      Role   PortID   Prio Cost    Sts Cost    Link-type Edge
---------- ------ -------- ---- ------- --- ------- --------- ----
Gi 4/0     Desg   128.418  128  20000   FWD 20000   P2P       Yes
Gi 4/1     Desg   128.419  128  20000   FWD 20000   P2P       Yes
Gi 4/8     Root   128.426  128  20000   FWD 20000   P2P       No
Gi 4/9     Altr   128.427  128  20000   BLK 20000   P2P       No
Force10#
```

Figure 287 show spanning-tree rstp brief command

Example 2

```
Force10#show spanning-tree rstp br
Executing IEEE compatible Spanning Tree Protocol
Root ID    Priority 32768, Address 0001.e801.6aa8
Root Bridge hello time 2, max age 20, forward delay 15
Bridge ID    Priority 32768, Address 0001.e801.6aa8
We are the root
Configured hello time 2, max age 20, forward delay 15

Interface                                     Designated
 Name      PortID   Prio Cost    Sts Cost        Bridge ID         PortID
---------- -------- ---- ------- --- ------- -------------------- --------
Gi 0/0     128.257  128  20000   EDS 0       32768 0001.e801.6aa8 128.257

Interface
 Name      Role   PortID   Prio Cost    Sts Cost    Link-type Edge
---------- ------ -------- ---- ------- --- ------- --------- ----
Gi 0/0     ErrDis 128.257  128  20000   EDS 0       P2P       No

Force10#show spanning-tree rstp
Root Identifier has priority 32768, Address 0001.e801.6aa8
Root Bridge hello time 2, max age 20, forward delay 15, max hops 0
Bridge Identifier has priority 32768, Address 0001.e801.6aa8
Configured hello time 2, max age 20, forward delay 15, max hops 0
We are the root
Current root has priority 32768, Address 0001.e801.6aa8
Number of topology changes 1, last change occured 00:00:31 ago on Gi 0/0

Port 257 (GigabitEthernet 0/0) is LBK_INC Discarding
Port path cost 20000, Port priority 128, Port Identifier 128.257
Designated root has priority 32768, address 0001.e801.6aa8
Designated bridge has priority 32768, address 0001.e801.6aa8
Designated port id is 128.257, designated path cost 0
Number of transitions to forwarding state 1
BPDU : sent 27, received 9
The port is not in the Edge port mode

Force10#
```

Loopback BPDU Inconsistency (LBK_INC)

Figure 288 show spanning-tree rstp with EDS and LBK

spanning-tree rstp

Configure Port cost, Edge port with optional Bridge Port Data Unit (BPDU) guard, or Port priority on the RSTP.

Syntax **spanning-tree rstp** {**cost** *Port cost* | **edge-port** [**bpduguard**] | **priority** *priority*}

To remove the port cost, edge port with optional BPDU, or port priority, use the **no spanning-tree rstp** {**cost** *Port cost* | **edge-port** [**bpduguard**] | **priority** *priority*} command.

Parameters

cost *Port cost*	(OPTIONAL) Enter the keyword **cost** followed by the port cost value. Range: 1 to 200000 Defaults: 100 Mb/s Ethernet interface = 200000 1-Gigabit Ethernet interface = 20000 10-Gigabit Ethernet interface = 2000 Port Channel interface with one 100 Mb/s Ethernet = 200000 Port Channel interface with one 1-Gigabit Ethernet = 20000 Port Channel interface with one 10-Gigabit Ethernet = 2000 Port Channel with two 1-Gigabit Ethernet = 18000 Port Channel with two 10-Gigabit Ethernet = 1800 Port Channel with two 100-Mbps Ethernet = 180000
edge-port	Enter the keyword **edge-port** to configure the interface as a Rapid Spanning Tree edge port.
bpduguard	(OPTIONAL) Enter the keyword **bpduguard** to configure a Bridge Port Data Unit guard on the edge-port.
priority *priority*	(OPTIONAL) Enter keyword **priority** followed by a value in increments of 16 as the priority. Range: 0 to 240. Default: 128

Defaults Not configured

Command Modes INTERFACE

Command History

Version 7.4.1.0	Added the optional Bridge Port Data Unit (BPDU) guard.
Version 6.2.1.1	Introduced

Usage Information The BPDU guard option prevents the port from participating in an active STP topology in case a BPDU appears on a port unintentionally, or is misconfigured, or is subject to a DOS attack. This option places the port into an error disable state if a BPDU appears, and a message is logged so that the administrator can take corrective action.

Note: A port configured as an edge port, on a RSTP switch, will immediately transition to the forwarding state. Only ports connected to end-hosts should be configured as an edge port. Consider an edge port similar to a port with a spanning-tree portfast enabled.

Example

```
Force10(conf)#interface gigabitethernet 4/0
Force10(conf-if-gi-4/0)#spanning-tree rstp edge-port
Force10(conf-if-gi-4/0)#show config
!
interface GigabitEthernet 4/0
 no ip address
 switchport
 spanning-tree rstp edge-port
 no shutdown
Force10#
```

Figure 289 spanning-tree rstp edge-port command

tc-flush-standard

Enable the MAC address flushing upon receiving every topology change notification.

Syntax **tc-flush-standard**

To disable, use the **no tc-flush-standard** command.

Defaults Disabled

Command Modes CONFIGURATION

Command History

Version 6.5.1.0	Introduced

Usage Information By default FTOS implements an optimized flush mechanism for RSTP. This helps in flushing the MAC addresses only when necessary (and less often) allowing for faster convergence during topology changes. However, if a standards-based flush mechanism is needed, this *knob* command can be turned on to enable flushing MAC addresses upon receiving every topology change notification.

Chapter 35 MSTP

The following commands configure and monitor the IEEE 802.1s Multiple Spanning Tree Protocol.

- debug spanning-tree mstp on page 825
- disable on page 826
- forward-delay on page 827
- hello-time on page 827
- max-age on page 828
- max-hops on page 828
- msti on page 829
- name on page 830
- protocol spanning-tree mstp on page 830
- revision on page 831
- show config on page 832
- show spanning-tree mst configuration on page 832
- show spanning-tree msti on page 833
- spanning-tree on page 835
- spanning-tree msti on page 836
- spanning-tree mstp edge-port on page 837
- tc-flush-standard on page 837

debug spanning-tree mstp

Enable debugging of Multiple Spanning Tree Protocol and view information on the protocol.

Syntax **debug spanning-tree mstp** [**all** | **bpdu** *interface* {**in** | **out**} | **events**]

To disable debugging, enter **no debug spanning-tree mstp**.

Parameters

all	(OPTIONAL) Enter the keyword **all** to debug all spanning tree operations.
bpdu *interface* {**in** | **out**}	(OPTIONAL) Enter the keyword **bpdu** to debug Bridge Protocol Data Units. (OPTIONAL) Enter the interface keyword along with the type slot/port of the interface you want displayed. Type slot/port options are the following: • For a Fast Ethernet interface, enter the keyword **FastEthernet** followed by the slot/port information. • For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For Port Channel groups, enter the keyword **port-channel** followed by a number: C-Series Range: 1-128 E-Series Range: 1-32 for EtherScale, 1-255 for TeraScale • For a SONET interface, enter the keyword **sonet** followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information. Optionally, enter an in or out parameter in conjunction with the optional interface: • For Receive, enter **in** • For Transmit, enter **out**
events	(OPTIONAL) Enter the keyword **events**to debug MSTP events.

Command Modes EXEC privilege

Example

```
Force10#debug spanning-tree mstp bpdu gigabitethernet 2/0 ?
in Receive (in)
out Transmit (out)
```

disable

Globally disable Multiple Spanning Tree Protocol on the E-Series.

Syntax **disable**

To enable Multiple Spanning Tree Protocol, enter **no disable**.

Defaults Multiple Spanning Tree Protocol is disabled

Command Modes MULTIPLE SPANNING TREE

Related Commands		
	protocol spanning-tree mstp	Enter MULTIPLE SPANNING TREE mode.

forward-delay

The amount of time the interface waits in the Blocking State and the Learning State before transitioning to the Forwarding State.

Syntax **forward-delay** *seconds*

To return to the default setting, enter **no forward-delay.**

Parameters		
	seconds	Enter the number of seconds the interface waits in the Blocking State and the Learning State before transiting to the Forwarding State. Range: 4 to 30 Default: 15 seconds.

Defaults 15 seconds

Command Modes MULTIPLE SPANNING TREE

Related Commands		
	max-age	Change the wait time before MSTP refreshes protocol configuration information.
	hello-time	Change the time interval between BPDUs.

hello-time

Set the time interval between generation of Multiple Spanning Tree Bridge Protocol Data Units (BPDUs).

Syntax **hello-time** *seconds*

To return to the default value, enter **no hello-time**.

Parameters		
	seconds	Enter a number as the time interval between transmission of BPDUs. Range: 1 to 10. Default: 2 seconds.

Defaults 2 seconds

Command Modes MULTIPLE SPANNING TREE

Related Commands

forward-delay	The amount of time the interface waits in the Blocking State and the Learning State before transitioning to the Forwarding State.
max-age	Change the wait time before MSTP refreshes protocol configuration information.

max-age

Set the time interval for the Multiple Spanning Tree bridge to maintain configuration information before refreshing that information.

Syntax **max-age** *seconds*

To return to the default values, enter **no max-age**.

Parameters

max-age	Enter a number of seconds the FTOS waits before refreshing configuration information. Range: 6 to 40 Default: 20 seconds.

Defaults 20 seconds

Command Modes MULTIPLE SPANNING TREE

Related Commands

forward-delay	The amount of time the interface waits in the Blocking State and the Learning State before transitioning to the Forwarding State.
hello-time	Change the time interval between BPDUs.

max-hops

Configure the maximum hop count.

Syntax **max-hops** *number*

To return to the default values, enter **no max-hops**.

Parameters

range	Enter a number for the maximum hop count. Range: 1 to 40 Default: 20

Defaults 20 hops

Command Modes MULTIPLE SPANNING TREE

Usage Information The **max-hops** is a configuration command that applies to both the IST and all MST instances in the MSTP region. The BPDUs sent out by the root switch set the remaining-hops parameter to the configured value of max-hops. When a switch receives the BPDU, it decrements the received value of the remaining hops and uses the resulting value as remaining-hops in the BPDUs. If the remaining-hops reaches zero, the switch discards the BPDU and ages out any information that it holds for the port.

msti

Configure Multiple Spanning Tree instance, bridge priority, and one or multiple VLANs mapped to the MST instance.

Syntax **msti** *instance* {**vlan** *range* | **bridge-priority** *priority*}

To disable mapping or bridge priority **no msti** *instance* {**vlan** *range* | **bridge-priority** *priority*}

Parameters

msti *instance*	Enter the Multiple Spanning Tree Protocol Instance Range: zero (0) to 63
vlan *range*	Enter the keyword **vlan** followed by the identifier range value. Range: 1 to 4094
bridge-priority *priority*	Enter the keyword **bridge-priority** followed by a value in increments of 4096 as the bridge priority. Range: zero (0) to 61440 Valid priority values are: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440. All other values are rejected.

Defaults default bridge-priority is 32768

Command Modes INTERFACE

Usage Information By default, all VLANs are mapped to MST instance zero (0) unless you use the **vlan** *range* command to map it to a non-zero instance.

name

The name you assign to the Multiple Spanning Tree region.

Syntax **name** *region-name*

To remove the region name, enter **no name**

Parameters

region-name	Enter the MST region name. Range: 32 character limit

Defaults no default name

Command Modes MULTIPLE SPANNING TREE

Usage Information For two MSTP switches to be within the same MSTP region, the switches must share the same region name (including matching case).

Related Commands

msti	Map the VLAN(s) to an MST instance
revision	Assign revision number to the MST configuration.

protocol spanning-tree mstp

Enter the MULTIPLE SPANNING TREE mode to enable and configure the Multiple Spanning Tree group.

Syntax **protocol spanning-tree mstp**

To disable the Multiple Spanning Tree group, enter **no protocol spanning-tree mstp** command.

Defaults Not configured.

Command Modes CONFIGURATION

Example

```
Force10(conf)#protocol spanning-tree mstp
Force10(config-mstp)#no disable
```

Figure 290 protocol spanning-tree mstp

Usage Information

MSTP is not enabled when you enter the MULTIPLE SPANNING TREE mode. To enable MSTP globally on the E-Series, enter no disable while in MULTIPLE SPANNING TREE mode.

Refer to the *FTOS Configuration Guide* for more information on Multiple Spanning Tree Protocol.

Related Commands

disable	Disable Multiple Spanning Tree.

Defaults

Disable.

Command Modes

MULTIPLE SPANNING TREE

Usage Information

Refer to the *FTOS Configuration Guide* for more information on Multiple Spanning Tree Protocol.

revision

The revision number for the Multiple Spanning Tree configuration

Syntax

revision *range*

To return to the default values, enter **no revision**.

Parameters

range	Enter the revision number for the MST configuration. Range: 0 to 65535 Default: 0

Defaults

0

Command Modes

MULTIPLE SPANNING TREE

Usage Information

For two MSTP switches to be within the same MST region, the switches must share the same revision number.

Related Commands		
	msti	Map the VLAN(s) to an MST instance
	name	Assign the region name to the MST region.

show config

View the current configuration for the mode. Only non-default values are shown.

Syntax **show config**

Command Modes MULTIPLE SPANNING TREE

Example

```
Force10(conf-mstp)#show config
!
protocol spanning-tree mstp
 no disable
 name CustomerSvc
 revision 2
 MSTI 10 VLAN 101-105
 max-hops 5
Force10(conf-mstp)#
```

Figure 291 show config command for the MULTIPLE SPANNING TREE mode

show spanning-tree mst configuration

View the Multiple Spanning Tree configuration

Syntax **show spanning-tree mst configuration**

Command Modes EXEC

EXEC privilege

Example

```
Force10#show spanning-tree mst configuration
MST region name: CustomerSvc
Revision: 2
MSTI    VID
  10     101-105
Force10#
```

Figure 292 show spanning-tree mst configuration

Usage Information You must enable Multiple Spanning Tree Protocol prior to using this command.

show spanning-tree msti

View the Multiple Spanning Tree instance

Syntax **show spanning-tree msti** [*instance-number* [**brief**]]

Parameters

instance-number	[Optional] Enter the Multiple Spanning Tree Instance number Range: 0 to 63
brief	[Optional] Enter the keyword brief to view a synopsis of the MST instance.

Command Modes EXEC

EXEC privilege

Command History

Version 6.4.1.0	Expanded to display port error disable state (EDS) caused by loopback BPDU inconsistency (see Figure 294)

Example

```
Force10#show spanning-tree msti 10
MSTI 10 VLANs mapped  101-105

Bridge Identifier has priority 32768, Address 0001.e802.3506
Configured hello time 2, max age 20, forward delay 15, max hops 5
Current root has priority 16384, Address 0001.e800.0a5c
Number of topology changes 0, last change occured 3058087

Port 82 (GigabitEthernet 2/0) is designated Forwarding
Port path cost 0, Port priority 128, Port Identifier 128.82
Designated root has priority 16384, address 0001.e800.0a:5c
Designated bridge has priority 32768, address 0001.e802.35:06
Designated port id is 128.82, designated path cost
Number of transitions to forwarding state 1
BPDU (Mrecords): sent 1109, received 0
The port is not in the portfast mode

Port 88 (GigabitEthernet 2/6) is root Forwarding
Port path cost 0, Port priority 128, Port Identifier 128.88
Designated root has priority 16384, address 0001.e800.0a:5c
Designated bridge has priority 16384, address 0001.e800.0a:5c
Designated port id is 128.88, designated path cost
Number of transitions to forwarding state 4
BPDU (Mrecords): sent 19, received 1103
The port is not in the portfast mode

Port 89 (GigabitEthernet 2/7) is alternate Discarding
Port path cost 0, Port priority 128, Port Identifier 128.89
Designated root has priority 16384, address 0001.e800.0a:5c
Designated bridge has priority 16384, address 0001.e800.0a:5c
Designated port id is 128.89, designated path cost
Number of transitions to forwarding state 3
BPDU (Mrecords): sent 7, received 1103
The port is not in the portfast mode

Force10#
```

Figure 293 show spanning-tree msti *instance-number*

Example 2

```
Force10#show spanning-tree msti 0 brief
MSTI 0 VLANs mapped  1-4094

Executing IEEE compatible Spanning Tree Protocol
Root ID    Priority 32768, Address 0001.e801.6aa8
Root Bridge hello time 2, max age 20, forward delay 15, max hops 20
Bridge ID    Priority 32768, Address 0001.e801.6aa8
We are the root of MSTI 0 (CIST)
Configured hello time 2, max age 20, forward delay 15, max hops 20
CIST regional root ID Priority 32768, Address 0001.e801.6aa8
CIST external path cost 0

Interface                                        Designated
 Name      PortID   Prio Cost    Sts Cost        Bridge ID         PortID
---------- -------- ---- ------- --- ------- -------------------- --------
Gi 0/0     128.257  128  20000   EDS 0       32768 0001.e801.6aa8 128.257

Interface
 Name      Role   PortID   Prio Cost    Sts Cost    Link-type Edge Boundary
---------- ------ -------- ---- ------- --- ------- --------- ---- --------
Gi 0/0     ErrDis 128.257  128  20000   EDS 0       P2P       No   No

Force10#show spanning-tree msti 0
MSTI 0 VLANs mapped  1-4094

Root Identifier has priority 32768, Address 0001.e801.6aa8
Root Bridge hello time 2, max age 20, forward delay 15, max hops 20
Bridge Identifier has priority 32768, Address 0001.e801.6aa8
Configured hello time 2, max age 20, forward delay 15, max hops 20
We are the root of MSTI 0 (CIST)
Current root has priority 32768, Address 0001.e801.6aa8
CIST regional root ID Priority 32768, Address 0001.e801.6aa8
CIST external path cost 0
Number of topology changes 1, last change occured 00:00:15 ago on Gi 0/0

Port 257 (GigabitEthernet 0/0) is LBK_INC Discarding
Port path cost 20000, Port priority 128, Port Identifier 128.257
Designated root has priority 32768, address 0001.e801.6aa8
Designated bridge has priority 32768, address 0001.e801.6aa8
Designated port id is 128.257, designated path cost 0
Number of transitions to forwarding state 1
BPDU (MRecords): sent 21, received 9
The port is not in the Edge port mode
```

Loopback BPDU Inconsistency (LBK_INC)

Figure 294 show spanning-tree msti with EDS and LBK

Usage Information You must enable Multiple Spanning Tree Protocol prior to using this command.

spanning-tree

Enable Multiple Spanning Tree Protocol on the interface.

Syntax **spanning-tree <cr>**

To disable the Multiple Spanning Tree Protocol on the interface, use **no spanning-tree**

Parameters		
	spanning-tree	Enter the keyword **spanning-tree** to enable the MSTP on the interface. Default: Enable

Defaults Enable

Command Modes INTERFACE

spanning-tree msti

Configure Multiple Spanning Tree instance cost and priority for an interface.

Syntax **spanning-tree msti** *instance* {**cost** *cost* | **priority** *priority*}

To remove the cost or priority for the MST instance, use
no spanning-tree msti *instance* {**cost** *cost* | **priority** *priority*}

Parameters		
	msti *instance*	Enter the keyword **msti** and the MST Instance number. Range: zero (0) to 63
	cost *cost*	(OPTIONAL) Enter the keyword **cost** followed by the port cost value. Range: 1 to 200000 Defaults: 100 Mb/s Ethernet interface = 200000 1-Gigabit Ethernet interface = 20000 10-Gigabit Ethernet interface = 2000 Port Channel interface with one 100 Mb/s Ethernet = 200000 Port Channel interface with one 1-Gigabit Ethernet = 20000 Port Channel interface with one 10-Gigabit Ethernet = 2000 Port Channel with two 1-Gigabit Ethernet = 18000 Port Channel with two 10-Gigabit Ethernet = 1800 Port Channel with two 100-Mbps Ethernet = 180000
	priority *priority*	Enter keyword **priority** followed by a value in increments of 16 as the priority. Range: 0 to 240. Default: 128

Defaults *cost* = depends on the interface type; *priority* = 128

Command Modes INTERFACE

spanning-tree mstp edge-port

Configures the interface as an Multiple Spanning Tree edge port and optionally a Bridge Protocol Data Unit (BPDU) guard.

Syntax **spanning-tree mstp edge-port {bpduguard}**

Parameters

mstp edge-port	Enter the keywords **mstp** followed by the keyword **edge-port** to configure the interface as a Multiple Spanning Tree edge port.
bpduguard	(OPTIONAL) Enter the keyword **bpduguard** to prevent the port from participating in the active STP topology in case a BPDU shows up on a port unintentionally, is misconfigured, or subject to a DOS attack. This option places the port into an error disable state if a BPDU appears, and a message is logged for the administrator to take corrective action.

Command Modes INTERFACE

Command History

Version 6.1.1.0	Support for BPDU guard added

Usage Information On an MSTP switch, a port configured as an edge port will immediately transition to the forwarding state. Only ports connected to end-hosts should be configured as an edge port. Consider an edge port similar to a port with spanning-tree portfast enabled.

tc-flush-standard

Enable the MAC address flushing upon receiving every topology change notification.

Syntax **tc-flush-standard**

To disable, use the **no tc-flush-standard** command.

Defaults Disabled

Command Modes CONFIGURATION

Command History

Version 6.5.1.0	Introduced

Usage Information By default FTOS implements an optimized flush mechanism for MSTP. This helps in flushing the MAC addresses only when necessary (and less often) allowing for faster convergence during topology changes. However, if a standards-based flush mechanism is needed, this *knob* command can be turned on to enable flushing MAC addresses upon receiving every topology change notification.

Chapter 36 Router Information Protocol

Platform Specific Feature: Router Information Protocol is supported on E-Series only.

Router Information Protocol (RIP) is a Distance Vector routing protocol. The FTOS supports both RIP version 1 (RIPv1) and RIP version 2 (RIPv2). The FTOS implementation of RIP is based on IETF RFCs 2453 and RFC 1058.

For more information on configuring RIP on the E-Series, refer to *FTOS Configuration Guide*. The following commands allow you to configure and enable RIP on the E-Series.

- auto-summary on page 840
- clear ip rip on page 840
- debug ip rip on page 841
- default-information originate on page 841
- default-metric on page 842
- distance on page 843
- distribute-list in on page 843
- distribute-list out on page 844
- ip poison-reverse on page 845
- ip rip receive version on page 845
- ip rip send version on page 846
- ip split-horizon on page 847
- maximum-paths on page 847
- neighbor on page 848
- network on page 848
- offset-list on page 849
- output-delay on page 850
- passive-interface on page 850
- redistribute on page 851
- redistribute isis on page 852
- redistribute ospf on page 852

- router rip on page 853
- show config on page 854
- show ip rip database on page 854
- timers basic on page 855
- version on page 856

auto-summary

C-Series	No
E-Series	✓

Restore the default behavior of automatic summarization of subnet routes into network routes. This command applies only to RIP version 2.

Syntax **auto-summary**

To send sub-prefix routing information, enter **no auto-summary**.

Default Enabled.

Command Modes ROUTER RIP

clear ip rip

C-Series	No
E-Series	✓

Clear all the RIP routes from the FTOS routing table.

Syntax **clear ip rip**

Command Modes EXEC privilege

Usage Information This command triggers updates of the main RIP routing tables.

debug ip rip

C-Series	No
E-Series	✓

Examine RIP routing information for troubleshooting.

Syntax **debug ip rip** [*interface* | **database** | **events** | **trigger**]

To turn off debugging output, use the **no debug ip rip** command.

Parameters

interface	(OPTIONAL) Enter the interface type slot/port as one of the following: • For a Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For a Port Channel, enter the keyword **port-channel** followed by a number from 1 to 32 for EtherScale, 1 to 255 for TeraScale. • For a SONET interface, enter the keyword **sonet** followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information. • For a VLAN, enter the keyword **vlan** followed by a number from 1 to 4094.
database	(OPTIONAL) Enter the keyword **database** to display messages when there is a change to the RIP database.
events	(OPTIONAL) Enter the keyword **events** to debug only RIP protocol changes.
trigger	(OPTIONAL) Enter the keyword **trigger** to debug only RIP trigger extensions.

Command Modes EXEC privilege

default-information originate

C-Series	No
E-Series	✓

Generate a default route for the RIP traffic.

Syntax **default-information originate** [**always**] [**metric** *metric-value*] [**route-map** *map-name*]

To return to the default values, enter **no default-information originate**.

Parameters

always	(OPTIONAL) Enter the keyword **always** to enable the E-Series software to always advertise the default route.
metric *metric-value*	(OPTIONAL) Enter the keyword **metric** followed by a number as the metric value. Range: 1 to 16
route-map *map-name*	(OPTIONAL) Enter the keyword **route-map** followed by the name of a configured route-map.

Defaults Disabled.

Command Modes ROUTER RIP

Usage Information The default route must be present in the E-Series routing table for the default-information originate command to take effect.

default-metric

C-Series	No
E-Series	✓

Change the default metric for routes. Use this command with the **redistribute** command to ensure that all redistributed routes use the same metric value.

Syntax **default-metric** *number*

To return the default metric to the original values, enter **no default-metric**.

Parameters

number	Specify a number. Range: 1 to 16. The default is 1.

Default 1

Command Modes ROUTER RIP

Usage Information This command ensures that route information being redistributed is converted to the same metric value.

Related Commands

redistribute	Allows you to redistribute routes learned by other methods.

distance

C-Series	No
E-Series	✓

Assign a weight or prioritization for all routes in the RIP routing table or only RIP routes using a certain IP address.

Syntax **distance** *weight* [*ip-address mask*]

To return to the default values, use the **no distance** *weight* [*ip-address mask*] command.

Parameters

weight	Enter a number from 1 to 255. The default is 120.
ip-address	(OPTIONAL) Enter the IP address, in dotted decimal format (A.B.C.D), of the host or network to receive the new distance metric. If you enter an IP address, you must also enter an mask for that IP address.
mask	(OPTIONAL) Enter a network mask in /prefix format (/x).

Defaults *weight* = 120

Command Modes ROUTER RIP

Related Commands

default-metric	Assign one distance metric to all routes learned using the redistribute command.

distribute-list in

C-Series	No
E-Series	✓

Configure a filter for incoming routing updates.

Syntax **distribute-list** *prefix-list-name* **in** [*interface*]

To delete the filter, use the **no distribute-list** *prefix-list-name* **in** command.

Parameters

prefix-list-name	Enter the name of a configured prefix list.
interface	(OPTIONAL) Identifies the interface type slot/port as one of the following: • For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For a Port Channel interface, enter the keyword **port-channel** followed by a a number from 1 to 32 for EtherScale, 1 to 255 for TeraScale. • For a SONET interface, enter the keyword **sonet** followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information. • For a VLAN, enter the keyword **vlan** followed by a number from 1 to 4094.

Defaults Not configured.

Command Modes ROUTER RIP

distribute-list out

C-Series	No
E-Series	✓

Configure a filter for outgoing routing updates.

Syntax **distribute-list** *prefix-list-name* **out** [*interface* | **bgp | connected** | **isis** | **ospf** | **static**]

To delete the filter, use the **no distribute-list** *prefix-list-name* **out** command.

Parameters

prefix-list-name	Enter the name of a configured prefix list.
interface	(OPTIONAL) Identifies the interface type slot/port as one of the following: • For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For a Port Channel interface, enter the keyword **port-channel** followed by a number from 1 to 32 for EtherScale, 1 to 255 for TeraScale. • For a SONET interface, enter the keyword **sonet** followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information. • For a VLAN, enter the keyword **vlan** followed by a number from 1 to 4094.
bgp	(OPTIONAL) Enter the keyword **bgp** to filter only BGP routes.
connected	(OPTIONAL) Enter the keyword **connected** to filter only directly connected routes.
isis	(OPTIONAL) Enter the keyword **isis** to filter only IS-IS routes.

ospf	(OPTIONAL) Enter the keyword **ospf** to filter all OSPF routes.
static	(OPTIONAL) Enter the keyword **static** to filter manually configured routes.

Defaults Not configured.

Command Modes ROUTER RIP

ip poison-reverse

C-Series	No
E-Series	✓

Set the prefix of the RIP routing updates to the RIP infinity value.

Syntax **ip poison-reverse**

To disable poison reverse, enter **no ip poison-reverse**.

Defaults Disabled.

Command Modes INTERFACE

Related Commands

ip split-horizon	Set RIP routing updates to exclude routing prefixes.

ip rip receive version

C-Series	No
E-Series	✓

Set the interface to receive specific versions of RIP. The RIP version you set on the interface overrides the version command in the ROUTER RIP mode.

Syntax **ip rip receive version** [1] [2]

To return to the default, enter **no ip rip receive version**.

Parameters

1	(OPTIONAL) Enter the number **1** for RIP version 1.
2	(OPTIONAL) Enter the number **2** for RIP version 2.

Defaults RIPv1 and RIPv2.

Command Modes INTERFACE

Usage Information If you want the interface to receive both versions of RIP, enter **ip rip receive version 1 2**.

Related Commands

ip rip send version	Sets the RIP version to be used for sending RIP traffic on an interface.
version	Sets the RIP version to be used for the E-Series software.

ip rip send version

C-Series	**No**
E-Series	✓

Set the interface to send a specific version of RIP. The version you set on the interface overrides the version command in the ROUTER RIP mode.

Syntax **ip rip send version** [1] [2]

To return to the default value, enter **no ip rip send version**.

Parameters

1	(OPTIONAL) Enter the number **1** for RIP version 1. The default is RIPv1.
2	(OPTIONAL) Enter the number **2** for RIP version 2.

Defaults RIPv1.

Command Modes INTERFACE

Usage Information To enable the interface to send both version of RIP packets, enter **ip rip send version 1 2**.

Related Commands

ip rip receive version	Sets the RIP version for the interface to receive traffic.
version	Sets the RIP version to be used for the E-Series software.

ip split-horizon

C-Series	No
E-Series	✓

Enable split-horizon for RIP data on the interface. As described in RFC 2453, the split-horizon scheme prevents any routes learned over a specific interface to be sent back out that interface.

Syntax **ip split-horizon**

To disable split-horizon, enter **no ip split-horizon.**

Defaults Enabled

Command Modes INTERFACE

Related Commands

ip poison-reverse	Set the prefix for RIP routing updates.

maximum-paths

C-Series	No
E-Series	✓

Set RIP to forward packets over multiple paths.

Syntax **maximum-paths** *number*

To return to the default values, enter **no maximum-paths**.

Parameters

number	Enter the number of paths. Range: 1 to 16. The default is 4 paths.

Defaults 4

Command Modes ROUTER RIP

Usage Information RIP supports a maximum of 16 ECMP paths.

neighbor

C-Series	No
E-Series	✓

Define a neighbor router with which to exchange RIP information.

Syntax

neighbor *ip-address*

To delete a neighbor setting, use the **no neighbor** *ip-address* command.

Parameters

ip-address	Enter the IP address, in dotted decimal format, of a router with which to exchange information.

Defaults

Not configured.

Command Modes

ROUTER RIP

Usage Information

When a neighbor router is identified, unicast data exchanges occur. Multiple neighbor routers are possible.

Use the passive-interface command in conjunction with the neighbor command to ensure that only specific interfaces are receiving and sending data.

Related Commands

passive-interface	Sets the interface to only listen to RIP broadcasts.

network

C-Series	No
E-Series	✓

Enable RIP for a specified network. Use this command to enable RIP on all networks connected to the E-Series.

Syntax

network *ip-address*

To disable RIP for a network, use the **no network** *ip-address* command.

Parameter

ip-address	Specify an IP network address in dotted decimal format. You cannot specify a subnet.

Defaults

No RIP network is configured.

Command Modes ROUTER RIP

Usage Information You can enable an unlimited number of RIP networks.

RIP operates over interfaces configured with any address specified by the network command.

offset-list

C-Series	No
E-Series	✓

Specify a number to add to the incoming or outgoing route metrics learned via RIP.

Syntax **offset-list** *prefix-list-name* {**in** | **out**} *offset* [*interface*]

To delete an offset list, use the **no offset-list** *prefix-list-name* {**in** | **out**} *offset* [*interface*] command.

Parameters

prefix-list-name	Enter the name of an established Prefix list to determine which incoming routes will be modified.
offset	Enter a number from zero (0) to 16 to be applied to the incoming route metric matching the access list specified. If you set an offset value to zero (0), no action is taken.
interface	(OPTIONAL) Enter the following keywords and slot/port or number information: • For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For a Port Channel interface, enter the keyword **port-channel** followed by a number from 1 to 32 for EtherScale, 1 to 255 for TeraScale. • For a SONET interface, enter the keyword **sonet** followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information. • For a VLAN, enter the keyword **vlan** followed by a number from 1 to 4094.

Defaults Not configured.

Command Modes ROUTER RIP

Usage Information When the offset metric is applied to an interface, that value takes precedence over an offset value that is not extended to an interface.

output-delay

C-Series	No
E-Series	✓

Set the interpacket delay of successive packets to the same neighbor.

Syntax **output-delay** *delay*

To return to the E-Series software defaults for interpacket delay, enter **no output-delay**.

Parameters

delay	Specify a number of milliseconds as the delay interval. Range: 8 to 50.

Default Not configured.

Command Modes ROUTER RIP

Usage Information This command is intended for low-speed interfaces.

passive-interface

C-Series	No
E-Series	✓

Suppress routing updates on a specified interface.

Syntax **passive-interface** *interface*

To delete a passive interface, use the **no passive-interface** *interface* command.

Parameters

interface	Enter the following information: • For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For a Port Channel interface, enter the keyword **port-channel** followed by a number from 1 to 32 for EtherScale, 1 to 255 for TeraScale. • For a SONET interface, enter the keyword **sonet** followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information. • For a VLAN, enter the keyword **vlan** followed by a number from 1 to 4094.

Defaults Not configured.

Command Modes ROUTER RIP

Usage Information Although the passive interface will neither send nor receive routing updates, the network on that interface will still be included in RIP updates sent via other interfaces.

Related Commands

neighbor	Enable RIP for a specified network.
network	Define a neighbor.

redistribute

C-Series	**No**
E-Series	✓

Redistribute information from other routing instances.

Syntax **redistribute** {**connected** | **static**}

To disable redistribution, use the **no redistribute** {**connected** | **static**} command.

Parameters

connected	Enter the keyword **connected** to specify that information from active routes on interfaces is redistributed.
static	Enter the keyword **static** to specify that information from static routes is redistributed.

Defaults Not configured.

Command Modes ROUTER RIP

Usage Information To redistribute the default route (0.0.0.0/0), configure the default-information originate command.

Related Commands

default-information originate	Generate a default route for RIP traffic.

redistribute isis

C-Series	No
E-Series	✓

Redistribute routing information from an IS-IS instance.

Syntax **redistribute isis** [*tag*] [**level-1** | **level-1-2** | **level-2**] [**metric** *metric-value*] [**route-map** *map-name*]

To disable redistribution, use the **no redistribute isis** [*tag*] [**level-1** | **level-1-2** | **level-2**] [**metric** *metric-value*] [**route-map** *map-name*] command.

Parameters

tag	(OPTIONAL) Enter the name of the IS-IS routing process.
level-1	(OPTIONAL) Enter the keyword **level-1** to redistribute only IS-IS Level-1 routes.
level-1-2	(OPTIONAL) Enter the keyword **level-1-2** to redistribute both IS-IS Level-1 and Level-2 routes.
level-2	(OPTIONAL) Enter the keyword **level-2** to redistribute only IS-IS Level-2 routes.
metric *metric-value*	(OPTIONAL) Enter the keyword **metric** followed by a number as the metric value. Range: 0 to16
route-map *map-name*	(OPTIONAL) Enter the keyword **route-map** followed by the name of a configured route map.

Defaults Not configured.

Command Modes ROUTER RIP

redistribute ospf

C-Series	No
E-Series	✓

Redistribute routing information from an OSPF process.

Syntax **redistribute ospf** *process-id* [**match external** {**1** | **2**} | **match internal** | **metric** *metric-value*] [**route-map** *map-name*]

To disable redistribution, enter no **redistribute ospf** *process-id* [**match external** {**1** | **2**} | **match internal** | **metric** *metric-value*] [**route-map** *map-name*] command.

Parameters

process-id	Enter a number that corresponds to the OSPF process ID to be redistributed. Range: 1 to 65355.
match external {**1** | **2**}	(OPTIONAL) Enter the keywords **match external** followed by the numbers 1 or 2 to indicated that external 1 routes or external 2 routes should be redistributed.
match internal	(OPTIONAL) Enter the keywords **match internal** to indicate that internal routes should be redistributed.
metric *metric-value*	(OPTIONAL) Enter the keyword **metric** followed by a number as the metric value. Range: 0 to16
route-map *map-name*	(OPTIONAL) Enter the keyword **route-map** followed by the name of a configured route map.

Defaults Not configured.

Command Modes ROUTER RIP

router rip

C-Series	**No**
E-Series	✓

Enter the ROUTER RIP mode to configure and enable RIP.

Syntax **router rip**

To disable RIP, enter **no router rip**.

Defaults Disabled.

Command Modes CONFIGURATION

Usage Information To enable RIP, you must assign a network address using the network command.

Example

```
Force10(conf)#router rip
Force10(conf-router_rip)#
```

Figure 295 router rip Command Example

Related Commands		
	network	Enable RIP.
	exit	Return to the CONFIGURATION mode.

show config

C-Series	No
E-Series	✓

View the changes you made to the RIP configuration. Default values are not shown.

Syntax **show config**

Command Modes ROUTER RIP

Example

```
Force10(conf-router_rip)#show config
!
router rip
 network 172.31.0.0
 passive-interface  GigabitEthernet 0/1
Force10(conf-router_rip)#
```

Figure 296 show config Command Example in ROUTER RIP Mode

show ip rip database

C-Series	No
E-Series	✓

View the routes learned by RIP. If the E-Series learned no RIP routes, no output is generated.

Syntax **show ip rip database** [*ip-address mask*]

Parameters

ip-address	(OPTIONAL) Specify an IP address in dotted decimal format to view RIP information on that network only. If you enter an IP address, you must also enter a mask for that IP address.
mask	(OPTIONAL) Specify a mask, in /network format, for the IP address.

Command Modes

EXEC

EXEC privilege

Example

```
Force10#show ip rip database
Total number of routes in RIP database: 1624
204.250.54.0/24
        [50/1] via 192.14.1.3, 00:00:12, GigabitEthernet 9/15
204.250.54.0/24         auto-summary
203.250.49.0/24
        [50/1] via 192.13.1.3, 00:00:12, GigabitEthernet 9/14
203.250.49.0/24         auto-summary
210.250.40.0/24
        [50/2] via 1.1.18.2, 00:00:14, Vlan 18
        [50/2] via 1.1.130.2, 00:00:12, Port-channel 30
210.250.40.0/24         auto-summary
207.250.53.0/24
        [50/2] via 6.1.6.1, 00:00:16, SONET 2/1
        [50/2] via 1.1.120.2, 00:00:55, Port-channel 20
        [50/2] via 1.1.130.2, 00:00:12, Port-channel 30
        [50/2] via 1.1.10.2, 00:00:18, Vlan 10
207.250.53.0/24         auto-summary
208.250.42.0/24
        [50/2] via 6.1.6.1, 00:00:16, SONET 2/1
        [50/2] via 1.1.120.2, 00:00:55, Port-channel 20
        [50/2] via 1.1.130.2, 00:00:12, Port-channel 30
        [50/2] via 1.1.10.2, 00:00:18, Vlan 10
208.250.42.0/24         auto-summary
```

Figure 297 show ip rip database Command Example (partial)

Table 68 describes the information displayed in the Figure 297.

Table 68 Fields in show ip rip database Command Output

Field	Description
Total number of routes in RIP database	Displays the number of RIP routes stored in the RIP database.
100.10.10.0/24 directly connected	Lists the route(s) directly connected.
150.100.0.0 redistributed	Lists the routes learned through redistribution.
209.9.16.0/24 ...	Lists the routes and the sources advertising those routes.

timers basic

Manipulate the RIP timers for routing updates, invalid, holddown times and flush time.

C-Series	No
E-Series	✓

Syntax **timers basic** *update invalid holddown flush*

To return to the default settings, enter **no timers basic**.

Parameters

update	Enter the number of seconds to specify the rate at which RIP routing updates are sent. Range: zero (0) to 4294967295. Default: 30 seconds.
invalid	Enter the number of seconds to specify the time interval before routing updates are declared invalid or expired. The *invalid* value should be at least three times the *update* timer value. Range: zero (0) to 4294967295. Default: 180 seconds.
holddown	Enter the number of seconds to specify a time interval during which the route is marked as unreachable but still sending RIP packets. The *holddown* value should be at least three times the *update* timer value. Range: zero (0) to 4294967295. Default: 180 seconds.
flush	Enter the number of seconds to specify the time interval during which the route is advertised as unreachable. When this interval expires, the route is flushed from the routing table. The *flush* value should be greater than the *update* value. Range: zero (0) to 4294967295. Default is 240 seconds.

Defaults *update* = 30 seconds; *invalid* = 180 seconds; *holddown* = 180 seconds; *flush* = 240 seconds.

Command Modes ROUTER RIP

Usage Information If the timers on one router are changed, the timers on all routers in the RIP domain must also be synchronized.

version

C-Series	No
E-Series	✓

Specify either RIP version 1 or RIP version 2.

Syntax **version** {**1** | **2**}

To return to the default version setting, enter **no version**.

Parameters

1	Enter the keyword **1** to specify RIP version 1.
2	Enter the keyword **2** to specify RIP version 2.

Default The FTOS sends RIPv1 and receives RIPv1 and RIPv2.

Command Modes ROUTER RIP

Related Commands

ip rip receive version	Set the RIP version to be received on the interface.
ip rip send version	Set the RIP version to be sent out the interface.

Chapter 37 OSPF

Open Shortest Path First (OSPF) is an Interior Gateway Protocol (IGP), which means that it distributes routing information between routers in a single Autonomous System (AS). OSPF is also a link-state protocol in which all routers contain forwarding tables derived from information about their links to their neighbors.

The Force10 Networks implementation of OSPF is based on IETF RFC 2328. The following commands allow you to configure and enable OSPF.

- area default-cost on page 861
- area nssa on page 861
- area range on page 862
- area stub on page 862
- area virtual-link on page 863
- auto-cost on page 864
- clear ip ospf on page 865
- clear ip ospf statistics on page 865
- debug ip ospf on page 866
- default-information originate on page 867
- default-metric on page 868
- distance on page 869
- distance ospf on page 869
- distribute-list in on page 870
- distribute-list out on page 871
- enable inverse mask on page 871
- flood-2328 on page 872
- graceful-restart grace-period on page 872
- graceful-restart helper-reject on page 873
- graceful-restart mode on page 873
- graceful-restart role on page 873
- ip ospf auth-change-wait-time on page 874
- ip ospf authentication-key on page 874
- ip ospf cost on page 875
- ip ospf dead-interval on page 875

- ip ospf hello-interval on page 876
- ip ospf message-digest-key on page 876
- ip ospf mtu-ignore on page 877
- ip ospf mtu-ignore on page 877
- ip ospf priority on page 878
- ip ospf retransmit-interval on page 879
- ip ospf transmit-delay on page 879
- log-adjacency-changes on page 880
- maximum-paths on page 880
- network area on page 880
- passive-interface on page 881
- redistribute on page 883
- redistribute bgp on page 884
- redistribute isis on page 884
- router ospf on page 886
- show config on page 887
- show ip ospf on page 887
- show ip ospf asbr on page 888
- show ip ospf database on page 889
- show ip ospf database asbr-summary on page 890
- show ip ospf database external on page 892
- show ip ospf database network on page 893
- show ip ospf database nssa-external on page 895
- show ip ospf database opaque-area on page 896
- show ip ospf database opaque-as on page 897
- show ip ospf database opaque-link on page 898
- show ip ospf database router on page 898
- show ip ospf database summary on page 900
- show ip ospf interface on page 902
- show ip ospf neighbor on page 904
- show ip ospf route on page 904
- show ip ospf statistics on page 905
- show ip ospf topology on page 909
- show ip ospf virtual-links on page 909
- summary-address on page 910
- timers spf on page 911

area default-cost

Set the metric for the summary default route generated by the area border router (ABR) into the stub area. Use this command on the border routers at the edge of a stub area.

Syntax **area** *area-id* **default-cost** *cost*

To return default values, use the **no area** *area-id* **default-cost** command.

Parameters

area-id	Specify the OSPF area in dotted decimal format (A.B.C.D.) or enter a number from zero (0) to 65535.
cost	Specifies the stub area's advertised external route metric. Range: zero (0) to 65535.

Defaults *cost* = 1; no areas are configured.

Command Modes ROUTER OSPF

Usage Information In the FTOS, cost is defined as reference bandwidth/bandwidth.

Related Commands

area stub	Create a stub area.

area nssa

Allows you to specify an area as a Not So Stubby Area (NSSA).

Syntax **area** *area-id* **nssa** [**default-information-originate**] [**no-redistribution**] [**no-summary**]

To delete an NSSA, enter **no area** *area-id* **nssa**.

Parameters

area-id	Specify the OSPF area in dotted decimal format (A.B.C.D) or enter a number from 0 and 65535.
no-redistribution	(OPTIONAL) Specify that the redistribute command should not distribute routes into the NSSA. You should only use this command in a NSSA Area Border Router (ABR).
default-information-originate	(OPTIONAL) Allows external routing information to be imported into the NSSA by using Type 7 default.
no-summary	(OPTIONAL) Specify that no summary LSAs should be sent into the NSSA.

Defaults Not configured.

Command Mode ROUTER OSPF

area range

Summarize routes matching an address/mask at an area border router (ABR).

Syntax **area** *area-id* **range** *ip-address mask* [**not-advertise**]

To disable route summarization, use the **no area** *area-id* **range** *ip-address mask* command.

Parameters

area-id	Specify the OSPF area in dotted decimal format (A.B.C.D.) or enter a number from zero (0) to 65535.
ip-address	Specify an IP address in dotted decimal format.
mask	Specify a mask for the destination prefix. Enter the full mask (for example, 255.255.255.0).
not-advertise	(OPTIONAL) Enter the keyword **not-advertise** to set the status to DoNotAdvertise (that is, the Type 3 summary-LSA is suppressed and the component networks remain hidden from other areas.)

Defaults No range is configured.

Command Modes ROUTER OSPF

Usage Information Only the routes within an area are summarized, and that summary is advertised to other areas by the ABR. External routes are not summarized.

Related Commands

area stub	Create a stub area.

area stub

Allows you to configure a stub area, which is an area not connected to other areas.

Syntax **area** *area-id* **stub** [**no-summary**]

To delete a stub area, enter **no area** *area-id* **stub**.

Parameters

area-id	Specify the stub area in dotted decimal format (A.B.C.D.) or enter a number from zero (0) to 65535.
no-summary	(OPTIONAL) Enter the keyword **no-summary** to prevent the ABR from sending summary Link State Advertisements (LSAs) into the stub area.

Defaults Disabled

Command Modes ROUTER OSPF

Usage Information Use this command to configure all routers and access servers within a stub.

area virtual-link

Allows you to set a virtual-link and its parameters.

Syntax **area** *area-id* **virtual-link** *router-id* [**authentication-key** *key*] [**dead-interval** *seconds*] [**hello-interval** *seconds*] [**message-digest-key** *keyid* **md5** *key*] [**retransmit-interval** *seconds*] [**transmit-delay** *seconds*]

To delete a virtual link, use the **no area** *area-id* **virtual-link** *router-id* command.

To delete a parameter of a virtual-link, use the **no area** *area-id* **virtual-link** *router-id* [**hello-interval** *seconds* | **retransmit-interval** *seconds* | **transmit-delay** *seconds* | **dead-interval** *seconds* | **authentication-key** *key* | **message-digest-key** *keyid* **md5** *key*] command.

Parameters

area-id	Specify the transit area for the virtual link in dotted decimal format (A.B.C.D.) or enter a number from zero (0) to 65535.
router-id	Specify an IP address in the dotted decimal format.
authentication-key *key*	(OPTIONAL) Enter the keyword **authentication-key** to enable simple authentication followed by an alphanumeric string up to 8 characters long.
dead-interval *seconds*	(OPTIONAL) Enter the keyword **dead-interval** followed by a number as the number of *seconds* for the interval. Range: 1 to 8192. Default: 40 seconds.
hello-interval *seconds*	(OPTIONAL) Enter the keyword **hello-interval** followed by the number of *seconds* for the interval. Range: 1 to 8192. Default: 10 seconds.
message-digest-key *keyid* **md5** *key*	(OPTIONAL) Enter the keyword **message-digest-key** followed by a number from 1 to 255 as the *keyid*. After the *keyid*, enter the keyword **md5** followed by the *key*. The *key* is an alphanumeric string up to 16 characters long.

retransmit-interval *seconds*	(OPTIONAL) Enter the keyword **retransmit-interval** followed by the number of *seconds* for the interval. Range: 1 to 8192. Default: 5 seconds.
transmit-delay *seconds*	(OPTIONAL) Enter the keyword **transmit-delay** followed by the number of *seconds* for the interval. Range: 1 to 8192. Default: 1 second.

Defaults **dead-interval** *seconds* = 40 seconds; **hello-interval** *seconds* = 10 seconds; **retransmit-interval** *seconds* = 5 seconds; **transmit-delay** *seconds* = 1 second

Command Modes ROUTER OSPF

Usage Information All OSPF areas must be connected to a backbone area (usually Area 0). Virtual links connect broken or discontiguous areas.

You cannot enable both authentication options. Choose either the **authentication-key** or **message-digest-key** option.

auto-cost

Specify how the OSPF interface cost is calculated based on the reference bandwidth method.

Syntax **auto-cost** [**reference-bandwidth** *ref-bw*]

To return to the default bandwidth or to assign cost based on the interface type, use the **no auto-cost** [**reference-bandwidth**] command.

Parameters

ref-bw	(OPTIONAL) Specify a reference bandwidth in megabits per second. Range: 1 to 4294967 Default: 100 megabits per second.

Defaults 100 megabits per second.

Command Modes ROUTER OSPF

clear ip ospf

Clear all OSPF routing tables.

Syntax **clear ip ospf** [**process**]

Parameters

process	(OPTIONAL) Enter the keyword **process** to reset the OSPF process.

Command Modes EXEC privilege

clear ip ospf statistics

Clear the packet statistics in interfaces and neighbors.

Syntax **clear ip ospf statistics** [**interface** *name* {**neighbor** *router-id*}]

Parameters

interface *name*	(OPTIONAL) Enter the keyword **interface** followed by one of the following interface keywords and slot/port or number information: • For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For Port Channel groups, enter the keyword **port-channel** followed by a number: C-Series Range: 1-128 E-Series Range: 1-32 for EtherScale, 1-255 for TeraScale • For a SONET interface, enter the keyword **sonet** followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information. • For a VLAN, enter the keyword **vlan** followed by a number from 1 to 4094.
neighbor *router-id*	(OPTIONAL) Enter the keyword **neighbor** followed by the neighbor's router-id in dotted decimal format (A.B.C.D.).

Defaults No defaults values or behavior

Command Modes EXEC privilege

Command History

Version 7.4.1.0	Introduced

Related Commands

show ip ospf statistics	Display the OSPF statistics

debug ip ospf

View debug information on OSPF. Entering **debug ip ospf** enables all OSPF debugging parameters.

Syntax **debug ip ospf** [**event** | **packet** | **spf**]

To cancel the debug command, enter **no debug ip ospf**.

Parameters

event	(OPTIONAL) Enter the keyword **event** to debug only OSPF event information.
packet	(OPTIONAL) Enter the keyword **packet** to debug only OSPF packet information.
spf	(OPTIONAL) Enter the keyword **spf** to view the Shortest Path First (spf) information.

Command Modes EXEC privilege

Example

```
Force10#debug ip ospf packet
Force10#
08:14:24 : OSPF(100:00):
Xmt. v:2 t:1(HELLO) l:44 rid:192.1.1.1
        aid:0.0.0.1 chk:0xa098 aut:0 auk: keyid:0 to:Gi 4/3 dst:224.0.0.5
            netmask:255.255.255.0 pri:1 N-, MC-, E+, T-,
            hi:10 di:40 dr:90.1.1.1 bdr:0.0.0.0
```

Figure 298 debug ip ospf Output

Table 69 describes the information in Figure 298.

Table 69 debug ip ospf Output Fields

Field	Description
8:14	Displays the time stamp.
OSPF	Displays the OSPF process ID: instance ID. FTOS supports only one instance of OSPF, so the instance ID is always 0.
v:	Displays the OSPF version. FTOS supports version 2 only.
t:	Displays the type of packet sent: • 1 - Hello packet • 2 - database description • 3 - link state request • 4 - link state update • 5 - link state acknowledgement
l:	Displays the packet length.
rid:	Displays the OSPF router ID.
aid:	Displays the Autonomous System ID.
chk:	Displays the OSPF checksum.

Table 69 debug ip ospf Output Fields

Field	Description
aut:	States if OSPF authentication is configured. One of the following is listed: • 0 - no authentication configured • 1 - simple authentication configured using the ip ospf authentication-key command) • 2 - MD5 authentication configured using the ip ospf message-digest-key command.
auk:	If the ip ospf authentication-key command is configured, this field displays the key used.
keyid:	If the ip ospf message-digest-key command is configured, this field displays the MD5 key
to:	Displays the interface to which the packet is intended.
dst:	Displays the destination IP address.
netmask:	Displays the destination IP address mask.
pri:	Displays the OSPF priority
N, MC, E, T	Displays information available in the Options field of the HELLO packet: • N + (N-bit is set) • N - (N-bit is not set) • MC+ (bit used by MOSPF is set and router is able to forward IP multicast packets) • MC- (bit used by MOSPF is not set and router cannot forward IP multicast packets) • E + (router is able to accept AS External LSAs) • E - (router cannot accept AS External LSAs) • T + (router can support TOS) • T - (router cannot support TOS)
hi:	Displays the amount of time configured for the HELLO interval.
di:	Displays the amount of time configured for the DEAD interval.
dr:	Displays the IP address of the designated router.
bdr:	Displays the IP address of the Border Area Router.

default-information originate

Configure the FTOS to generate a default external route into an OSPF routing domain.

Syntax **default-information originate** [**always**] [**metric** *metric-value*] [**metric-type** *type-value*] [**route-map** *map-name*]

To return to the default values, enter **no default-information originate**.

Parameters

always	(OPTIONAL) Enter the keyword **always** to specify that default route information must always be advertised.
metric *metric-value*	(OPTIONAL) Enter the keyword metric followed by a number to configure a metric value for the route. Range: 1 to 16777214
metric-type *type-value*	(OPTIONAL) Enter the keyword **metric-type** followed by an OSPF link state type of 1 or 2 for default routes. The values are: • 1 = Type 1 external route • 2 = Type 2 external route.
route-map *map-name*	(OPTIONAL) Enter the keyword **route-map** followed by the name of an established route map.

Defaults Disabled.

Command Modes ROUTER OSPF

Related Commands

redistribute	Redistribute routes from other routing protocols into OSPF.

default-metric

Change the metrics of redistributed routes to a value useful to OSPF. Use this command with the redistribute command.

Syntax **default-metric** *number*

To return to the default values, enter **no default-metric**.

Parameters

number	Enter a number as the metric. Range: 1 to 16777214.

Defaults Disabled.

Command Modes ROUTER OSPF

Related Commands

redistribute	Redistribute routes from other routing protocols into OSPF.

distance

Define an administrative distance for particular routes to a specific IP address.

Syntax **distance** *weight* [*ip-address mask access-list-name*]

To delete the settings, use the **no distance** *weight* [*ip-address mask access-list-name*] command.

Parameters

weight	Specify an administrative distance. Range: 1 to 255. Default: 110
ip-address	(OPTIONAL) Enter a router ID in the dotted decimal format. If you enter a router ID, you must include the mask for that router address.
mask	(OPTIONAL) Enter a mask in dotted decimal format or /n format.
access-list-name	(OPTIONAL) Enter the name of an IP standard access list.

Defaults 110

Command Modes ROUTER OSPF

distance ospf

Configure an OSPF distance metric for different types of routes.

Syntax **distance ospf** [**external** *dist3*] [**inter-area** *dist2*] [**intra-area** *dist1*]

To delete these settings, enter **no distance ospf**.

Parameters

external *dist3*	(OPTIONAL) Enter the keyword **external** followed by a number to specify a distance for external type 5 and 7 routes. Range: 1 to 255 Default: 110.
inter-area *dist2*	(OPTIONAL) Enter the keyword **inter-area** followed by a number to specify a distance metric for routes between areas. Range: 1 to 255 Default: 110.
intra-area *dist1*	(OPTIONAL) Enter the keyword **intra-area** followed by a number to specify a distance metric for all routes within an area. Range: 1 to 255 Default: 110.

Defaults **external** *dist3* = 110; **inter-area** *dist2* = 110; **intra-area** *dist1* = 110.

Command Modes ROUTER OSPF

Usage Information To specify a distance for routes learned from other routing domains, use the redistribute command.

distribute-list in

Apply a filter to incoming routing updates from OSPF to the routing table.

Syntax **distribute-list** *prefix-list-name* **in** [*interface*]

To delete a filter, use the **no distribute-list** *prefix-list-name* **in** [*interface*] command.

Parameters

prefix-list-name	Enter the name of a configured prefix list.
interface	(OPTIONAL) Enter one of the following keywords and slot/port or number information: • For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For Port Channel groups, enter the keyword **port-channel** followed by a number: C-Series Range: 1-128 E-Series Range: 1-32 for EtherScale, 1-255 for TeraScale • For a SONET interface, enter the keyword **sonet** followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information. • For a VLAN, enter the keyword **vlan** followed by a number from 1 to 4094.

Defaults Not configured.

Command Modes ROUTER OSPF

distribute-list out

Apply a filter to restrict certain routes destined for the local routing table after SPF calculation.

Syntax **distribute-list** *prefix-list-name* **out** [**connected** | **isis** | **rip** | **static**]

To remove a filter, use the **no distribute-list** *prefix-list-name* **out** [**connected** | **isis** | **rip** | **static**] command.

Parameters

prefix-list-name	Enter the name of a configured prefix list.
connected	(OPTIONAL) Enter the keyword **connected** to specify that connected routes are distributed.
isis	(OPTIONAL) Enter the keyword **isis** to specify that IS-IS routes are distributed.
rip	(OPTIONAL) Enter the keyword **rip** to specify that RIP routes are distributed.
static	(OPTIONAL) Enter the keyword **static** to specify that only manually configured routes are distributed.

Defaults Not configured.

Command Modes ROUTER OSPF

Usage Information The distribute-list out command applies to routes being redistributed by autonomous system boundary routers (ASBRs) into OSPF. It can be applied to external type 2 and external type 1 routes, but not to intra-area and inter-area routes.

enable inverse mask

FTOS, by default, permits user to input OSPF **network** command with net-mask. This command provides a choice between inverse-mask or net-mask (the default).

Syntax **enable inverse mask**

To return to the default net-mask, enter **no enable inverse mask**

Defaults net-mask

Command Modes CONFIGURATION

flood-2328

Enable RFC-2328 flooding behavior.

Syntax **flood-2328**

To disable, use the **no flood-2328** command.

Defaults Disabled

Command Modes ROUTER OSPF (conf-router-ospf)

Command History

Version 7.5.1.0	Introduced

Usage Information In OSPF, flooding is the most resource-consuming task. The flooding algorithm, described in RFC-2328, requires that OSPF flood LSAs (Link State Advertisements) on all interfaces, as governed by LSA's flooding scope (see Section 13 of the RFC). When multiple direct links connect two routers, the RFC-2328 flooding algorithm generates significant redundant information across all links.

By default, FTOS implements an enhanced flooding procedure that dynamically and intelligently determines when to optimize flooding. Whenever possible, the OSPF task attempts to reduce flooding overhead by selectively flooding on a subset of the interfaces between two routers.

When **flood-2328** is enabled, this command configures FTOS to flood LSAs on all interfaces.

graceful-restart grace-period

Specifies the time duration, in seconds, that the router's neighbors will continue to advertise the router as fully adjacent regardless of the synchronization state during a graceful restart.

Syntax **graceful-restart grace-period** *seconds*

To disable gace periord, enter **no graceful-restart grace-period**

Parameters

seconds	Time duration, in seconds, that specifies the duration of the restart process before OSPF terminates the process. Range: 40 to 3000 seconds

Defaults Not Configured

Command Modes ROUTER OSPF

graceful-restart helper-reject

Specify the OSPF router to not act as a helper during graceful restart.

Syntax **graceful-restart helper-reject** *ip-address*

To return to default value, enter **no graceful-restart helper-reject**.

Parameters

ip-address	Enter the OSPF router-id, in IP address format, of the restart router that *will not* act as a helper during graceful restart.

Defaults Not Configured

Command Modes ROUTER OSPF

graceful-restart mode

Enable the graceful restart mode.

Syntax **graceful-restart mode** [**planned-only** \ **unplanned-only**]

To disable graceful restart mode, enter **no graceful-restart mode**.

Parameters

planned-only	(OPTIONAL) Enter the keywords **planned-only** to indicate graceful restart is supported in a planned restart condition only.
unplanned-only	(OPTIONAL) Enter the keywords **unplanned-only** to indicate graceful restart is supported in an unplanned restart condition only.

Defaults Support for both planned and unplanned failures.

Command Modes ROUTER OSPF

graceful-restart role

Specify the role for your OSPF router during graceful restart.

Syntax **graceful-restart role** [**helper-only** \ **restart-only**]

To disable graceful restart role, enter **no graceful-restart role**.

Parameters		
	role helper-only	(OPTIONAL) Enter the keywords **helper-only** to specify the OSPF router is a helper only during graceful restart.
	role restart-only	(OPTIONAL) Enter the keywords **restart-only** to specify the OSPF router is a restart only during graceful-restart.

Defaults OSPF routers are, by default, both helper and restart routers during a graceful restart.

Command Modes ROUTER OSPF

ip ospf auth-change-wait-time

OSPF provides a grace period while OSPF chages its interface authentication type. During the grace period, OSPF sends out packets with new and old authentication scheme till the grace period expires.

Syntax **ip ospf auth-change-wait-time** *seconds*

To return to the default, enter **no ip ospf auth-change-wait-time**.

Parameters		
	seconds	Enter seconds Range: 0 to 300

Defaults zero (0) seconds

Command Modes INTERFACE

ip ospf authentication-key

Enable authentication and set an authentication key on OSPF traffic on an interface.

Syntax **ip ospf authentication-key** [*encryption-type*] *key*

To delete an authentication key, enter **no ip ospf authentication-key**.

Parameters		
	encryption-type	(OPTIONAL) Enter 7 to encrypt the key.
	key	Enter an 8 character string. Strings longer than 8 characters are truncated.

Defaults Not configured.

Command Modes INTERFACE

Usage Information All neighboring routers in the same network must use the same password to exchange OSPF information.

ip ospf cost

Change the cost associated with the OSPF traffic on an interface.

Syntax **ip ospf cost** *cost*

To return to default value, enter **no ip ospf cost**.

Parameters

cost	Enter a number as the cost. Range: 1 to 65535.

Defaults The default cost is based on the reference bandwidth.

Command Modes INTERFACE

Usage Information If this command is not configured, cost is based on the auto-cost command.

When you configure OSPF over multiple vendors, use the ip ospf cost command to ensure that all routers use the same cost. Otherwise, OSPF routes improperly.

Related Commands

auto-cost	Control how the OSPF interface cost is calculated.

ip ospf dead-interval

Set the time interval since the last hello-packet was received from a router. After the interval elapses, the neighboring routers declare the router dead.

Syntax **ip ospf dead-interval** *seconds*

To return to the default values, enter **no ip ospf dead-interval**.

Parameters

seconds	Enter the number of seconds for the interval. Range: 1 to 65535. Default: 40 seconds.

Defaults 40 seconds

Command Modes INTERFACE

Usage Information By default, the dead interval is four times more than the default hello-interval.

Related Commands

ip ospf hello-interval	Set the time interval between hello packets.

ip ospf hello-interval

Specify the time interval between the hello packets sent on the interface.

Syntax **ip ospf hello-interval** *seconds*

To return to the default value, enter **no ip ospf hello-interval**.

Parameters

seconds	Enter a the number of second as the delay between hello packets. Range: 1 to 65535. Default: 10 seconds.

Defaults 10 seconds

Command Modes INTERFACE

Usage Information The time interval between hello packets must be the same for routers in a network.

Related Commands

ip ospf dead-interval	Set the time interval before a router is declared dead.

ip ospf message-digest-key

Enable OSPF MD5 authentication and send an OSPF message digest key on the interface.

Syntax **ip ospf message-digest-key** *keyid* **md5** *key*

To delete a key, use the **no ip ospf message-digest-key** *keyid* command.

Parameters

keyid	Enter a number as the key ID. Range: 1 to 255.
key	Enter a continuous character string as the password.

Defaults No MD5 authentication is configured.

Command Modes INTERFACE

Usage Information To change to a different key on the interface, enable the new key while the old key is still enabled. The FTOS will send two packets: the first packet authenticated with the old key, and the second packet authenticated with the new key. This process ensures that the neighbors learn the new key and communication is not disrupted by keeping the old key enabled.

After the reply is received and the new key is authenticated, you must delete the old key. Force10 Networks recommends keeping only one key per interface.

Note: The MD5 secret is stored as plain text in the configuration file with service password encryption.

ip ospf mtu-ignore

Disable OSPF MTU mismatch detection upon receipt of database description (DBD) packets.

Syntax **ip ospf mtu-ignore**

To return to the default, enter **no ip ospf mtu-ignore**.

Defaults Enabled

Command Modes INTERFACE

ip ospf network

Set the network type for the interface.

Syntax **ip ospf network** {**broadcast** | **point-to-point**}

To return to the default, enter **no ip ospf network**.

Parameters

broadcast	Enter the keyword **broadcast** to designate the interface as part of a broadcast network.
point-to-point	Enter the keyword **point-to-point** to designate the interface as part of a point-to-point network.

Defaults Not configured.

Command Modes ROUTER OSPF

ip ospf priority

Set the priority of the interface to determine the Designated Router for the OSPF network.

Syntax **ip ospf priority** *number*

To return to the default setting, enter **no ip ospf priority**.

Parameters

number	Enter a number as the priority. Range: 0 to 255. The default is 1.

Defaults 1

Command Modes INTERFACE

Usage Information Setting a priority of 0 makes the router ineligible for election as a Designated Router or Backup Designated Router.

Use this command for interfaces connected to multi-access networks, not point-to-point networks.

ip ospf retransmit-interval

Set the retransmission time between lost link state advertisements (LSAs) for adjacencies belonging to the interface.

Syntax **ip ospf retransmit-interval** *seconds*

To return to the default values, enter **no ip ospf retransmit-interva**l.

Parameters

seconds	Enter the number of seconds as the interval between retransmission. Range: 1 to 3600. Default: 5 seconds. This interval must be greater than the expected round-trip time for a packet to travel between two routers.

Defaults 5 seconds

Command Modes INTERFACE

Usage Information Set the time interval to a number large enough to prevent unnecessary retransmissions. For example, the interval should be larger for interfaces connected to virtual links.

ip ospf transmit-delay

Set the estimated time elapsed to send a link state update packet on the interface.

Syntax **ip ospf transmit-delay** *seconds*

To return to the default value, enter **no ip ospf transmit-delay**.

Parameters

seconds	Enter the number of seconds as the transmission time. This value should be greater than the transmission and propagation delays for the interface. Range: 1 to 3600. Default: 1 second.

Defaults 1 second

Command Modes INTERFACE

log-adjacency-changes

Set the E-Series software to send a Syslog message about changes in the OSPF adjacency state.

Syntax **log-adjacency-changes**

To disable the Syslog messages, enter **no log-adjacency-changes**.

Defaults Disabled.

Command Mode ROUTER OSPF

maximum-paths

Enable the software to forward packets over multiple paths.

Syntax **maximum-paths** *number*

To disable packet forwarding over multiple paths, enter **no maximum-paths**.

Parameters

number	Specify the number of paths. Range: 1 to 16. Default: 4 paths.

Defaults 4

Command Modes ROUTER OSPF

network area

Define which interfaces run OSPF and the OSPF area for those interfaces.

Syntax **network** *ip-address mask* **area** *area-id*

To disable an OSPF area, use the **no network** *ip-address mask* **area** *area-id* command.

Parameters

ip-address	Specify a primary or secondary address in dotted decimal format. The primary address is required before adding the secondary address.
mask	Enter a network mask in /prefix format. (/x)
area-id	Enter the OSPF area ID as either a decimal value or in a valid IP address. Decimal value range: 0 to 65535 IP address format: dotted decimal format A.B.C.D. **Note:** If the area ID is smaller than 65535, it will be converted to a decimal value. For example, if you use an area ID of 0.0.0.1, it will be converted to 1.

Command Modes ROUTER OSPF

Usage Information To enable OSPF on an interface, the network area command must include, in its range of addresses, the primary IP address of an interface.

Note: An interface can be attached only to a single OSPF area.

If you delete all the network area commands for Area 0, the show ip ospf command output will not list Area 0.

passive-interface

Suppress both receiving and sending routing updates on an interface.

Syntax **passive-interface** {**default** | *interface*}

To enable both the receiving and sending routing, enter the **no passive-interface** *interface* command.

To return all OSPF interfaces (current and future) to active, enter the **no passive-interface default** command.

Parameters

default	Enter the keyword **default** to make all OSPF interfaces (current and future) passive.
interface	Enter the following keywords and slot/port or number information: • For a Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For Port Channel groups, enter the keyword **port-channel** followed by a number: C-Series Range: 1-128 E-Series Range: 1-32 for EtherScale, 1-255 for TeraScale • For a SONET interface, enter the keyword **sonet** followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information. • For a VLAN, enter the keyword **vlan** followed by a number from 1 to 4094.

Command Modes

ROUTER OSPF

Command History

Version 7.4.1.0	Modified to include the **default** keyword.

Usage Information

Although the passive interface will neither send nor receive routing updates, the network on that interface will still be included in OSPF updates sent via other interfaces.

The default keyword sets all interfaces as passive. You can then configure individual interfaces, where adjacencies are desired, using the **no passive-interface** *interface* command. The no form of this command is inserted into the configuration for individual interfaces when the **no passive-interface** *interface* command is issued while **passive-interface default** is configured.

This command behavior has changed as follows:

passive-interface *interface*

- The previous **no passive-interface** *interface* is removed from the running configuration.
- The ABR status for the router is updated.
- Save **passive-interface** *interface* into the running configuration.

passive-interface default

- All present and future OSPF interface are marked as *passive*.
- Any adjacency are explicitly terminated from all OSPF interfaces.
- All previous **passive-interface** *interface* commands are removed from the running configuration.
- All previous **no passive-interface** *interface* commands are removed from the running configuration.

no passive-interface *interface*

- Remove the interface from the passive list.
- The ABR status for the router is updated.

- If **passive-interface default** is specified, then save **no passive-interface** *interface* into the running configuration.

No passive-interface default

- Clear everything and revert to the default behavior.
- All previously marked passive interfaces are removed.
- May update ABR status.

redistribute

Redistribute information from another routing protocol throughout the OSPF process.

Syntax

redistribute {**connected** | **rip** | **static**} [**metric** *metric-value* | **metric-type** *type-value*] [**route-map** *map-name*] [**tag** *tag-value*]

To disable redistribution, use the **no redistribute** {**connected** | **isis** | **rip** | **static**} command.

Parameters

connected	Enter the keyword **connected** to specify that information from active routes on interfaces is redistributed.
rip	Enter the keyword **rip** to specify that RIP routing information is redistributed.
static	Enter the keyword **static** to specify that information from static routes is redistributed.
metric *metric-value*	(OPTIONAL) Enter the keyword **metric** followed by a number. Range: 0 (zero) to 16777214.
metric-type *type-value*	(OPTIONAL) Enter the keyword **metric-type** followed by one of the following: • 1 = OSPF External type 1 • 2 = OSPF External type 2
route-map *map-name*	(OPTIONAL) Enter the keyword **route-map** followed by the name of the route map.
tag *tag-value*	(OPTIONAL) Enter the keyword **tag** followed by a number. Range: 0 to 4294967295

Defaults

Not configured.

Command Modes

ROUTER OSPF

Usage Information

To redistribute the default route (0.0.0.0/0), configure the default-information originate command.

Related Commands		
	default-information originate	Generate a default route into the OSPF routing domain.

redistribute bgp

Redistribute BGP routing information throughout the OSPF instance.

Syntax **redistribute bgp** *as number* [**metric** *metric-value*] | [**metric-type** *type-value*] | [**tag** *tag-value*]

To disable redistribution, use the **no redistribute bgp** *as number* [**metric** *metric-value*] | [**metric-type** *type-value*] | [**tag** *tag-value*] command.

Parameters

as number	Enter the autonomous system number. Range: 1 to 65535
metric *metric-value*	(OPTIONAL) Enter the keyword **metric** followed by the metric-value number. Range: 0 to16777214
metric-type *type-value*	(OPTIONAL) Enter the keyword **metric-type** followed by one of the following: • 1 = for OSPF External type 1 • 2 = for OSPF External type 2
tag *tag-value*	(OPTIONAL) Enter the keyword **tag** to set the tag for routes redistributed into OSPF. Range: 0 to 4294967295

Defaults No default behavior or values

Command Modes CONFIGURATION ROUTER OSPF (conf-router_ospf)

redistribute isis

Allows you to redistribute IS-IS routing information throughout the OSPF instance.

Syntax **redistribute isis** [*tag*] [**level-1** | **level-1-2** | **level-2**] [**metric** *metric-value* | **metric-type** *type-value*] [**route-map** *map-name*] [**tag** *tag-value*]

To disable redistribution, use the **no redistribute isis** [*tag*] [**level-1** | **level-1-2** | **level-2**] [**metric** *metric-value* | **metric-type** *type-value*] [**route-map** *map-name*] [**tag** *tag-value*] command.

Parameters

tag	(OPTIONAL) Enter the name of the IS-IS routing process.
level-1	(OPTIONAL) Enter the keyword **level-1** to redistribute only IS-IS Level-1 routes.
level-1-2	(OPTIONAL) Enter the keyword **level-1-2** to redistribute both IS-IS Level-1 and Level-2 routes.
level-2	(OPTIONAL) Enter the keyword **level-2** to redistribute only IS-IS Level-2 routes.
metric *metric-value*	(OPTIONAL) Enter the keyword **metric** followed by a number. Range: 0 (zero) to 4294967295.
metric-type *type-value*	(OPTIONAL) Enter the keyword **metric-type** followed by one of the following: • 1 = for OSPF External type 1 • 2 = for OSPF External type 2
route-map *map-name*	(OPTIONAL) Enter the keyword **route-map** followed by the name of the route map.
tag *tag-value*	(OPTIONAL) Enter the keyword **tag** followed by a number. Range: 0 to 4294967295

Defaults Not configured.

Command Modes ROUTER OSPF

router-id

Use this command to configure a fixed rounter ID.

Syntax **router-id** *ip-address*

To remove the fixed router-id, use the **no router-id** *ip-address* command.

Parameters

ip-address	Enter the router ID in the IP address format

Defaults This command has no default behavior or values.

Command Modes ROUTER OSPF

Example

```
Force10(conf)#router ospf  100
Force10(conf-router_ospf)#router-id 1.1.1.1
Changing router-id will bring down existing OSPF adjacency [y/n]:


Force10(conf-router_ospf)#show config
!
router ospf 100
router-id 1.1.1.1
Force10(conf-router_ospf)#no router-id
Changing router-id will bring down existing OSPF adjacency [y/n]:
Force10#
```

Figure 299 router-id Command Examples

Usage Information

You can configure an arbitrary value in the IP address format for each router. However, each router ID must be unique. If this command is used on an OSPF router process, which is already active (that is, has neighbors), a prompt reminding you that changing router-id will bring down the existing OSPF adjacency. The new router ID is effective at the next reload

router ospf

Enter the ROUTER OSPF mode to configure an OSPF instance.

Syntax **router ospf** *process-id*

To clear an OSPF instance, enter **no router ospf**.

Parameters

process-id	Enter a number for the OSPF instance. Range: 1 to 65535.

Defaults Not configured.

Command Modes CONFIGURATION

Example

```
Force10(conf)#router ospf 2
Force10(conf-router_ospf)#
```

Figure 300 router ospf Command Example

Usage Information

You must have an IP address assigned to an interface to enter the ROUTER OSPF mode and configure OSPF. Only one instance of OSPF is supported per E-Series system.

show config

View the non-default values in the current OSPF configuration.

Syntax **show config**

Command Modes ROUTER OSPF

Example

```
Force10(conf-router_ospf)#show config
!
router ospf 3
 passive-interface FastEthernet 0/1
Force10(conf-router_ospf)#
```

Figure 301 show config Command Example

show ip ospf

View information on the OSPF process configured on the E-Series.

Syntax **show ip ospf**

Command Modes EXEC

EXEC privilege mode

Usage Information If you delete all the network area commands for Area 0, the show ip ospf command output will not list Area 0.

Example

```
Force10>show ip ospf
Routing Process ospf 1 with ID 11.1.2.1
Supports only single TOS (TOS0) routes
It is an autonomous system boundaryrouter
SPF schedule delay 0 secs, Hold time between two SPFs 5 secs
Number of area in this router is 1, normal 1 stub 0 nssa 0
   Area BACKBONE (0.0.0.0)
       Number of interface in this area is 2
       SPF algorithm executed 4 times
       Area ranges are
Force10>
```

Figure 302 show ip ospf Command Example

Table 70 describes the information found in Figure 302

Table 70 show ip ospf Command Example

Line Beginning with	Description
“Routing Process...”	Displays the OSPF process ID and the IP address associated with the process ID.
“Supports only...”	Displays the number of Type of Service (TOS) rouse supported.
“SPF schedule...”	Displays the delay and hold time configured for this process ID.
“Number of...”	Displays the number and type of areas configured for this process ID.

Related Commands

show ip ospf database	Displays information about the OSPF routes configured.
show ip ospf interface	Displays the OSPF interfaces configured.
show ip ospf neighbor	Displays the OSPF neighbors configured.
show ip ospf virtual-links	Displays the OSPF virtual links configured.

show ip ospf asbr

Display all ASBR routers visible to OSPF.

Syntax

show ip ospf asbr

Defaults

No default values or behavior

Command Modes

EXEC

EXEC privilege

Command History

Version 7.5.1.0	Introduced

Usage Information

Use this command to isolate problems with external routes. In OSPF, external routes are calculated by add LSA cost to the cost of reaching the ASBR router. If an external route is not of correct cost, use this command to determine if the path to the originating router is correct. The display output is not sorted in any order.

Note: ASBR’s that are not in directly connected areas, are also displayed.

Example

```
Force10#show ip ospf asbr

RouterID         Flags    Cost   Nexthop         Interface    Area
3.3.3.3         -/-/-/   2      10.0.0.2        Gi 0/1       1
1.1.1.1          E/-/-/   0      0.0.0.0          -            0
Force10#
```

Figure 303 show ip ospf asbr Command Example

You can to determine if an ASBR is in a directly connected area (or not) by the flags. For ASBRs in a directly connect area, E flags are set. In Figure 303, router 1.1.1.1 is in a directly connect area since the Flags is E/-/-/. For remote ASBRs, the E flags is clear (-/-/-/)

show ip ospf database

View all LSA information. If OSPF is not enabled on the E-Series, no output is generated.

Syntax **show ip ospf database** [**database-summary**]

Parameters

database-summary	(OPTIONAL) Enter the keywords **database-summary** to the view the number of LSA types in each area and the total number of LSAs.

Command Modes EXEC

EXEC privilege

Example

```
Force10>show ip ospf database

            OSPF Router with ID (11.1.2.1) (Process ID 1)
                Router (Area 0.0.0.0)
Link ID         ADV Router        Age     Seq#          Checksum    Link count
11.1.2.1        11.1.2.1          673     0x80000005    0x707e          2
13.1.1.1        13.1.1.1          676     0x80000097    0x1035          2
192.68.135.2    192.68.135.2      1419    0x80000294    0x9cbd          1

                Network (Area 0.0.0.0)
Link ID         ADV Router        Age     Seq#          Checksum
10.2.3.2        13.1.1.1          676     0x80000003    0x6592
10.2.4.2        192.68.135.2      908     0x80000055    0x683e

                Type-5 AS External
Link ID         ADV Router        Age     Seq#          Checksum  Tag
0.0.0.0         192.68.135.2      908     0x80000052    0xeb83    100
1.1.1.1         192.68.135.2      908     0x8000002a    0xbd27    0
10.1.1.0        11.1.2.1          718     0x80000002    0x9012    0
10.1.2.0        11.1.2.1          718     0x80000002    0x851c    0
10.2.2.0        11.1.2.1          718     0x80000002    0x7927    0
10.2.3.0        11.1.2.1          718     0x80000002    0x6e31    0
10.2.4.0        13.1.1.1          1184    0x80000068    0x45db    0
11.1.1.0        11.1.2.1          718     0x80000002    0x831e    0
11.1.2.0        11.1.2.1          718     0x80000002    0x7828    0
12.1.2.0        192.68.135.2      1663    0x80000054    0xd8d6    0
13.1.1.0        13.1.1.1          1192    0x8000006b    0x2718    0
13.1.2.0        13.1.1.1          1184    0x8000006b    0x1c22    0
172.16.1.0      13.1.1.1          148     0x8000006d    0x533b    0
Force10>
```

Figure 304 show ip ospf database Command Example

Table 71 describes the fields in the Figure 304.

Table 71 show ip ospf database Command Example Fields

Field	Description
Link ID	Identifies the router ID.
ADV Router	Identifies the advertising router's ID.
Age	Displays the link state age.
Seq#	Identifies the link state sequence number. This number allows you to identify old or duplicate link state advertisements.
Checksum	Displays the Fletcher checksum of an LSA's complete contents.
Link count	Displays the number of interfaces for that router.

Related Commands

show ip ospf database asbr-summary	Displays only ASBR summary LSA information.

show ip ospf database asbr-summary

View information about AS Boundary LSAs.

Syntax **show ip ospf database asbr-summary** [*link-state-id*] [**adv-router** *ip-address*]

Parameters

link-state-id	(OPTIONAL) Specify LSA ID in dotted decimal format. The LSA ID value depends on the LSA type, and it can be one of the following: • the network's IP address for Type 3 LSAs or Type 5 LSAs • the router's OSPF router ID for Type 1 LSAs or Type 4 LSAs • the default destination (0.0.0.0) for Type 5 LSAs
adv-router *ip-address*	(OPTIONAL) Enter the keywords **adv-router** ip-address to display only the LSA information about that router.

Command Modes EXEC

EXEC privilege

Example

```
Force10#show ip ospf database asbr-summary

            OSPF Router with ID (1.1.1.10) (Process ID 100)

                Summary Asbr (Area 0.0.0.0)

  LS age: 1437
  Options: (No TOS-capability, No DC, E)
  LS type: Summary Asbr
  Link State ID: 103.1.50.1
  Advertising Router: 1.1.1.10
  LS Seq Number: 0x8000000f
  Checksum: 0x8221
  Length: 28
  Network Mask: /0
       TOS: 0 Metric: 2

  LS age: 473
  Options: (No TOS-capability, No DC, E)
  LS type: Summary Asbr
  Link State ID: 104.1.50.1
  Advertising Router: 1.1.1.10
  LS Seq Number: 0x80000010
  Checksum: 0x4198
  Length: 28
--More--
```

Figure 305 show ip ospf database asbr-summary Command Example (Partial)

Table 72 describes the information displayed in Figure 305.

Table 72 show ip ospf database asbr-summary Command Example fields

Item	Description
LS Age	Displays the LSA's age.
Options	Displays the optional capabilities available on router. The following options can be found in this item: • TOS-capability or No TOS-capability is displayed depending on whether the router can support Type of Service. • DC or No DC is displayed depending on whether the originating router can support OSPF over demand circuits. • E or No E is displayed on whether the originating router can accept AS External LSAs.
LS Type	Displays the LSA's type.
Link State ID	Displays the Link State ID.
Advertising Router	Identifies the advertising router's ID.
Checksum	Displays the Fletcher checksum of the an LSA's complete contents.
Length	Displays the length in bytes of the LSA.
Network Mask	Displays the network mask implemented on the area.
TOS	Displays the Type of Service (TOS) options. Option 0 is the only option.
Metric	Displays the LSA metric.

Related Commands

show ip ospf database	Displays OSPF database information.

show ip ospf database external

View information on the AS external (type 5) LSAs.

Syntax **show ip ospf database external** [*link-state-id*] [**adv-router** *ip-address*]

Parameters

link-state-id	(OPTIONAL) Specify LSA ID in dotted decimal format. The LSA ID value depends on the LSA type, and it can be one of the following: • the network's IP address for Type 3 LSAs or Type 5 LSAs • the router's OSPF router ID for Type 1 LSAs or Type 4 LSAs • the default destination (0.0.0.0) for Type 5 LSAs
adv-router *ip-address*	(OPTIONAL) Enter the keywords **adv-router** ip-address to display only the LSA information about that router.

Command Modes EXEC

EXEC privilege

Example

```
Force10#show ip ospf database external

            OSPF Router with ID (20.20.20.5) (Process ID 1)

                Type-5 AS External

  LS age: 612
  Options: (No TOS-capability, No DC, E)
  LS type: Type-5 AS External
  Link State ID: 12.12.12.2
  Advertising Router: 20.31.3.1
  LS Seq Number: 0x80000007
  Checksum: 0x4cde
  Length: 36
  Network Mask: /32
       Metrics Type: 2
       TOS: 0
       Metrics: 25
       Forward Address: 0.0.0.0
       External Route Tag: 43

  LS age: 1868
  Options: (No TOS-capability, DC)
  LS type: Type-5 AS External
  Link State ID: 24.216.12.0
  Advertising Router: 20.20.20.8
  LS Seq Number: 0x80000005
  Checksum: 0xa00e
  Length: 36
  Network Mask: /24
       Metrics Type: 2
       TOS: 0
       Metrics: 1
       Forward Address: 0.0.0.0
       External Route Tag: 701
Force10#
```

Figure 306 show ip ospf database external Command Example

Table 73 describes the information displayed in Figure 306.

Table 73 show ip ospf database external Command Example Fields

Item	Description
LS Age	Displays the LSA age.
Options	Displays the optional capabilities available on router. The following options can be found in this item: • TOS-capability or No TOS-capability is displayed depending on whether the router can support Type of Service. • DC or No DC is displayed depending on whether the originating router can support OSPF over demand circuits. • E or No E is displayed on whether the originating router can accept AS External LSAs.
LS Type	Displays the LSA's type.
Link State ID	Displays the Link State ID.
Advertising Router	Identifies the router ID of the LSA's originating router.
LS Seq Number	Identifies the link state sequence number. This number allows you to identify old or duplicate LSAs.
Checksum	Displays the Fletcher checksum of an LSA's complete contents.
Length	Displays the length in bytes of the LSA.
Network Mask	Displays the network mask implemented on the area.
Metrics Type	Displays the external type.
TOS	Displays the TOS options. Option 0 is the only option.
Metrics	Displays the LSA metric.
Forward Address	Identifies the address of the forwarding router. Data traffic is forwarded to this router. If the forwarding address is 0.0.0.0, data traffic is forwarded to the originating router.
External Route Tag	Displays the 32-bit field attached to each external route. This field is not used by the OSPF protocol, but can be used for external route management.

Related Commands

show ip ospf database	Displays OSPF database information.

show ip ospf database network

View the network (type 2) LSA information.

Syntax **show ip ospf database network** [*link-state-id*] [**adv-router** *ip-address*]

Parameters

link-state-id	(OPTIONAL) Specify LSA ID in dotted decimal format. The LSA ID value depends on the LSA type, and it can be one of the following: • the network's IP address for Type 3 LSAs or Type 5 LSAs • the router's OSPF router ID for Type 1 LSAs or Type 4 LSAs • the default destination (0.0.0.0) for Type 5 LSAs
adv-router *ip-address*	(OPTIONAL) Enter the keywords **adv-router** ip-address to display only the LSA information about that router.

Command Modes

EXEC

EXEC privilege

Example

```
Force10#show ip ospf data network

            OSPF Router with ID (20.20.20.5) (Process ID 1)

                Network (Area 0.0.0.0)

  LS age: 1372
  Options: (No TOS-capability, DC, E)
  LS type: Network
  Link State ID: 202.10.10.2
  Advertising Router: 20.20.20.8
  LS Seq Number: 0x80000006
  Checksum: 0xa35
  Length: 36
  Network Mask: /24
       Attached Router: 20.20.20.8
       Attached Router: 20.20.20.9
       Attached Router: 20.20.20.7

                Network (Area 0.0.0.1)

  LS age: 252
  Options: (TOS-capability, No DC, E)
  LS type: Network
  Link State ID: 192.10.10.2
  Advertising Router: 192.10.10.2
  LS Seq Number: 0x80000007
  Checksum: 0x4309
  Length: 36
  Network Mask: /24
       Attached Router: 192.10.10.2
       Attached Router: 20.20.20.1
       Attached Router: 20.20.20.5
Force10#
```

Figure 307 show ip ospf database network Command Example

Table 74 describes the information displayed in Figure 307.

Table 74 show ip ospf database network Command Example fields

Item	Description
LS Age	Displays the LSA age.
Options	Displays the optional capabilities available on router. The following options can be found in this item: • TOS-capability or No TOS-capability is displayed depending on whether the router can support Type of Service. • DC or No DC is displayed depending on whether the originating router can support OSPF over demand circuits. • E or No E is displayed on whether the originating router can accept AS External LSAs.
LS Type	Displays the LSA's type.
Link State ID	Displays the Link State ID.
Advertising Router	Identifies the router ID of the LSA's originating router.
Checksum	Identifies the link state sequence number. This number allows you to identify old or duplicate LSAs.
Length	Displays the Fletcher checksum of an LSA's complete contents.
Network Mask	Displays the length in bytes of the LSA.
Attached Router	Identifies the IP address of routers attached to the network.

Related Commands

show ip ospf database	Displays OSPF database information.

show ip ospf database nssa-external

View NSSA-External (type 7) LSA information.

Syntax **show ip ospf database nssa-external** [*link-state-id*] [**adv-router** *ip-address*]

Parameters

link-state-id	(OPTIONAL) Specify LSA ID in dotted decimal format. The LSA ID value depends on the LSA type, and it can be one of the following: • the network's IP address for Type 3 LSAs or Type 5 LSAs • the router's OSPF router ID for Type 1 LSAs or Type 4 LSAs • the default destination (0.0.0.0) for Type 5 LSAs
adv-router *ip-address*	(OPTIONAL) Enter the keywords **adv-router** ip-address to display only the LSA information about that router.

Command Modes

EXEC

EXEC privilege

Related Commands

show ip ospf database	Displays OSPF database information.

show ip ospf database opaque-area

View the opaque-area (type 10) LSA information.

Syntax **show ip ospf database opaque-area** [*link-state-id*] [**adv-router** *ip-address*]

Parameters

link-state-id	(OPTIONAL) Specify LSA ID in dotted decimal format. The LSA ID value depends on the LSA type, and it can be one of the following: • the network's IP address for Type 3 LSAs or Type 5 LSAs • the router's OSPF router ID for Type 1 LSAs or Type 4 LSAs • the default destination (0.0.0.0) for Type 5 LSAs
adv-router *ip-address*	(OPTIONAL) Enter the keywords **adv-router** ip-address to display only the LSA information about that router.

Command Modes EXEC

EXEC privilege

Example

```
Force10>show ip ospf database opaque-area

            OSPF Router with ID (3.3.3.3) (Process ID 1)

                Type-10 Opaque Link Area (Area 0)

  LS age: 1133
  Options: (No TOS-capability, No DC, E)
  LS type: Type-10 Opaque Link Area
  Link State ID: 1.0.0.1
  Advertising Router: 10.16.1.160
  LS Seq Number: 0x80000416
  Checksum: 0x376
  Length: 28
  Opaque Type: 1
  Opaque ID: 1
  Unable to display opaque data

  LS age: 833
  Options: (No TOS-capability, No DC, E)
  LS type: Type-10 Opaque Link Area
  Link State ID: 1.0.0.2
  Advertising Router: 10.16.1.160
  LS Seq Number: 0x80000002
  Checksum: 0x19c2
--More--
```

Figure 308 show ip ospf database opaque-area Command Example (Partial)

Table 75 describes the information in Figure 308.

Table 75 show ip ospf database opaque-area Command Example Fields

Item	Description
LS Age	Displays the LSA's age.
Options	Displays the optional capabilities available on router. The following options can be found in this item: • TOS-capability or No TOS-capability is displayed depending on whether the router can support Type of Service. • DC or No DC is displayed depending on whether the originating router can support OSPF over demand circuits. • E or No E is displayed on whether the originating router can accept AS External LSAs.
LS Type	Displays the LSA's type.
Link State ID	Displays the Link State ID.
Advertising Router	Identifies the advertising router's ID.
Checksum	Displays the Fletcher checksum of the an LSA's complete contents.
Length	Displays the length in bytes of the LSA.
Opaque Type	Displays the Opaque type field (the first 8 bits of the Link State ID).
Opaque ID	Displays the Opaque type-specific ID (the remaining 24 bits of the Link State ID).

Related Commands

show ip ospf database	Displays OSPF database information.

show ip ospf database opaque-as

View the opaque-as (type 11) LSA information.

Syntax **show ip ospf database opaque-as** [*link-state-id*] [**adv-router** *ip-address*]

Parameters

link-state-id	(OPTIONAL) Specify LSA ID in dotted decimal format. The LSA ID value depends on the LSA type, and it can be one of the following: • the network's IP address for Type 3 LSAs or Type 5 LSAs • the router's OSPF router ID for Type 1 LSAs or Type 4 LSAs • the default destination (0.0.0.0) for Type 5 LSAs
adv-router *ip-address*	(OPTIONAL) Enter the keywords **adv-router** ip-address to display only the LSA information about that router.

Command Modes

EXEC

EXEC privilege

Related Commands

show ip ospf database	Displays OSPF database information.

show ip ospf database opaque-link

View the opaque-link (type 9) LSA information.

Syntax **show ip ospf database opaque-link** [*link-state-id*] [**adv-router** *ip-address*]

Parameters

link-state-id	(OPTIONAL) Specify LSA ID in dotted decimal format. The LSA ID value depends on the LSA type, and it can be one of the following: • the network's IP address for Type 3 LSAs or Type 5 LSAs • the router's OSPF router ID for Type 1 LSAs or Type 4 LSAs • the default destination (0.0.0.0) for Type 5 LSAs
adv-router *ip-address*	(OPTIONAL) Enter the keywords **adv-router** ip-address to display only the LSA information about that router.

Command Modes EXEC

EXEC privilege

Related Commands

show ip ospf database	Displays OSPF database information.

show ip ospf database router

View the router (type 1) LSA information.

Syntax **show ip ospf database router** [*link-state-id*] [**adv-router** *ip-address*]

Parameters

link-state-id	(OPTIONAL) Specify LSA ID in dotted decimal format. The LSA ID value depends on the LSA type, and it can be one of the following: • the network's IP address for Type 3 LSAs or Type 5 LSAs • the router's OSPF router ID for Type 1 LSAs or Type 4 LSAs • the default destination (0.0.0.0) for Type 5 LSAs
adv-router *ip-address*	(OPTIONAL) Enter the keywords **adv-router** ip-address to display only the LSA information about that router.

Command Modes EXEC

EXEC privilege

Example

```
Force10#show ip ospf database router

            OSPF Router with ID (1.1.1.10) (Process ID 100)

                Router (Area 0.0.0.0)

  LS age: 967
  Options: (No TOS-capability, No DC, E)
  LS type: Router
  Link State ID: 1.1.1.10
  Advertising Router: 1.1.1.10
  LS Seq Number: 0x8000012f
  Checksum: 0x3357
  Length: 144
  AS Boundary Router
  Area Border Router
   Number of Links: 10

    Link connected to: a Transit Network
     (Link ID) Designated Router address: 192.68.129.1
     (Link Data) Router Interface address: 192.68.129.1
     Number of TOS metric: 0
      TOS 0 Metric: 1

    Link connected to: a Transit Network
     (Link ID) Designated Router address: 192.68.130.1
     (Link Data) Router Interface address: 192.68.130.1
     Number of TOS metric: 0
      TOS 0 Metric: 1

    Link connected to: a Transit Network
     (Link ID) Designated Router address: 192.68.142.2
     (Link Data) Router Interface address: 192.68.142.2
     Number of TOS metric: 0
      TOS 0 Metric: 1

    Link connected to: a Transit Network
     (Link ID) Designated Router address: 192.68.141.2
     (Link Data) Router Interface address: 192.68.141.2
     Number of TOS metric: 0
      TOS 0 Metric: 1

    Link connected to: a Transit Network
     (Link ID) Designated Router address: 192.68.140.2
     (Link Data) Router Interface address: 192.68.140.2
     Number of TOS metric: 0
      TOS 0 Metric: 1

    Link connected to: a Stub Network
     (Link ID) Network/subnet number: 11.1.5.0
--More--
```

Figure 309 show ip ospf database router Command Example (Partial)

Table 76 describes the information displayed in Figure 309.

Table 76 show ip ospf database router Command Example Fields

Item	Description
LS Age	Displays the LSA age.
Options	Displays the optional capabilities available on router. The following options can be found in this item: • TOS-capability or No TOS-capability is displayed depending on whether the router can support Type of Service. • DC or No DC is displayed depending on whether the originating router can support OSPF over demand circuits. • E or No E is displayed on whether the originating router can accept AS External LSAs.
LS Type	Displays the LSA's type.

Table 76 show ip ospf database router Command Example Fields (continued)

Item	Description
Link State ID	Displays the Link State ID.
Advertising Router	Identifies the router ID of the LSA's originating router.
LS Seq Number	Displays the link state sequence number. This number detects duplicate or old LSAs.
Checksum	Displays the Fletcher checksum of an LSA's complete contents.
Length	Displays the length in bytes of the LSA.
Number of Links	Displays the number of active links to the type of router (Area Border Router or AS Boundary Router) listed in the previous line.
Link connected to:	Identifies the type of network to which the router is connected.
(Link ID)	Identifies the link type and address.
(Link Data)	Identifies the router interface address.
Number of TOS Metric	Lists the number of TOS metrics.
TOS 0 Metric	Lists the number of TOS 0 metrics.

Related Commands

show ip ospf database	Displays OSPF database information.

show ip ospf database summary

View the network summary (type 3) LSA routing information.

Syntax **show ip ospf database summary** [*link-state-id*] [**adv-router** *ip-address*]

Parameters

link-state-id	(OPTIONAL) Specify LSA ID in dotted decimal format. The LSA ID value depends on the LSA type, and it can be one of the following: • the network's IP address for Type 3 LSAs or Type 5 LSAs • the router's OSPF router ID for Type 1 LSAs or Type 4 LSAs • the default destination (0.0.0.0) for Type 5 LSAs
adv-router *ip-address*	(OPTIONAL) Enter the keywords **adv-router** ip-address to display only the LSA information about that router.

Command Modes EXEC

EXEC privilege

Example

```
Force10#show ip ospf database summary

            OSPF Router with ID (1.1.1.10) (Process ID 100)

                Summary Network (Area 0.0.0.0)

  LS age: 1551
  Options: (No TOS-capability, DC, E)
  LS type: Summary Network
  Link State ID: 192.68.16.0
  Advertising Router: 192.168.17.1
  LS Seq Number: 0x80000054
  Checksum: 0xb5a2
  Length: 28
  Network Mask: /24
       TOS: 0 Metric: 1

  LS age: 9
  Options: (No TOS-capability, No DC, E)
  LS type: Summary Network
  Link State ID: 192.68.32.0
  Advertising Router: 1.1.1.10
  LS Seq Number: 0x80000016
  Checksum: 0x987c
  Length: 28
  Network Mask: /24
       TOS: 0 Metric: 1

  LS age: 7
  Options: (No TOS-capability, No DC, E)
  LS type: Summary Network
  Link State ID: 192.68.33.0
  Advertising Router: 1.1.1.10
  LS Seq Number: 0x80000016
  Checksum: 0x1241
  Length: 28
  Network Mask: /26
       TOS: 0 Metric: 1

Force10#
```

Figure 310 show ip ospf database summary Command Example

Table 77 describes the information displayed in Figure 310.

Table 77 show ip ospf database summary Command Example Fields

Items	Description
LS Age	Displays the LSA age.
Options	Displays the optional capabilities available on router. The following options can be found in this item: • TOS-capability or No TOS-capability is displayed depending on whether the router can support Type of Service. • DC or No DC is displayed depending on whether the originating router can support OSPF over demand circuits. • E or No E is displayed on whether the originating router can accept AS External LSAs.
LS Type	Displays the LSA's type.
Link State ID	Displays the Link State ID.
Advertising Router	Identifies the router ID of the LSA's originating router.
LS Seq Number	Identifies the link state sequence number. This number allows you to identify old or duplicate LSAs.
Checksum	Displays the Fletcher checksum of an LSA's complete contents.

Table 77 show ip ospf database summary Command Example Fields (continued)

Items	Description
Length	Displays the length in bytes of the LSA.
Network Mask	Displays the network mask implemented on the area.
TOS	Displays the TOS options. Option 0 is the only option.
Metric	Displays the LSA metrics.

Related Commands

show ip ospf database	Displays OSPF database information.

show ip ospf interface

View the OSPF interfaces configured. If OSPF is not enabled on the E-Series, no output is generated.

Syntax **show ip ospf interface** [*interface*]

Parameters

interface	(OPTIONAL) Enter the following keywords and slot/port or number information: • For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For the null interface, enter the keyword **null** followed by zero (0). • For loopback interfaces, enter the keyword **loopback** followed by a number from 0 to 16383. • For Port Channel groups, enter the keyword **port-channel** followed by a number: C-Series Range: 1-128 E-Series Range: 1-32 for EtherScale, 1-255 for TeraScale • For a SONET interface, enter the keyword **sonet** followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information. • For a VLAN, enter the keyword **vlan** followed by the VLAN ID. The range is from 1 to 4094.

Command Modes EXEC

EXEC privilege

Example

```
Force10>show ip ospf int

GigabitEthernet 13/17 is up, line protocol is up
  Internet Address 192.168.1.2/30, Area 0.0.0.1
  Process ID 1, Router ID 192.168.253.2, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 192.168.253.2, Interface address 192.168.1.2
  Backup Designated Router (ID) 192.168.253.1, Interface address 192.168.1.1
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:02
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 192.168.253.1 (Backup Designated Router)

GigabitEthernet 13/23 is up, line protocol is up
  Internet Address 192.168.0.1/24, Area 0.0.0.1
  Process ID 1, Router ID 192.168.253.2, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DROTHER, Priority 1
  Designated Router (ID) 192.168.253.5, Interface address 192.168.0.4
  Backup Designated Router (ID) 192.168.253.3, Interface address 192.168.0.2
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:08
  Neighbor Count is 3, Adjacent neighbor count is 2
    Adjacent with neighbor 192.168.253.5 (Designated Router)
    Adjacent with neighbor 192.168.253.3 (Backup Designated Router)

Loopback 0 is up, line protocol is up
  Internet Address 192.168.253.2/32, Area 0.0.0.1
  Process ID 1, Router ID 192.168.253.2, Network Type LOOPBACK, Cost: 1
Loopback interface is treated as a stub Host.
Force10>
```

Figure 311 show ip ospf interface Command Example

Table 78 describes the information displayed in Figure 311.

Table 78 show ip ospf interface Command Example Fields

Line beginning with	Description
GigabitEthernet...	This line identifies the interface type slot/port and the status of the OSPF protocol on that interface.
Internet Address...	This line displays the IP address, network mask and area assigned to this interface.
Process ID...	This line displays the OSPF Process ID, Router ID, Network type and cost metric for this interface.
Transmit Delay...	This line displays the interface's settings for Transmit Delay, State, and Priority. In the State setting, BDR is Backup Designated Router.
Designated Router...	This line displays the ID of the Designated Router and its interface address.
Backup Designated...	This line displays the ID of the Backup Designated Router and its interface address.
Timer intervals...	This line displays the interface's timer settings for Hello interval, Dead interval, Transmit Delay (Wait), and Retransmit Interval.
Hello due...	This line displays the amount time till the next Hello packet is sent out this interface.
Neighbor Count...	This line displays the number of neighbors and adjacent neighbors. Listed below this line are the details about each adjacent neighbor.

show ip ospf neighbor

View the OSPF neighbors configured.

Syntax **show ip ospf neighbor**

Command Modes EXEC

EXEC privilege

Example

```
Force10#show ip ospf neighbor

Neighbor ID     Pri     State           Dead Time Address         Interface Area
20.20.20.7      1       FULL/DR         00:00:32  182.10.10.3     Gi 0/0    0.0.0.2
192.10.10.2     1       FULL/DR         00:00:37  192.10.10.2     Gi 0/1    0.0.0.1
20.20.20.1      1       FULL/DROTHER00:00:36  192.10.10.4     Gi 0/1    0.0.0.1
Force10#
```

Figure 312 show ip ospf neighbor Command Example

Table 79 describes the information displayed in Figure 312.

Table 79 show ip ospf neighbor Command Example Fields

Row Heading	Description
Neighbor ID	Displays the neighbor router ID.
Pri	Displays the priority assigned neighbor.
State	Displays the OSPF state of the neighbor.
Dead Time	Displays the expected time until the E-Series software declares the neighbor dead.
Address	Displays the IP address of the neighbor.
Interface	Displays the interface type slot/port information.
Area	Displays the neighbor's area (process ID).

show ip ospf route

Display routes as calculated by OSPF and stored in OSPF RIB.

Syntax **show ip ospf route**

Defaults No default values or behavior

Command Modes

EXEC

EXEC privilege

Command History

Version 7.5.1.0	Introduced

Usage Information

This command is useful in isolating routing problems between OSPF and RTM. For example, if a route is missing from the RTM/FIB but is visible from the display output of this command, then likely the problem is with downloading the route to the RTM.

This command has the following limitations:

- The display output is sorted by prefixes; intra-area ECMP routes are not displayed together.
- For Type 2 external routes, type1 cost is not displayed.

Example

```
Force10#show ip ospf route

Prefix            Cost   Nexthop         Interface    Area       Type
1.1.1.1           1       0.0.0.0           Lo 0        0       Intra-Area
3.3.3.3           2      13.0.0.3         Gi 0/47       1       Intra-Area
13.0.0.0          1       0.0.0.0         Gi 0/47       0       Intra-Area
150.150.150.0     2      13.0.0.3         Gi 0/47       -       External
172.30.1.0        2      13.0.0.3         Gi 0/47       1       Intra-Area
Force10#
```

Figure 313 show ip ospf route Command Example

show ip ospf statistics

Display OSPF statistics.

Syntax **show ip ospf statistics global** | [**interface** *name* {**neighbor** *router-id*}]

Parameters

global	Enter the keyword **global** to display the packet counts received on all running OSPF interfaces and packet counts received and transmitted by all OSPF neighbors.
interface *name*	(OPTIONAL) Enter the keyword **interface** followed by one of the following interface keywords and slot/port or number information: • For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For Port Channel groups, enter the keyword **port-channel** followed by a number: C-Series Range: 1-128 E-Series Range: 1-32 for EtherScale, 1-255 for TeraScale • For a SONET interface, enter the keyword **sonet** followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information. • For a VLAN, enter the keyword **vlan** followed by a number from 1 to 4094.
neighbor *router-id*	(OPTIONAL) Enter the keyword **neighbor** followed by the neighbor's router-id in dotted decimal format (A.B.C.D.).

Defaults

No default behavior or values

Command Modes

EXEC

EXEC privilege

Command History

Version 7.4.1.0	Introduced

Example

```
Force10#show ip ospf statistics global

 OSPF Packet Count
     Total    Error    Hello    DDiscr   LSReq    LSUpd   LSAck
RX   10         0       8        2         0         0      0
TX   10         0      10        0         0         0      0

 OSPF Global Queue Length
              TxQ-Len     RxQ-Len     Tx-Mark     Rx-Mark
Hello-Q            0           0           0           2
LSR-Q              0           0           0           0
Other-Q            0           0           0           0

 Error packets (Only for RX)

Intf-Down           0   Non-Dr              0   Self-Org            0
Wrong-Len           0   Invld-Nbr           0   Nbr-State           0
Auth-Err            0   MD5-Err             0   Chksum              0
Version             0   AreaMis             0   Conf-Issues         0
No-Buffer           0   Seq-No              0   Socket              0
Q-OverFlow          0   Unkown-Pkt          0

 Error packets (Only for TX)

Socket Errors         0
Force10#
```

Figure 314 show ip ospf statistics global Command Example

Table 80 defines the display output shown in Figure 314..

Table 80 show ip ospf statistics global Command Example Fields

Row Heading	Description
Total	Displays the total number of packets received/transmitted by the OSPF process
Error	Displays the error count while receiving and transmitting packets by the OSPF process
Hello	Number of OSPF Hello packets
DDiscr	Number of database description packets
LSReq	Number of link state request packets
LSUpd	Number of link state update packets
LSAck	Number of link state acknowledgement packets
TxQ-Len	The transmission queue length
RxQ-Len	The reception queue length
Tx-Mark	The highest number mark in the transmission queue
Rx-Mark	The highest number mark in the reception queue
Hello-Q	The queue, for transmission or reception, for the hello packets
LSR-Q	The queue, for transmission or reception, for the link state request packets.
Other-Q	The queue, for transmission or reception, for the link state acknowledgement, database description, and update packets.

Table 81 list the error type definition that appear in Figure 314.

Table 81 show ip ospf statistics global Error Definitions

Error Type	Description
Intf_Down	Received packets on an interface that is either down or OSPF is not enabled.
Non-Dr	Received packets with a destination address of ALL_DRS even though SELF is not a designated router
Self-Org	Receive the self originated packet
Wrong_Len	The received packet length is different to what was indicated in the OSPF header
Invld-Nbr	LSA, LSR, LSU, and DDB are received from a peer which is not a neighbor peer
Nbr-State	LSA, LSR, and LSU are received from a neighbor with stats less than the loading state
Auth-Error	Simple authentication error
MD5-Error	MD5 error
Cksum-Err	Checksum Error
Version	Version mismatch
AreaMismatch	Area mismatch
Conf-Issue	The received hello packet has a different hello or dead interval than the configuration
No-Buffer	Buffer allocation failure
Seq-no	A sequence no errors occurred during the database exchange process

Table 81 show ip ospf statistics global Error Definitions

Error Type	Description
Socket	Socket Read/Write operation error
Q-overflow	Packet(s) dropped due to queue overflow
Unknown-Pkt	Received packet is not an OSPF packet

The **show ip ospf statistics** (Figure 315) displays the error packet count received on each interface as:

- The hello-timer remaining value for each interface
- The wait-timer remaining value for each interface
- The grace-timer remaining value for each interface
- The packet count received and transmitted for each neighbor
- Dead timer remaining value for each neighbor
- Transmit timer remaining value for each neighbor
- The LSU Q length and its highest mark for each neighbor
- The LSR Q length and its highest mark for each neighbor

Example

```
Force10#show ip ospf statistics

Interface GigabitEthernet 0/8

    Hello-Timer 9, Wait-Timer 0, Grace-Timer 0
    Error packets (Only for RX)

Intf-Down       0   Non-Dr               0   Self-Org          0
Wrong-Len       0   Invld-Nbr            0   Nbr-State         0
Auth-Error      0   MD5-Error            0   Cksum-Err         0
Version         0   AreaMisMatch         0   Conf-Issue        0
SeqNo-Err       0   Unkown-Pkt           0

    Neighbor ID 9.1.1.2

              Hello       DDiscr     LSReq    LSUpd     LSAck
    RX          59          3         1         1         1
    TX          62          2         1         0         0

     Dead-Timer         37, Transmit-Timer          0
     LSU-Q-Len           0, LSU-Q-Wmark             0
     LSR-Q-Len           0, LSR-Q-Wmark             1
```

Figure 315 show ip ospf statistics Command Example

Related Commands

clear ip ospf statistics	Clear the packet statistics in all interfaces and neighbors

show ip ospf topology

Display routers in directly connected areas.

Syntax **show ip ospf topology**

Defaults No default values or behavior

Command Modes EXEC

EXEC privilege

Command History

Version 7.5.1.0	Introduced

Usage Information This command can be used to isolate problems with inter-area and external routes. In OSPF inter-area and external routes are calculated by adding LSA cost to the cost of reaching the router. If an inter-area or external route is not of correct cost, the display can determine if the path to the originating router is correct or not.

Example

```
Force10#show ip ospf topology

Router ID        Flags    Cost   Nexthop         Interface    Area
3.3.3.3         E/B/-/   1      20.0.0.3       Gi 13/1      0
1.1.1.1          E/-/-/   1      10.0.0.1        Gi 7/1       1
Force10#
```

Figure 316 show ip ospf topology Command Example

show ip ospf virtual-links

View the OSPF virtual links configured and is useful for debugging OSPF routing operations. If no OSPF virtual-links are enabled on the E-Series, no output is generated.

Syntax **show ip ospf virtual-links**

Command Modes EXEC

EXEC privilege

Example

```
Force10#show ip ospf virt

Virtual Link to router 192.168.253.5 is up
    Run as demand circuit
    Transit area 0.0.0.1, via interface GigabitEthernet 13/16, Cost of using 2
    Transmit Delay is 1 sec, State POINT_TO_POINT,
        Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
        Hello due in 00:00:02
Force10#
```

Figure 317 show ip ospf virtual-links Command Example

Table 82 describes the information displayed in Figure 317.

Table 82 show ip ospf virtual-links Command Example Fields

Items	Description
"Virtual Link..."	This line specifies the OSPF neighbor to which the virtual link was created and the link's status.
"Run as..."	This line states the nature of the virtual link.
"Transit area..."	This line identifies the area through which the virtual link was created, the interface used, and the cost assigned to that link.
"Transmit Delay..."	This line displays the transmit delay assigned to the link and the State of the OSPF neighbor.
"Timer intervals..."	This line displays the timer values assigned to the virtual link. The timers are Hello is hello-interval, Dead is dead-interval, Wait is transmit-delay, and Retransmit is retransmit-interval.
"Hello due..."	This line displays the amount of time until the next Hello packet is expected from the neighbor router.
"Adjacency State..."	This line displays the adjacency state between neighbors.

summary-address

Set the OSPF ASBR to advertise one external route.

Syntax **summary-address** *ip-address mask* [**not-advertise**] [**tag** *tag-value*]

To disable summary address, use the **no summary-address** *ip-address mask* command.

Parameters

ip-address	Specify the IP address in dotted decimal format of the address to be summarized.
mask	Specify the mask in dotted decimal format of the address to be summarized.

not-advertise	(OPTIONAL) Enter the keyword **not-advertise** to suppress that match the network prefix/mask pair.
tag *tag-value*	(OPTIONAL) Enter the keyword **tag** followed by a value to match on routes redistributed through a route map. Range: 0 to 4294967295

Defaults Not configured.

Command Modes ROUTER OSPF

Usage Information The command area range summarizes routes for the different areas.

With "not-advertise" parameter configured, this command can be used to filter out some external routes. For example, you want to redistribute static routes to OSPF, but you don't want OSPF to advertise routes with prefix 1.1.0.0. Then you can configure `summary-address 1.1.0.0 255.255.0.0 not-advertise` to filter out all the routes fall in range 1.1.0.0/16.

Related Commands

area range	Summarizes routes within an area.

timers spf

Set the time interval between when the E-Series receives a topology change and starts an shortest path first (spf) calculation.

Syntax **timers spf** *delay holdtime*

To return to the default, enter **no timers spf**.

Parameters

delay	Enter a number as the delay. Range: 0 to 4294967295. Default: 5 seconds
holdtime	Enter a number as the hold time. Range: 0 to 4294967295. Default: 10 seconds.

Defaults *delay* = 5 seconds; *holdtime* = 10 seconds

Command Modes ROUTER OSPF

Usage Information Setting the *delay* and *holdtime* parameters to a low number enables the E-Series to switch to an alternate path quickly but requires more CPU usage.

Chapter 38 IPv6 OSPFv3

Platform Specific Feature: IPv6 OSPFv3 is supported on E-Series only.

Open Shortest Path First version 3 (OSPFv3) supports version 6 of the Internet Protocol (IPv6). The fundamental mechanisms of OSPF (flooding, DR election, area support, SPF calculations, etc.) remain unchanged. However, OSPFv3 runs on a per-link basis instead of on a per-IP-subnet basis. Most changes were necessary to handle the increased address size of IPv6.

The Force10 Networks implementation of OSPFv3 is based on IETF RFC 2740. The following commands allow you to configure and enable OSPFv3.

- clear ipv6 ospf process on page 914
- debug ipv6 ospf packet on page 914
- default-information originate on page 915
- ipv6 ospf area on page 916
- ipv6 ospf cost on page 917
- ipv6 ospf dead-interval on page 918
- ipv6 ospf hello-interval on page 918
- ipv6 ospf priority on page 919
- ipv6 router ospf on page 920
- passive-interface on page 920
- redistribute on page 921
- router-id on page 922
- show ipv6 ospf database on page 923
- show ipv6 ospf interface on page 924
- show ipv6 ospf neighbor on page 925

clear ipv6 ospf process

C-Series	No
E-Series	✓

Reset an OSPFv3 router process without removing or re-configuring the process.

Syntax **clear ipv6 ospf process | process** *process-id*

Parameters

process	Enter the keyword **process** to reset the OSPFv3 process.
process *process-id*	(OPTIONAL) Enter the keyword **process** followed by the process identification number.

Command Modes EXEC

EXEC privilege

Command History

Version 7.4.1.0	Introduced

debug ipv6 ospf packet

C-Series	No
E-Series	✓

Display debug information on OSPF IPv6 packets.

Syntax **debug ipv6 ospf packet** [*interface*]

To cancel the debug, use the **no debug ipv6 ospf packet** [*interface*] command.

Parameters

interface	(OPTIONAL) Enter one of the following keywords and slot/port or number information: • For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For a Port Channel, enter the keyword **port-channel** followed by a number from 1 to 32 for EtherScale, 1 to 255 for TeraScale. • For a SONET interface, enter the keyword **sonet** followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information. • For a VLAN, enter the keyword **vlan** followed by a number from 1 to 4094

Command Modes EXEC privilege

Command History

Version 7.4.1.0	Introduced

Example

```
Force10#debug ipv6 ospf packet

OSPFv3 packet related debugging is on for all interfaces

05:21:01 : OSPFv3: Sending, Ver:3, Type:1(Hello), Len:40, Router
ID:223.255.255.254, Area ID:0, Inst:0, on Po 255

05:21:03 : OSPFv3: Received, Ver:3, Type:1(Hello), Len:40, Router
ID:223.255.255.255, Area ID:0, Chksum:a177, Inst:0, from Vl 100

05:20:25 : OSPFv3: Sending, Ver:3, Type:4(LS Update), Len:580, Router
ID:223.255.255.254, Area ID:0, Inst:0, on Vl 1000

Force10#
```

Figure 318 debug ipv6 ospf packet Command Example

Table 83 describes the information in Figure 318.

Table 83 debug ip ospf Output Fields

Field	Description
OSPFv3 ...	Debugging is on for all OSPFv3 packets and all interfaces
05:21:01	Displays the time stamp.
Sending Ver:3	Sending OSPF3 version.
Type:	Displays the type of packet sent: • 1 - Hello packet • 2 - database description • 3 - link state request • 4 - link state update • 5 - link state acknowledgement
Length:	Displays the packet length.
Router ID:	Displays the OSPF3 router ID.
Area ID:	Displays the Area ID.
Chksum:	Displays the OSPF3 checksum.

default-information originate

C-Series	**No**
E-Series	✓

Configure FTOS to generate a default external route into the OSPFv3 routing domain.

Syntax **default-information originate** [**always** [**metric** *metric-value*] [**metric-type** *type-value*]] [**route-map** *map-name*]

To return to the default, use the **no default-information originate** command.

Parameters

always	(OPTIONAL) Enter the keyword **always** to indicate that default route information must always be advertised.
metric *metric-value*	(OPTIONAL) Enter the keyword **metric** followed by the number to configure a metric value for the route. Range: 1 to 16777214
metric-type *type-value*	(OPTIONAL) Enter the keyword **metric-type** followed by the OSPFv3 link state type of 1 or 2 for default routes. The values are: 1 = Type 1 external route 2 = Type 2 external route Default: 2
route-map *map-name*	(OPTIONAL) Enter the keyword **route-map** followed by the name of an established route map.

Defaults Disabled

Command Modes ROUTER OSPFv3

Command History

Version 7.4.1.0	Introduced

Related Commands

redistribute	Redistribute routes from other routing protocols into OSPFv3.

ipv6 ospf area

C-Series	**No**
E-Series	✓

Enable IPv6 OSPF on an interface.

Syntax **ipv6 ospf** *process-id* **area** *area-id*

To disable OSPFv6 routing for an interface, use the **no ipv6 ospf** *process-id* **area** *area-id* command.

Parameters

process-id	Enter the process identification number.
area *area-id*	Specify the OSPF area. Range: 0 to 65535

Defaults No default values or behavior

Command Modes INTERFACE

Command History

Version 7.4.1.0	Introduced

ipv6 ospf cost

C-Series	**No**
E-Series	✓

Explicitly specify the cost of sending a packet on an inter.

Syntax **ipv6 ospf cost** *interface-cost*

To reset the interface cost to the default value, use the **no ipv6 ospf cost** *interface-cost* command.

Parameters

interface-cost	Enter a unsigned integer value expressed as the link-state metric. Range: 1 to 65535

Defaults Default cost based on the bandwidth

Command Modes INTERFACE

Command History

Version 7.4.1.0	Introduced

Usage Information In general, the path cost is calculated as:

10^8 / bandwidth

Using this formula, the default path cost are calculated as:

- GigabitEthernet—Default cost is 1
- TenGigabitEthernet—Default cost is 1
- Ethernet—Default cost is 10

ipv6 ospf dead-interval

C-Series	No
E-Series	✓

Set the time interval since the last hello-packet was received from a router. After the time interval elapses, the neighboring routers declare the router down.

Syntax **ipv6 ospf dead-interval** *seconds*

To return to the default time interval, use the **no ipv6 ospf dead-interval** command.

Parameters

seconds	Enter the time interval in seconds. Range: 1 to 65535 seconds Default: 40 seconds (Ethernet)

Defaults As above

Command Modes INTERFACE

Command History

Version 7.4.1.0	Introduced

Usage Information By default, the dead interval is four times longer than the default hello-interval.

Related Commands

ipv6 ospf hello-interval	Specify the time interval between hello packets

ipv6 ospf hello-interval

C-Series	No
E-Series	✓

Specify the time interval between the hello packets sent on the interface.

Syntax **ipv6 ospf hello-interval** *seconds*

To return to the default value, enter **no ipv6 ospf hello-interval**.

Parameters

seconds	Enter a the time interval in seconds as the time between hello packets. Range: 1 to 65535. Default: 10 seconds (Ethernet) 30 seconds (nonbroadcast).

Defaults As above

Command Modes INTERFACE

Command History

Version 7.4.1.0	Introduced

Usage Information The time interval between hello packets must be the same for routers in a network.

Related Commands

ipv6 ospf dead-interval	Set the time interval since the last hello-packet was received from a router.

ipv6 ospf priority

C-Series	**No**
E-Series	✓

Set the priority of the interface to determine the Designated Router for the OSPFv3 network.

Syntax **ipv6 ospf priority** *number*

To return to the default value, use the **no pv6 ospf priority** command.

Parameters

number	Enter a number as the priority. Range: 0 to 255. Default: 1

Defaults 1

Command Modes INTERFACE

Command History

Version 7.4.1.0	Introduced

Usage Information Setting a priority of 0 makes the router ineligible for election as a Designated Router or Backup Designated Router.

Use this command for interfaces connected to multi-access networks, not point-to-point networks.

ipv6 router ospf

C-Series	No
E-Series	✓

Enable OSPF for IPv6 router configuration.

Syntax **ipv6 router ospf** *process-id*

To exit OSPF for IPv6, enter **no ipv6 router ospf** *process-id*

Parameters

process-id	Enter the process identification number. Range: 1 to 65535

Defaults No default behavior or values

Command Modes CONFIGURATION

Command History

Version 7.4.1.0	Introduced

passive-interface

C-Series	No
E-Series	✓

Disable (suppress) sending routing updates on an interface.

Syntax **passive-interface** *interface*

To enable sending routing updates on an interface, use the **no passive-interface** *interface* command.

Parameters

interface	Enter the following keywords and slot/port or number information: • For a Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For a Port Channel, enter the keyword **port-channel** followed by a number from 1 to 255 for TeraScale. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information. • For a VLAN, enter the keyword **vlan** followed by a number from 1 to 4094.

Defaults

Enabled, that is sending of routing updates are enabled by default

Command Modes

ROUTER OSPFv3

Command History

Version 7.4.1.0	Introduced

Usage Information

By default, no interfaces are *passive*. Routing updates are sent to all interfaces on which the routing protocol is enabled.

If you disable the sending of routing updates on an interface, the particular address prefix will continue to be advertised to other interfaces, and updates from other routers on that interface continue to be received and processed.

OSPFv3 for IPv6 routing information is neither sent nor received through the specified router interface. The specified interface address appears as a stub network in the OSPFv3 for IPv6 domain.

redistribute

C-Series	**No**
E-Series	✓

Redistribute into OSPFv3.

Syntax

redistribute {**bgp** *as number*} {**connected** | **static**} [**metric** *metric-value* | **metric-type** *type-value*] [**route-map** *map-name*] [**tag** *tag-value*]

To disable redistribution, use the **no redistribute** {**connected** | **static**} command.

Parameters

bgp *as number*	Enter the keyword **bgp** followed by the autonomous system number. Range: 1 to 65535
connected	Enter the keyword **connected** to redistribute routes from physically connected interfaces.

static	Enter the keyword **static** redistribute manually configured routes.
metric *metric-value*	Enter the keyword **metric** followed by the metric value. Range: 0 to 16777214 Default: 20
metric-type *type-value*	(OPTIONAL) Enter the keyword **metric-type** followed by the OSPFv3 link state type of 1 or 2 for default routes. The values are: 1 = Type 1 external route 2 = Type 2 external route Default: 2
route-map *map-name*	(OPTIONAL) Enter the keyword **route-map** followed by the name of an established route map. If the route map is not configured, the default is deny (to drop all routes).
tag *tag-value*	(OPTIONAL) Enter the keyword **tag** to set the tag for routes redistributed into OSPFv3. Range: 0 to 4294967295 Default: 0

Default Not configured.

Command Modes ROUTER OSPFv3

Command History

Version 7.4.1.0	Introduced

Usage Information To redistribute the default route (**x:x:x:x::x**), configure the default-information originate command.

Related Commands

default-information originate	Configure default external route into OSPFv3

router-id

C-Series	No
E-Series	✓

Designate a fixed router ID.

Syntax **router-id** *ip-address*

To return to the previous router ID, use the **no router-id** *ip-address* command.

Parameters

ip-address	Enter the router ID in the dotted decimal format.

Defaults The router ID is selected automatically from the set of IPv4 addresses configured on a router

Command Modes ROUTER OSPF

Command History

Version 7.4.1.0	Introduced

Usage Information You can configure an arbitrary value in the IP address for each router. However, each router ID must be unique.

If this command is used on an OSPFv3 process that is already active (has neighbors), all the neighbor adjacencies are brought down immediately and new sessions are initiated with the new router ID.

Related Commands

clear ipv6 ospf process	Reset an OSPFv3 router process

show ipv6 ospf database

C-Series	No
E-Series	✓

Display the information related to an OSPFv3 database for a specified router including link-state advertisements (LSAs).

Syntax **show ipv6 ospf database** [**database-summary**]

Parameters

database-summary	(OPTIONAL) Enter the keywords **database-summary** to view just a summary of database LSA information.

Defaults No default behavior or values

Command Modes EXEC

EXEC privilege

Example

```
Force10#show ipv6 ospf database database-summary

OSPFv3 Router with ID (1.1.1.1) (Process ID 1)

Process 1 database summary
Type                    Count/Status
Oper Status              1
Admin Status             1
Area Bdr Rtr Status      1
AS Bdr Rtr Status        1
AS Scope LSA Count       0
AS Scope LSA Cksum sum   0
Originate New LSAS       50
Rx New LSAS              22
Ext LSA Count            0
Rte Max Eq Cost Paths    10

Area 0 database summary
Type                    Count/Status
Brd Rtr Count            1
AS Bdr Rtr Count         1
LSA count                6
Rtr LSA Count            2
Net LSA Count            1
Inter Area Pfx LSA Count 1
Inter Area Rtr LSA Count 0
Group Mem LSA Count      0
Type-7 LSA count         0
Intra Area Pfx LSA Count 2
Intra Area TE LSA Count  2

Area 1 database summary
Type                    Count/Status
Brd Rtr Count            1
AS Bdr Rtr Count         1
LSA count                8
Rtr LSA Count            1
Net LSA Count            0
Inter Area Pfx LSA Count 5
Inter Area Rtr LSA Count 0
Group Mem LSA Count      0
Type-7 LSA count         0
Intra Area Pfx LSA Count 2
Intra Area TE LSA Count  2
E1200-T2C2#sh ipv6 ospf neighbor

Neighbor ID     Pri   State              Dead Time Interface ID
Interface
63.114.8.36     1     FULL/DR           00:00:37  4          Gi 9/0

Force10#
```

Figure 319 show ipv6 ospf database database-summary Command

show ipv6 ospf interface

C-Series	No
E-Series	✔

View OSPFv3 interface information.

Syntax **show ipv6 ospf** [*interface*]

Parameters

interface	(OPTIONAL) Enter one of the following keywords and slot/port or number information: • For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For a Port Channel, enter the keyword **port-channel** followed by a number from 1 to 32 for EtherScale, 1 to 255 for TeraScale. • For a SONET interface, enter the keyword **sonet** followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information. • For a VLAN, enter the keyword **vlan** followed by a number from 1 to 4094

Defaults No default behavior or values

Command Modes EXEC

Command History

Version 7.4.1.0	Introduced

Example

```
Force10#show ipv6 ospf interface gigabitethernet 1/0

GigabitEthernet 1/0 is up, line protocol is up
  Link Local Address fe80::201:e8ff:fe17:5bbd, Interface ID 67420217
  Area 0, Process ID 1, Instance ID 0, Router ID 11.1.1.1
  NetworkType BROADCAST, Cost: 1, Passive: No
  Transmit Delay is 100 sec, State DR, Priority 1
  Designated router on this network is 11.1.1.1 (local)
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 1, Retransmit 5

Force10#
```

show ipv6 ospf neighbor

C-Series	**No**
E-Series	✓

Display the OSPF neighbor information on a per-interface basis.

Syntax **show ipv6 ospf neighbor** [*interface*]

Parameters

interface	(OPTIONAL) Enter the following keywords and slot/port or number information: • For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For a Port Channel interface, enter the keyword **port-channel** followed by a number from 1 to 255 for TeraScale. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information. • For a VLAN, enter the keyword **vlan** followed by the VLAN ID. The range is from 1 to 4094.

Defaults No default behavior or values

Command Modes EXEC

EXEC privilege

Command History

Version 7.4.1.0	Introduced

Example

```
Force10#show ipv6 ospf neighbor gi 9/0

Neighbor ID     Pri   State              Dead Time Interface ID Interface
63.114.8.36     1     FULL/DR             00:00:38  4            Gi 9/0

Force10#
```

Figure 320 show ipv6 ospf neighbor Command Example

Chapter 39 Bidirectional Forwarding Detection

C-Series	NO
E-Series	✓

Platform Specific Feature: Bidirectional Forwarding Detection (BFD) is supported on E-Series only.

Bidirectional Forwarding Detection (BFD) is a detection protocol that provides fast forwarding path failure detection. The FTOS implementation is based on the standards specified in the IETF Draft draft-ietf-bfd-base-03 and interoperates with other industry implementations of BFD.

Note: BFD is supported on physical Layer 3 interfaces only.

- bfd enable (Configuration) on page 928
- bfd enable (Interface) on page 928
- bfd interval on page 929
- bfd all-neighbors (IS-IS) on page 930
- bfd all-neighbors (OSPF) on page 931
- bfd neighbor on page 931
- bfd protocol-liveness on page 932
- clear bfd counters on page 933
- debug bfd on page 933
- ip route bfd on page 934
- isis bfd all-neighbors on page 935
- show bfd counters on page 936
- show bfd neighbors on page 937

bfd enable (Configuration)

C-Series	No
E-Series	✓

Enable the BFD protocol.

Syntax **bfd enable**

To disable the BFD protocol, use the **no bfd enable** command.

Defaults Disabled

Command Modes CONFIGURATION

Command History

Version 7.4.1.0	Introduced

bfd enable (Interface)

C-Series	No
E-Series	✓

Enable the BFD on an interface.

Syntax **bfd enable**

To disable the BFD on an interface, use the **no bfd enable** command.

Defaults Enabled

Command Modes INTERFACE

Command History

Version 7.4.1.0	Introduced

bfd interval

C-Series	No
E-Series	✓

Configure the BFD sessions timers on the interface.

Syntax

bfd interval *milliseconds* **min_rx** *milliseconds* **multiplier** *value* **role** [**active** | **passive**]

To revert to the default, use the **no bfd interval** *milliseconds* **min_rx** *milliseconds* **multiplier** *value* **role** [**active** | **passive**] command.

Parameters

milliseconds	Enter the transmit interval, in milliseconds, between BFD packets. Range: 50 to1000 milliseconds Default: 100 milliseconds
min_rx *milliseconds*	Enter the keyword **min_rx** followed by the minimum receive interval in milliseconds. Range: 50 to1000 milliseconds Default: 100 milliseconds
multiplier *value*	Enter the keyword **multiplier** followed by the detect multiplier value used for to compute holdown. Range: 3 to 50 Default: 3
role [**active** | **passive**]	Enter the keyword **role** followed by either **active** or **passive** keyword to define the role taken by a BFD session. Default: **active**

Defaults

Defaults as listed above

Command Modes

INTERFACE

Command History

Version 7.4.1.0	Introduced

Example

```
Force10(conf-if-gi-0/3)#bfd interval 250 min_rx 300 multiplier 4 role passive
Force10(conf-if-gi-0/3)#
```

bfd all-neighbors (IS-IS)

C-Series	No
E-Series	✓

Enable BFD for all neighbors discovered by the IS-IS protocol over all interfaces.

Syntax

bfd all-neighbors [**interval** *min_tx milliseconds min_rx milliseconds* **multiplier** *value* **role** {**active** | **passive**}]

To disable BFD on all IS-IS discovered neighbors, use the **no bfd all-neighbors** [**interval** *min_tx milliseconds min_rx milliseconds* **multiplier** *value* **role** {**active** | **passive**}] command.

Parameters

interval *min_tx milliseconds*	(OPTIONAL) Enter the keyword **interval** followed by the minimum transmit (tx) interval, in milliseconds, between BFD packets. Range: 50 to1000 milliseconds Default: 100 milliseconds
min_rx milliseconds	(OPTIONAL) Enter the minimum receive (rx) interval in milliseconds. Range: 50 to1000 milliseconds Default: 100 milliseconds.
multiplier *value*	(OPTIONAL) Enter the keyword **multiplier** followed by the detect multiplier value used to compute holdown. Range: 3 to 50 Default: 3
role {**active**	**passive**}	(OPTIONAL) Enter the keyword **role** followed by either the active or passive keyword to define the role taken by a BFD session. Default: active

Defaults

Defaults as above

Command Modes

ROUTER ISIS (conf-router-isis)

Command History

Version 7.5.1.0	Introduced

Usage Information

The timer values specified in this command will be overridden by timer values specified in the INTERFACE mode. Note that using the *no* form of this command will not disable BFD on an interface if BFD is explicitly enabled on that interface using the isis bfd all-neighbors.

Related Commands

isis bfd all-neighbors	Enable BFD on all IS-IS neighbors discovered on this interface

bfd all-neighbors (OSPF)

C-Series	No
E-Series	✓

Enable BFD for all OSPF neighbors.

Syntax **bfd all-neighbors** [**interval** *milliseconds* **min_rx** *milliseconds* **multiplier** *value* **role** [**active** | **passive**]]

To disable BFD on all OSPF neighbors, use the **no bfd all-neighbors** [**interval** *milliseconds* **min_rx** *milliseconds* **multiplier** *value* **role** [**active** | **passive**]] command.

Parameters

interval *milliseconds*	Enter the keyword **interval** followed by the transmit interval, in milliseconds, between BFD packets. Range: 50 to1000 milliseconds Default: 100 milliseconds
min_rx *milliseconds*	Enter the keyword **min_rx** followed by the minimum receive interval in milliseconds. Range: 50 to1000 milliseconds Default: 100 milliseconds
multiplier *value*	Enter the keyword **multiplier** followed by the detect multiplier value used for to compute holdown. Range: 3 to 50 Default: 3
role [**active**	**passive**]	Enter the keyword **role** followed by either **active** or **passive** keyword to define the role taken by a BFD session. Default: **active**

Defaults Defaults as listed above

Command Modes ROUTER OSPF

Command History

Version 7.4.1.0	Introduced

bfd neighbor

C-Series	No
E-Series	✓

Configure the neighbor for the BFD session.

Syntax **bfd neighbor** {*ip-address*}

To remove the BFD neighbor, use the **no bfd neighbor** {*ip-address*} command.

Parameters

ip-address	Enter an IP address in dotted decimal format

Defaults No default values or behavior

Command Modes INTERFACE

Command History

Version 7.4.1.0	Introduced

Related Commands

show bfd neighbors	Display the bfd neighbors

bfd protocol-liveness

C-Series	**No**
E-Series	✓

Enable the BFD protocol liveness feature.

Syntax **bfd protocol-liveness**

To disable the protocol liveness, use the **no bfd protocol-liveness** command.

Defaults Disabled

Command Modes CONFIGURATION

Command History

Version 7.4.1.0	Introduced

Usage Information Protocol liveness enables detection of software process failures within the BFD protocol framework. On being notified by the operating system about a protocol task crash, BFD will bring down the sessions that the protocol has registered for. Thus the peer routers immediately bring down their BFD sessions. If the peer routers so choose, they might take corrective action by choosing alternative paths for the routes that originally pointed to this router.

clear bfd counters

C-Series	No
E-Series	✓

Clear the BFD counters.

Syntax **clear bfd counters** [*interface*]

Parameters

interface	(OPTIONAL) Enter one of the following keywords and slot/port or number information: • For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For **SONET** interfaces, enter the keyword sonet followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information.

Defaults No default values or behavior

Note: Without an interface specified, the command clears all interface BFD counters.

Command Modes EXEC privilege

Command History

Version 7.4.1.0	Introduced

Related Commands

show bfd counters	Display the BFD counters

debug bfd

C-Series	No
E-Series	✓

Enable BFD debugging.

Syntax **debug bfd** {**detail** | **event** | **packet**} [**all** | *interface*] [*mode*] [**count** *number*]

To disable BFD debugging, use the **no debug bfd** {**detail** | **event** | **packet**} [**all** | *interface*] [*mode*] [**count** *number*] command.

Parameters

detail	(OPTIONAL) Enter the keyword **detail** to display detailed information about the BFD packet.
event	(OPTIONAL) Enter the keyword **event** to display information about BFD transitions according to the BFD state machine.
packet	(OPTIONAL) Enter the keyword **packet** to display brief information about control packets.
all	Enter the keyword **all** to enable debug on all interfaces.
interface	(OPTIONAL) Enter one of the following keywords and slot/port or number information: • For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For **SONET** interfaces, enter the keyword sonet followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information.
mode	(OPTIONAL) Enter one of the following supported debug transmission modes: • To display information for both received and sent packets, enter the keyword **both** • To display information for received packets, enter the keyword **rx** • To display information for sent packets, enter the keyword **tx** Default: **both**
count *number*	(OPTIONAL) Enter the keyword **count** followed by the number of debug messages to display. Range: 1-65534 Default: Infinite—that is, if a count number is not specified an infinite number of debug messages will display

Defaults

Disabled

Command Modes

EXEC privilege

Command History

Version 7.4.1.0	Introduced

Usage Information

Since BFD can potentially transmit 20 packets per interface, debug information should be restricted. The **count** option is not supported for packets and detail debug when enabled on all interfaces.

ip route bfd

C-Series	No
E-Series	✓

Enable BFD for all neighbors configured through static routes.

Syntax **ip route bfd** [**interval** *milliseconds* **min_rx** *milliseconds* **multiplier** *value* **role** [**active** | **passive**]]

To disable BFD for all neighbors configured through static routes, use the **no ip route bfd** [**interval** *milliseconds* **min_rx** *milliseconds* **multiplier** *value* **role** [**active | passive**]] command.

Parameters

interval *milliseconds*	Enter the keyword **interval** followed by the transmit interval, in milliseconds, between BFD packets. Range: 50 to1000 milliseconds Default: 100 milliseconds
min_rx *milliseconds*	Enter the keyword **min_rx** followed by the minimum receive interval in milliseconds. Range: 50 to1000 milliseconds Default: 100 milliseconds
multiplier *value*	Enter the keyword **multiplier** followed by the detect multiplier value used for to compute holdown. Range: 3 to 50 Default: 3
role [**active	passive**]	Enter the keyword **role** followed by either **active** or **passive** keyword to define the role taken by a BFD session. Default: **active**

Defaults Defaults as listed above

Command Modes CONFIGURATION

Command History

Version 7.4.1.0	Introduced

Related Commands

show bfd neighbors	Display BFD neighbors

isis bfd all-neighbors

C-Series	**No**
E-Series	✓

Enable BFD on all IS-IS neighbors discovered on this interface

Syntax **isis bfd all-neighbors** [**disable** | [**interval** *min_tx milliseconds min_rx milliseconds* **multiplier** *value* **role** {**active** | **passive**}]]

To disable all IS-IS neighbors discovered on this interface, use the **no isis bfd all-neighbors** [**disable** | [**interval** *min_tx milliseconds min_rx milliseconds* **multiplier** *value* **role** {**active** | **passive**}]] command.

Parameters

disable	(OPTIONAL) Enter the keyword **disable** to disable BFD on this interface.
interval *min_tx milliseconds*	(OPTIONAL) Enter the keyword **interval** followed by the minimum transmit (tx) interval, in milliseconds, between BFD packets. Range: 50 to1000 milliseconds Default: 100 milliseconds
min_rx milliseconds	(OPTIONAL) Enter the minimum receive (rx) interval in milliseconds. Range: 50 to1000 milliseconds Default: 100 milliseconds.
multiplier *value*	(OPTIONAL) Enter the keyword **multiplier** followed by the detect multiplier value used to compute holdown. Range: 3 to 50 Default: 3
role {**active**	**passive**}	(OPTIONAL) Enter the keyword **role** followed by either the active or passive keyword to define the role taken by a BFD session. Default: active

Defaults Defaults as above

Command Modes INTERFACE

Command History

Version 7.5.1.0	Introduced

Usage Information The timer values specified in this command will override timer values specified in the router configuration mode. Use the keyword **disable** to disable BFD on a specific interface while BFD is configured in the router configuration mode. The **disable** keyword overrides any prior times configured and vice-a-versa. This command provides the flexibility to fine tune the timer values based on individual interface needs.

show bfd counters

C-Series	No
E-Series	✓

Display BFD counter information for interfaces with BFD configuration.

Syntax **show bfd counters** {[*interface*] | {[**isis** | **ospf** | **static-route**] [*interface*]}}

Parameters

interface	(OPTIONAL) Enter one of the following keywords and slot/port or number information: • For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For **SONET** interfaces, enter the keyword sonet followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information.
isis	(OPTIONAL) Enter the keyword **isis** to display counter information on interfaces that have BFD sessions established by the IS-IS protocol.
ospf	(OPTIONAL) Enter the keyword **ospf** to display counter information on interfaces that have BFD sessions established by the OSPF protocol.
static-route	(OPTIONAL) Enter the keyword static-**route** to see counter information on interfaces that have BFD sessions established through configured static routes.

Defaults No default values or behavior

Command Modes EXEC privilege

Command History

Version 7.5.1.0	Added support for IS-IS
Version 7.4.1.0	Introduced

Example

```
Force10#show bfd counters

Interface                Tx          Rx
GigabitEthernet 1/3      522         625
Force10#
```

show bfd neighbors

C-Series	**No**
E-Series	✓

View BFD neighbor information on all interfaces or the specified interface.

Syntax **show bfd neighbors** *interface* [**detail**]

Parameters

interface	Enter one of the following keywords and slot/port or number information: • For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For **SONET** interfaces, enter the keyword sonet followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information.
detail	(OPTIONAL) Enter the keyword **detail** to view detailed information on BFD neighbors.

Defaults No default values or behavior

Command Modes EXEC privilege

Command History

Version 7.4.1.0	Introduced

Example

```
Force10#show bfd neighbors

*       - Active session role
Ad Dn   - Admin Down
C       - CLI
I       - ISIS
O       - OSPF
R       - Static Route (RTM)

  LocalAddr       RemoteAddr      Interface State Rx-int Tx-int Mult Clients
* 10.1.3.2        10.1.3.1        Gi 1/3    Up    300    250    3    C
Force10#
```

Figure 321 show bfd neighbors Command

Example

```
Force10#show bfd neighbors detail

Session Discriminator: 1
Neighbor Discriminator: 1
Local Addr: 10.1.3.2
Local MAC Addr: 00:01:e8:02:15:0e
Remote Addr: 10.1.3.1
Remote MAC Addr: 00:01:e8:27:2b:f1
Int: GigabitEthernet 1/3
State: Up
Configured parameters:
 TX:  100ms, RX:  100ms, Multiplier: 3
Neighbor parameters:
 TX:  250ms, RX:  300ms, Multiplier: 4
Actual parameters:
 TX:  300ms, RX:  250ms, Multiplier: 3
Role: Active
Delete session on Down: False
Client Registered: CLI
Uptime: 00:02:04
Statistics:
 Number of packets received from neighbor: 376
 Number of packets sent to neighbor: 314
 Number of state changes: 2
 Number of messages from IFA about port state change: 0
 Number of messages communicated b/w Manager and Agent: 6
Force10#
```

Figure 322 show bfd neighbors detail Command

Related Commands

bfd neighbor	Configure the neighbor for the BFD session.
bfd all-neighbors (OSPF)	Enable BFD for all OSPF neighbors

Chapter 40 IS-IS Protocol

Platform Specific Feature: IS-IS Protocol is supported on E-Series only.

IS-IS (Intermediate System to Intermediate System), developed by the International Organization for Standardization (OSI), is an interior gateway protocol that uses a shortest-path-first algorithm. IS-IS facilitates the communication between open systems, supporting routers passing both IP and OSI traffic.

A router is considered an *intermediate system.* Networks are partitioned into manageable routing domains, called areas. Intermediate systems send, receive, and forward packets to other routers within their area (Level 1 and Level 1-2 devices). Only Level 1-2 and Level 2 devices communicate with other areas.

FTOS supports ISO/IEC 10589 and the following RFCs:

- RFC 1142, *OSI IS-IS Intra-Domain Routing Protocol* (This is an ASCII version of ISO/IEC 10589)
- RFC 1195, *Use of OSI IS-IS for Routing in TCP/IP and Dual Environments*
- RFC 2763, *Dynamic Hostname Exchange Mechanism for IS-IS*
- RFC 2966, *Domain-wide Prefix Distribution with Two-Level IS-IS*
- RFC 3373, Three-Way Handshake for Intermediate System to Intermediate System (IS-IS) Point-to-Point Adjacencies

The following commands allow you to enable IS-IS on the E-Series.

- advertise on page 943
- area-password on page 944
- clear config on page 944
- clear isis on page 945
- clns host on page 945
- debug isis on page 946
- debug isis adj-packets on page 946
- debug isis local-updates on page 947
- debug isis snp-packets on page 948

- debug isis spf-triggers on page 948
- debug isis update-packets on page 949
- default-information originate on page 949
- distance on page 950
- distribute-list in on page 951
- distribute-list out on page 952
- distribute-list redistributed-override on page 953
- domain-password on page 953
- hello padding on page 954
- hostname dynamic on page 955
- ignore-lsp-errors on page 955
- ip router isis on page 956
- isis circuit-type on page 956
- isis csnp-interval on page 957
- isis hello-interval on page 958
- isis hello-multiplier on page 959
- isis hello padding on page 959
- isis metric on page 960
- isis network point-to-point on page 961
- isis password on page 961
- isis priority on page 962
- is-type on page 963
- log-adjacency-changes on page 963
- lsp-gen-interval on page 964
- lsp-mtu on page 965
- lsp-refresh-interval on page 965
- max-area-addresses on page 966
- max-lsp-lifetime on page 967
- maximum-paths on page 967
- metric-style on page 968
- net on page 969
- passive-interface on page 969
- redistribute on page 970
- redistribute bgp on page 972
- redistribute ospf on page 973
- router isis on page 974
- set-overload-bit on page 975
- show config on page 976
- show isis database on page 976
- show isis hostname on page 978

- show isis interface on page 978
- show isis neighbors on page 979
- show isis protocol on page 980
- show isis traffic on page 981
- spf-interval on page 983

advertise

C-Series	No
E-Series	✓

Leak routes between levels (distribute IP prefixes between level 1 and level 2 and vice versa).

Syntax **advertise** {**level1-into-level2** | **level2-into-level1**} *prefix-list-name*

To return to the default, use the **no advertise** {**level1-into-level2** | **level2-into-level1**}[*prefix-list-name*] command.

Parameters

level1-into-level2	Enter the keyword **level1-into-level2** to advertise Level 1 routes into Level 2 LSPs. This is the default.
level2-into-level1	Enter the keyword **level2-into-level1** to advertise Level 2 inter-area routes into Level 1 LSPs. Described in RFC 2966.
prefix-list-name	Enter the name of a configured IP prefix list. Routes meeting the criteria of the IP Prefix list are leaked.

Defaults **level1-into-level2** (that is, Level 1 to Level 2 leaking enabled.)

Command Modes ROUTER ISIS (conf-router_isis)

Usage Information You cannot disable leaking from one level to another, *however* you can regulate the rate flow from one level to another via an IP Prefix list. If the IP Prefix list is not configured, all routes are leaked.

Additional information can be found in IETF RFC 2966, *Domain-wide Prefix Distribution with Two-Level IS-IS.*

area-password

C-Series	No
E-Series	✓

Configure authentication password for an area.

Syntax **area-password** [**hmac-md5** | *encryption-type*] *password*

To delete a password, enter **no area-password**.

Parameters

hmac-md5	(OPTIONAL) Enter the keyword **hmac-md5** to encrypt the password.
encryption-type	(OPTIONAL) Enter 7 to encrypt the password using DES.
password	Enter a 1—16-character length alphanumeric string to prevent unauthorized access or incorrect routing information corrupting the link state database. The password is processed as plain text which only provides limited security.

Defaults Not configured.

Command Modes ROUTER ISIS (conf-router_isis)

Usage Information Use the area-password command on routers within an area to prevent the link state database from receiving incorrect routing information from unauthorized routers.

The password configured is injected into Level 1 LSPs, CSNPs, and PSNPs.

Related Commands

domain-password	Allows you to set the authentication password for a routing domain.
isis password	Allows you to configure an authentication password for an interface.

clear config

C-Series	No
E-Series	✓

Clear IS-IS configurations that display under the `router isis` heading of the show running-config command output.

Syntax **clear config**

Command Modes ROUTER ISIS

Usage Information Use caution when you enter this command. Back up your configuration prior to using this command or your IS-IS configuration will be erased.

Related Commands		
	copy	Use this command to save the current configuration to another location.

clear isis

C-Series	No
E-Series	✓

Restart the IS-IS process. All IS-IS data is cleared.

Syntax **clear isis** [*tag*] {* | **database** | **traffic**}

Parameters

tag	(Optional) Enter an alphanumeric string to specify the IS-IS routing tag area.
*	Enter the keyword * to clear all IS-IS information and restarts the IS-IS process. This command removes IS-IS neighbor information and IS-IS LSP database information and the full SPF calculation will be done.
database	Clears IS-IS LSP database information.
traffic	Clears IS-IS counters.

Command Modes EXEC privilege

clns host

C-Series	No
E-Series	✓

Define a name-to-network service mapping point (NSAP) mapping that can then be used with commands that require NSAPs and system IDs.

Syntax **clns host** *name nsap*

Parameters

name	Enter an alphanumeric string to identify the name-to-NSAP mapping.
nsap	Enter a specific NSAP address that will be associated with the *name* parameter.

Defaults Not configured.

Command Modes ROUTER ISIS (conf-router_isis)

Usage Information

Use this command to configure a shortcut name that can used instead of entering a long string of numbers associated with an NSAP address.

Related Commands

hostname dynamic	Enables dynamic learning of hostnames from routers in the domain and allows the routers to advertise the hostnames in LSPs.

debug isis

C-Series	No
E-Series	✓

Enable debugging for all IS-IS operations.

Syntax

debug isis

To disable debugging of IS-IS, enter **no debug isis**.

Command Modes

EXEC privilege

Usage Information

Entering **debug isis** enables all debugging parameters.

Use this command to view all debugging information in one output. To turn off debugging, you normally enter separate **no** forms of each command. Enter the **no debug isis** command to disable all debug messages for IS-IS at once.

debug isis adj-packets

C-Series	No
E-Series	✓

Enable debugging on adjacency-related activity such as hello packets that are sent and received on IS-IS adjacencies.

Syntax

debug isis adj-packets [*interface*]

To turn off debugging, use the **no debug isis adj-packets** [*interface*] command.

Parameters

interface	(OPTIONAL) Identifies the interface type slot/port as one of the following: • For a Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For a Port Channel, enter the keyword **port-channel** followed by a number from 1 to 32 for EtherScale, 1 to 255 for TeraScale. • For a SONET interface, enter the keyword **sonet** followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information. • For a VLAN, enter the keyword **vlan** followed by a number from 1 to 4094.

Command Modes EXEC privilege

debug isis local-updates

C-Series	**No**
E-Series	✓

Enables debugging on a specific interface and provides diagnostic information to debug IS-IS local update packets.

Syntax **debug isis local-updates** [*interface*]

To turn off debugging, enter the **no debug isis local-updates** [*interface*] command.

Parameters

interface	(OPTIONAL) Identifies the interface type slot/port as one of the following: • For a Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For a Port Channel, enter the keyword **port-channel** followed by a number from 1 to 32 for EtherScale, 1 to 255 for TeraScale. • For a SONET interface, enter the keyword **sonet** followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information. • For a VLAN, enter the keyword **vlan** followed by a number from 1 to 4094.

Command Modes EXEC privilege

debug isis snp-packets

C-Series	No
E-Series	✓

Enable debugging on a specific interface and provides diagnostic information to debug IS-IS complete sequence number PDU (CSNP) and partial sequence number PDU (PSNP) packets.

Syntax **debug isis snp-packets** [*interface*]

To turn off debugging, enter the **no debug isis snp-packets** [*interface*] command.

Parameters

interface	(OPTIONAL) Identifies the interface type slot/port as one of the following: • For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For a Port Channel interface, enter **port-channel** followed by a number from 1 to 32 for EtherScale, 1 to 255 for TeraScale. • For a SONET interface, enter the keyword **sonet** followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information. • For a VLAN, enter the keyword **vlan** followed by a number from 1 to 4094.

Command Modes EXEC privilege

debug isis spf-triggers

C-Series	No
E-Series	✓

Enable debugging on the events that triggered IS-IS shortest path first (SPF) events for debugging purposes.

Syntax **debug isis spf-triggers**

To turn off debugging, enter **no debug isis spf-triggers**.

Command Modes EXEC privilege

debug isis update-packets

C-Series	No
E-Series	✓

Enable debugging on Link State PDUs (LSPs) that are detected by a router.

Syntax **debug isis update-packets** [*interface*]

To turn off debugging, enter the **no debug isis update-packets** [*interface*] command.

Parameters

interface	(OPTIONAL) Identifies the interface type slot/port as one of the following: • For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For a Port Channel interface, enter **port-channel** followed by a number from 1 to 32 for EtherScale, 1 to 255 for TeraScale. • For a SONET interface, enter the keyword **sonet** followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information. • For a VLAN, enter the keyword **vlan** followed by a number from 1 to 4094.

Command Modes EXEC privilege

default-information originate

C-Series	No
E-Series	✓

Generate a default route into an IS-IS routing domain and controls the distribution of default information.

Syntax **default-information originate** [**always**] [**metric** *metric*] [**route-map** *map-name*]

To disable the generation of a default route into the specified IS-IS routing domain, enter the **no default-information originate** [**always**] [**metric** *metric*] [**route-map** *map-name*] command.

Parameters

always	(OPTIONAL) Enter the keyword **always** to have the default route always advertised

metric *metric*	(OPTIONAL) Enter the keyword **metric** followed by a number to assign to the route. Range: 0 to 16777215
route-map *map-name*	(OPTIONAL) A default route will be generated by the routing process if the route map is satisfied.

Defaults

Not configured.

Command Modes

ROUTER ISIS (conf-router_isis)

Usage Information

When you use this command to redistribute routes into a routing domain, the router becomes an autonomous system (AS) boundary router. An AS boundary router does not always generate a default route into a routing domain. The router still requires its own default route before it can generate one.

How a metric value assigned to a default route is advertised depends on how on the configuration of the metric-style command. If the metric-style is set for narrow mode and the metric value in the default-information originate command is set to a number higher than 63, the metric value advertised in LSPs will be 63. If the metric-style is set for wide mode, their the metric value in the default-information originate command is advertised.

Related Commands

redistribute	Redistribute routes from one routing domain to another routing domain.
isis metric	Configure a metric for an interface
metric-style	Set the metric style for the router.
show isis database	Display the IS-IS link state database.

distance

C-Series	**No**
E-Series	✓

Define the administrative distance for learned routes.

Syntax

distance *weight* [*ip-address mask* [*prefix-list*]]

To return to the default values, enter the **no distance** *weight* command.

Parameters

weight	The administrative distance value indicates the reliability of a routing information source. Range: 1 to 255. (A higher relative value indicates lower reliability. Routes with smaller values are given preference.) Default: 115
ip-address mask	(OPTIONAL) Enter an IP address in dotted decimal format and enter a mask in either dotted decimal or /prefix format.
prefix-list	(OPTIONAL) Enter the name of a prefix list name.

Defaults *weight* = 115

Command Modes ROUTER ISIS (conf-router_isis)

Usage Information The administrative distance indicates the trust value of incoming packets. A low administrative distance indicates a high trust rate. A high value indicates a lower trust rate. For example, a weight of 255 is interpreted that the routing information source is not trustworthy and should be ignored.

distribute-list in

C-Series	**No**
E-Series	✓

Filter network prefixes received in updates.

Syntax **distribute-list** *prefix-list-name* **in** [*interface*]

To return to the default values, enter the **no distribute-list** *prefix-list-name* **in** [*interface*] command.

Parameters

prefix-list-name	Specify the prefix list to filter prefixes in routing updates.
interface	(OPTIONAL) Identifies the interface type slot/port as one of the following: • For a1- Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For a Port Channel interface, enter **port-channel** followed by a number from 1 to 32 for EtherScale, 1 to 255 for TeraScale. • For a SONET interface, enter the keyword **sonet** followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information. • For a VLAN, enter the keyword **vlan** followed by a number from 1 to 4094.

Defaults Not configured.

Command Modes ROUTER ISIS (conf-router_isis)

Related Commands

distribute-list out	Suppress networks from being advertised in updates.
redistribute	Redistributes routes from one routing domain to another routing domain.

distribute-list out

C-Series	No
E-Series	✓

Suppress network prefixes from being advertised in outbound updates.

Syntax

distribute-list *prefix-list-name* **out** [**connected** | **ospf** *process-id* | **rip** | **static**]

To return to the default values, enter the no **distribute-list** *prefix-list-name* **out** [**connected** | **ospf** *process-id* | **rip** | **static**] command.

Parameters

prefix-list-name	Specify the prefix list to filter prefixes in routing updates.
connected	(OPTIONAL) Enter the keyword **connected** for directly connected routing process.
ospf *process-id*	(OPTIONAL) Enter the keyword **ospf** followed by the OSPF process-ID number. Range: 1 to 65535
rip	(OPTIONAL) Enter the keyword **rip** for RIP routes.
static	(OPTIONAL) Enter the keyword **static** for user-configured routing process.

Defaults

Not configured.

Command Modes

ROUTER ISIS (conf-router_isis)

Usage Information

You can assign a name to a routing process so a prefix list will be applied to only the routes derived from the specified routing process.

Related Commands

distribute-list in	Filters networks received in updates.
redistribute	Redistributes routes from one routing domain to another routing domain.

distribute-list redistributed-override

C-Series	No
E-Series	✓

Supress flapping of routes when the same route is redistributed into IS-IS from multiple routers in the network.

Syntax **distribute-list redistributed-override in**

To return to the default, use the **no distribute-list redistributed-override in** command.

Defaults No default behavior or values

Command Modes ROUTER ISIS (conf-router_isis)

Command History

Version 6.3.1.0	Introduced

Usage Information When the command is executed, IS-IS will not download the route to the routing table if the same route was redistributed into IS-IS routing protocol on the same router.

domain-password

C-Series	No
E-Series	✓

Set the authentication password for a routing domain.

Syntax **domain-password** [**hmac-md5** | *encryption-type*] *password*

To disable the password, enter **no domain-password**.

Parameters

hmac-md5	(OPTIONAL) Enter the keyword **hmac-md5** to encrypt the password using MD5.
encryption-type	(OPTIONAL) Enter 7 to encrypt the password using DES.
password	Enter an alphanumeric string up to 16 characters long. If you do not specify an encryption type or hmac-md5 keywords, the password is processed as plain text which provides limited security.

Defaults No default password.

Command Modes ROUTER ISIS (conf-router_isis)

Usage Information

The domain password is inserted in Level 2 link state PDUs (LSPs), complete sequence number PDUs (CSNPs), and partial sequence number PDUs (PSNPs).

Related Commands

area-password	Configure an IS-IS area authentication password.
isis password	Configure the authentication password for an interface.

hello padding

C-Series	**No**
E-Series	✓

Use to turn ON or OFF padding for LAN and point-to-point hello PDUs or to selectively turn padding ON or OFF for LAN or point-to-point hello PDUs.

Syntax

hello padding [**multi-point** | **point-to-point**]

To return to default, use **no hello padding** [**multi-point** | **point-to-point**].

Parameters

multi-point	(OPTIONAL) Enter the keyword **multi-point** to pad only LAN hello PDUs.
point-to-point	(OPTIONAL) Enter the keyword **point-to-point** to pad only point-to-point PDUs.

Defaults

Both LAN and point-to-point hello PDUs are padded.

Command Modes

ROUTER ISIS (conf-router_isis)

Usage Information

IS-IS hellos are padded to the full maximum transmission unit (MTU) size. Padding IS-IS Hellos (IIHS) to the full MTU provides early error detection of large frame transmission problems or mismatched MTUs on adjacent interfaces.

Related Commands

isis hello padding	Turn ON or OFF hello padding on an interface basis.

hostname dynamic

C-Series	No
E-Series	✓

Enables dynamic learning of hostnames from routers in the domain and allows the routers to advertise the hostname in LSPs.

Syntax **hostname dynamic**

To disable this command, enter **no hostname dynamic**.

Defaults Enabled.

Command Modes ROUTER ISIS (conf-router_isis)

Usage Information Use this command to build name-to-systemID mapping tables through the protocol. All **show** commands that display systems also display the hostname.

Related Commands

clns host	Define a name-to-NSAP mapping.

ignore-lsp-errors

C-Series	No
E-Series	✓

Ignore LSPs with bad checksums instead of purging those LSPs.

Syntax **ignore-lsp-errors**

To return to the default values, enter **no ignore-lsp-errors**.

Defaults In IS-IS, the default *deletes* LSPs with internal checksum errors (**no ignore-lsp-errors**).

Command Modes ROUTER ISIS (conf-router_isis)

Usage Information IS-IS normally purges LSPs with an incorrect data link checksum, causing the LSP source to regenerate the message. A cycle of purging and regenerating LSPs can occur when a network link continues to deliver accurate LSPs even though there is a link causing data corruption. This could cause disruption to your system operation.

ip router isis

C-Series	No
E-Series	✓

Configure IS-IS routing processes on an interface and attach an area tag name to the routing process.

Syntax

ip router isis [*tag*]

To disable IS-IS on an interface, enter the **no ip router isis** [*tag*] command.

Parameters

tag	(OPTIONAL) The tag you specify identifies a specific area routing process. If you do not specify a tag, a null tag is assigned.

Defaults

No processes are configured.

Command Modes

INTERFACE

Command History

Version 7.5.1.0	Introduced

Usage Information

You must use the net command to assign a network entity title to enable IS-IS.

Related Commands

net	Configures an IS-IS network entity title (NET) for the routing process.
router isis	Enables the IS-IS routing protocol.

isis circuit-type

C-Series	No
E-Series	✓

Configure the adjacency type on interfaces.

Syntax

isis circuit-type {**level-1** | **level-1-2** | **level-2-only**}

To return to the default values, enter **no isis circuit-type**.

Parameters

level-1	You can form a Level 1 adjacency if there is at least one common area address between this system and neighbors. You cannot form Level 2 adjacencies on this interface.
level-1-2	You can form a Level 1 and Level 2 adjacencies when the neighbor is also configured as Level-1-2 and there is at least one common area, if not, then a Level 2 adjacency is established. This is the default.
level-2-only	You can form a Level 2 adjacencies when other Level 2 or Level 1-2 routers and their interfaces are configured for Level 1-2 or Level 2. Level 1 adjacencies cannot be established on this interface.

Defaults level-1-2

Command Modes INTERFACE

Usage Information Because the default establishes Level 1 and Level 2 adjacencies, you do not need to configure this command. Routers in an IS-IS system should be configured as a Level 1-only, Level 1-2, or Level 2-only system.

Only configure interfaces as Level 1 or Level 2 on routers that are between areas (for example, a Level 1-2 router) to prevent the software from sending unused hello packets and wasting bandwidth.

isis csnp-interval

C-Series	**No**
E-Series	✓

Configure the IS-IS complete sequence number PDU (CSNP) interval on an interface.

Syntax **isis csnp-interval** *seconds* [**level-1** | **level-2**]

To return to the default values, enter the **no isis csnp-interval** [*seconds*] [**level-1** | **level-2**] command.

Parameters

seconds	Interval of transmission time between CSNPs on multi-access networks for the designated intermediate system. Range: 0 to 65535 Default: 10
level-1	(OPTIONAL) Independently configures the interval of time between transmission of CSNPs for Level 1.
level-2	(OPTIONAL) Independently configures the interval of time between transmission of CSNPs for Level 2.

Defaults *seconds* = 10; **level-1** (if not otherwise specified)

Command Modes INTERFACE

Usage Information The default values of this command are typically satisfactory transmission times for a specific interface on a designated intermediate system. To maintain database synchronization, the designated routers send CSNPs.

Level 1 and Level 2 CSNP intervals can be configured independently.

isis hello-interval

C-Series	No
E-Series	✓

Specify the length of time between hello packets sent.

Syntax **isis hello-interval** *seconds* [**level-1** | **level-2**]

To return to the default values, enter the **no isis hello-interval** [*seconds*] [**level-1** | **level-2**] command.

Parameters

seconds	Allows you to set the length of time between hello packet transmissions. Range: 1 to 65535 Default: 10
level-1	(OPTIONAL) Select this value to configure the hello interval for Level 1. This is the default.
level-2	(OPTIONAL) Select this value to configure the hello interval for Level 2.

Defaults *seconds* = 10; **level-1** (if not otherwise specified)

Command Modes INTERFACE

Usage Information Hello packets are held for a length of three times the value of the hello interval. Use a high hello interval seconds to conserve bandwidth and CPU usage. Use a low hello interval seconds for faster convergence (but uses more bandwidth and CPU resources).

Related Commands

isis hello-multiplier	Specifies the number of IS-IS hello packets a neighbor must miss before the router should declare the adjacency as down.

isis hello-multiplier

C-Series	No
E-Series	✓

Specify the number of IS-IS hello packets a neighbor must miss before the router declares the adjacency down.

Syntax **isis hello-multiplier** *multiplier* [**level-1** | **level-2**]

To return to the default values, enter **no isis hello-multiplier** [*multiplier*] [**level-1** | **level-2**].

Parameters

multiplier	Specifies an integer that sets the multiplier for hello holding time. Never configure a hello-multiplier lower then the default (3). Range: 3 to 1000 Default: 3
level-1	(OPTIONAL) Select this value to configure the hello multiplier independently for Level 1 adjacencies. This is the default.
level-2	(OPTONAL) Select this value to configure the hello multiplier independently for Level 2 adjacencies.

Defaults *multiplier* =3; **level-1** (if not otherwise specified)

Command Modes INTERFACE

Usage Information The holdtime (the product of the hello-multiplier multiplied by the hello-interval) determines how long a neighbor waits for a hello packet before declaring the neighbor is down so routes can be recalculated.

Related Commands

isis hello-interval	Specify the length of time between hello packets.

isis hello padding

C-Series	No
E-Series	✓

Turn ON or OFF padding of hello PDUs from the interface mode.

Syntax **isis hello padding**

To return to the default, use the **no isis hello padding**.

Defaults Padding of hello PDUs is enabled (ON).

Command Modes INTERFACE

Usage Information Hello PDUs are "padded" only when both the global and interface padding options are ON. Turning either one OFF will disable padding for the corresponding interface(s).

Related Commands

hello padding	Turn ON or OFF padding for LAN and point-to-point hello PDUs.

isis metric

C-Series	**No**
E-Series	✓

Assign a metric to an interface.

Syntax **isis metric** *default-metric* [**level-1** | **level-2**]

To return to the default values, enter **no isis metric** [*default-metric*] [**level-1** | **level-2**].

Parameters

default-metric	Metric assigned to the link and used to calculate the cost from each other router via the links in the network to other destinations. You can configure this metric for Level 1 or Level 2 routing. Range: 0 to 63 for narrow and transition metric styles; 0 to 16777215 for wide metric styles. Default: 10
level-1	(OPTIONAL) Enter **level-1** to configure the shortest path first (SPF) calculation for Level 1 (intra-area) routing. This is the default.
level-2	(OPTIONAL) Enter **level-2** to configure the SPF calculation for Level 2 (inter-area) routing.

Defaults *default-metric* = 10; **level-1** (if not otherwise specified)

Command Modes INTERFACE

Usage Information Force10 Networks recommends configuring metrics on all interfaces. Without configuring this command, the IS-IS metrics are similar to hop-count metrics.

isis network point-to-point

C-Series	No
E-Series	✓

Enable the software to treat a broadcast interface as a point-to-point interface.

Syntax **isis network point-to-point**

To disable the feature, enter **no isis network point-to-point**.

Defaults Not enabled.

Command Modes INTERFACE

isis password

C-Series	No
E-Series	✓

Configure an authentication password for an interface.

Syntax **isis password** [**hmac-md5**] *password* [**level-1** | **level-2**]

To delete a password, enter the **no isis password** [*password*] [**level-1** | **level-2**] command.

Parameters

encryption-type	(OPTIONAL) Enter 7 to encrypt the password using DES.
hmac-md5	(OPTIONAL) Enter the keyword **hmac-md5** to encrypt the password using MD5.
password	Assign the interface authentication password.
level-1	(OPTIONAL) Independently configures the authentication password for Level 1. The router acts as a station router for Level 1 routing. This is the default.
level-2	(OPTIONAL) Independently configures the authentication password for Level 2. The router acts as an area router for Level 2 routing.

Defaults No default password. **level-1** (if not otherwise specified)

Command Modes INTERFACE

Usage Information To protect your network from unauthorized access, use this command to prevent unauthorized routers from forming adjacencies.

You can assign different passwords for different routing levels by using the **level-1** and **level-2** keywords.

The **no** form of this command disables the password for Level 1 or Level 2 routing, using the respective keywords **level-1** or **level-2**.

This password provides limited security as it is processed as plain text.

isis priority

C-Series	No
E-Series	✔

Set priority of the designated router you select.

Syntax **isis priority** *value* [**level-1** | **level-2**]

To return to the default values, enter the **no isis priority** [*value*] [**level-1** | **level-2**] command.

Parameters

value	This value sets the router priority. The higher the value, the higher the priority. Range: 0 to 127 Default: 64
level-1	(OPTIONAL) Specify the priority for Level 1. This is the default.
level-2	(OPTIONAL) Specify the priority for Level 2.

Defaults *value* = 64; **level-1** (if not otherwise specified)

Command Modes INTERFACE

Usage Information You can configure priorities independently for Level 1 and Level 2. Priorities determine which router on a LAN will be the designated router. Priorities are advertised within hellos. The router with the highest priority will become the designated intermediate system (DIS).

Routers with priority of 0 cannot be a designated router. Setting the priority to 0 lowers the chance of this system becoming the DIS, but does not prevent it. If all the routers have priority 0, one with highest MAC address will become DIS even though its priority is 0.

is-type

C-Series	No
E-Series	✓

Configure IS-IS operating level for a router.

Syntax **is-type** {**level-1** | **level-1-2** | **level-2-only**}

To return to the default values, enter **no is-type**.

Parameters

level-1	Allows a router to act as a Level 1 router.
level-1-2	Allows a router to act as both a Level 1 and Level 2 router. This is the default.
level-2-only	Allows a router to act as a Level 2 router.

Defaults **level-1-2**

Command Modes ROUTER ISIS (conf-router_isis)

Usage Information The IS-IS protocol automatically determines area boundaries and are able to keep Level 1 and Level 2 routing separate. Poorly planned use of this feature may cause configuration errors, such as accidental area partitioning.

If you are configuring only one area in your network, you do not need to run both Level 1 and Level 2 routing algorithms. The IS type can be configured as Level 1.

log-adjacency-changes

C-Series	No
E-Series	✓

Generate a log messages for adjacency state changes.

Syntax **log-adjacency-changes**

To disable this function, enter **no log-adjacency-changes**.

Defaults Adjacency changes are not logged.

Command Modes ROUTER ISIS (conf-router_isis)

Usage Information This command allow you to monitor adjacency state changes, which is useful when you monitor large networks. Messages are logged in the system error message facility.

lsp-gen-interval

C-Series	No
E-Series	✓

Set the minimum interval between successive generations of link-state packets (LSPs).

Syntax **lsp-gen-interval** [**level-1 | level-2**] *interval seconds* [*initial_wait_interval seconds* [*second_wait_interval seconds*]]

To restore default values, use the **no lsp-gen-interval** [**level-1 | level-2**] *interval seconds* [*initial_wait_interval seconds* [*second_wait_interval seconds*]] command.

Parameters

level-1	(OPTIONAL) Enter the keyword **level-1** to apply the configuration to generation of Level-1 LSPs.
level-2	(OPTIONAL) Enter the keyword **level-2** to apply the configuration to generation of Level-2 LSPs.
interval seconds	Enter the maximum number of seconds between LSP generations. Range: 0 to 120 seconds Default: 5 seconds
initial_wait_interval seconds	(OPTIONAL) Enter the initial wait time, in seconds, before running the first LSP generation. Range: 0 to 120 seconds Default: 1 second
second_wait_interval seconds	(OPTIONAL) Enter the wait interval, in seconds, between the first and second LSP generation. Range: 0 to 120 seconds Default: 5 seconds

Defaults Defaults as above

Command Modes ROUTER ISIS (conf-router-isis)

Command History

Version 7.5.1.0	Expanded to support LSP Throttling Enhancement

Usage Information LSP throttling slows down the frequency at which LSPs are generated during network instability. Even though throttling LSP generations slows down network convergence, no throttling can result in a network not functioning as expected. If network topology is unstable, throttling slows down the scheduling of LSP generations until the topology regains its stability.

The first generation is controlled by the initial wait interval and the second generation is controlled by the second wait interval. Each subsequent wait interval is twice as long as the previous one until the wait interval reaches the maximum wait time specified (*interval seconds*). Once the network calms down and there are no triggers for two times the maximum interval, fast behavior is restored (the initial wait time).

lsp-mtu

C-Series	No
E-Series	✓

Set the maximum transmission unit (MTU) of IS-IS link-state packets (LSPs). This command only limits the size of LSPs generated by this router.

Syntax **lsp-mtu** *size*

To return to the default values, enter **no lsp-mtu**.

Parameters

size	The maximum LSP size, in bytes. Range: 128 to 1497 for non-jumbo mode; 128 to 9195 for jumbo mode. Default: 1497

Defaults 1497 bytes

Command Modes ROUTER ISIS (conf-router_isis)

Usage Information The link MTU (mtu command) and the LSP MTU size must be the same

Since each device can generate a maximum of 255 LSPs, consider carefully whether the lsp-mtu command should be configured.

lsp-refresh-interval

C-Series	No
E-Series	✓

Set the link state PDU (LSP) refresh interval. LSPs must be refreshed before they expire. When the LSPs are not refreshed after a refresh interval, they are kept in a database until their max-lsp-lifetime reaches zero and then LSPs will be purged.

Syntax **lsp-refresh-interval** *seconds*

To restore the default refresh interval, enter **no lsp-refresh-interval**.

Parameters

seconds	The LSP refresh interval, in seconds. This value has to be less than the seconds value specified with the max-lsp-lifetime command. Range: 1 to 65535 seconds. Default: 900

Defaults 900 seconds

Command Modes ROUTER ISIS (conf-router_isis)

Usage Information The refresh interval determines the rate at which route topology information is transmitted preventing the information from becoming obsolete.

The refresh interval must be less than the LSP lifetime specified with the max-lsp-lifetime command. A low value reduces the amount of time that undetected link state database corruption can persist at the cost of increased link utilization. A higher value reduces the link utilization caused by the flooding of refreshed packets.

Related Commands

max-lsp-lifetime	Sets the maximum interval that LSPs persist without being refreshed

max-area-addresses

C-Series	**No**
E-Series	✓

Configure manual area addresses.

Syntax **max-area-addresses** *number*

To return to the default values, enter **no max-area-addresses**.

Parameters

number	Set the maximum number of manual area addresses. Range: 3 to 6. Default: 3

Defaults 3 addresses

Command Modes ROUTER ISIS (conf-router_isis)

Usage Information Use this command to configure the number of area addresses on router. This value should be consistent with routers in the same area, or else, the router will form only Level 2 adjacencies. The value should be same among all the routers to form Level 1 adjacencies.

max-lsp-lifetime

C-Series	No
E-Series	✓

Set the maximum time that link-state packets (LSPs) exist without being refreshed.

Syntax **max-lsp-lifetime** *seconds*

To restore the default time, enter **no max-lsp-lifetime**.

Parameters

seconds	The maximum lifetime of LSP in seconds. This value must be greater than the lsp-refresh-interval . The higher the value the longer the LSPs are kept. Range: 1 to 65535 Default: 1200

Defaults 1200 seconds

Command Modes ROUTER ISIS (conf-router_isis)

Usage Information Change the maximum LSP lifetime with this command. The maximum LSP lifetime must always be greater than the LSP refresh interval.

The *seconds* parameter enables the router to keep LSPs for the specified length of time. If the value is higher, the overhead is reduced on slower-speed links.

Related Commands

lsp-refresh-interval	Use this command to set the link-state packet (LSP) refresh interval.

maximum-paths

C-Series	No
E-Series	✓

Allows you to configure the maximum number of parallel paths allowed in a routing table.

Syntax **maximum-paths** *number*

To return to the default values, enter **no maximum-paths**.

Parameters

number	Enter a number as the maximum number of parallel paths an IP routing installs in a routing table. Range: 1 to 16. Default: 4

Defaults 4

Command Mode ROUTER ISIS (conf-router_isis)

metric-style

C-Series	**No**
E-Series	✓

Configure a router to generate and accept old-style, new-style, or both styles of type, length, and values (TLV).

Syntax **metric-style** {**narrow** [**transition**] | **transition** | **wide** [**transition**]} [**level-1 | level-2**]

To return to the default values, enter the **no metric-style** {**narrow** [**transition**] | **transition | wide** [**transition**]} [**level-1 | level-2**] command.

Parameters

narrow	Allows you to configure the E-Series to generate and accept old-style TLVs. Metric range: 0 to 63
transition	Allows you to configure the E-Series to generate both old-style and new-style TLVs. Metric range: 0 to 63
wide	Allows you to configure the E-Series to generate and accept only new-style TLVs. Metric range: 0 to 16777215
level-1	Enables the metric style on Level 1.
level-2	Enables the metric style on Level 2.

Defaults **narrow**; if no Level is specified, Level-1 and Level-2 are configured.

Command Modes ROUTER ISIS (conf-router_isis)

Usage Information Refer to Appendix D for more information on this command.

If you enter the **metric-style wide** command, the E-Series generates and accepts only new-style TLVs. The router uses less memory and other resources rather than generating both old-style and new-style TLVs.

The new-style TLVs have wider metric fields than old-style TLVs.

Related Commands

isis metric	Use this command to configure a metric for an interface.

net

C-Series	No
E-Series	✓

Use this mandatory command to configure an IS-IS network entity title (NET) for a routing process. If a NET is not configured, the IS-IS process will not start.

Syntax **net** *network-entity-title*

To remove a net, enter **no net** *network-entity-title*.

Parameters

network-entity-title	Specify the area address and system ID for an IS-IS routing process. The first 1 to 13 bytes identify the area address. The next 6 bytes identify the system ID. The last 1 byte is the selector byte, always identified as zero zero (00). This argument can be applied to an address or a name.

Defaults Not configured.

Command Modes ROUTER ISIS (conf-router_isis)

passive-interface

C-Series	No
E-Series	✓

Suppress routing updates on an interface. This command stops the router from sending updates on that interface.

Syntax **passive-interface** *interface*

To delete a passive interface configuration, enter the **no passive-interface** *interface* command.

Parameters

interface	Enter the following keywords and slot/port or number information: • For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For Loopback interface, enter the keyword **loopback** followed by a number from zero (0) to 16383. • For a Port Channel interface, enter the keyword **port-channel** followed by a number from 1 to 32 for EtherScale, 1 to 255 for TeraScale. • For a SONET interface, enter the keyword **sonet** followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information. • For a VLAN, enter the keyword **vlan** followed by a number from 1 to 4094.

Defaults Not configured.

Command Modes ROUTER ISIS (conf-router_isis)

Usage Information Although the passive interface will neither send nor receive routing updates, the network on that interface will still be included in IS-IS updates sent via other interfaces

redistribute

C-Series	**No**
E-Series	✓

Redistribute routes from one routing domain to another routing domain.

Syntax **redistribute** {**static** | **connected** | **rip**} [**level-1** | **level-1-2** | **level-2**] [**metric** *metric-value*] [**metric-type** {**external** | **internal**}] [**route-map** *map-name*]

To end redistribution or disable any of the specified keywords, enter the **no redistribute** {**static** | **connected | rip**} [**metric** *metric-value*] [**metric-type** {**external** | **internal**}] [**level-1** | **level-1-2** | **level-2**] [**route-map** *map-name*] command.

Parameters

connected	Enter the keyword **connected** redistribute active routes into IS-IS.
rip	Enter the keyword **rip** to redistribute RIP routes into IS-IS.
static	Enter the keyword **static** to redistribute user-configured routes into IS-IS.
metric *metric-value*	(OPTIONAL) Assign a value to the redistributed route. Range: 0 to 16777215 Default: 0. You should use a value that is consistent with the destination protocol.

metric-type {**external** | **internal**}	(OPTIONAL) The external link type associated with the default route advertised into a routing domain. You must specify one of the following: • **external** • **internal**
level-1	(OPTIONAL) Routes are independently redistributed into IS-IS as Level 1 routes.
level-1-2	(OPTIONAL) Routes are independently redistributed into IS-IS as Level-1-2 routes.
level-2	(OPTIONAL) Routes are independently redistributed into IS-IS as Level 2 routes. This is the default.
route-map *map-name*	(OPTIONAL) If the **route-map** argument is not entered, all routes are redistributed. If a *map-name* value is not specified, then no routers are imported.

Defaults

metric *metric-value* = 0; **metric-type**= internal; **level-2**

Command Modes

ROUTER ISIS (conf-router_isis)

Usage Information

To redistribute a default route (0.0.0.0/0), configure the default-information originate command.

Changing or disabling a keyword in this command will not affect the state of the other command keywords.

When an LSP with an internal metric is received, the FTOS considers the route cost taking into consideration the advertised cost to reach the destination.

Redistributed routing information is filtered with the distribute-list out command to ensure that the routes are properly are passed to the receiving routing protocol.

How a metric value assigned to a redistributed route is advertised depends on how on the configuration of the metric-style command. If the metric-style command is set for narrow or transition mode and the metric value in the redistribute command is set to a number higher than 63, the metric value advertised in LSPs will be 63. If the metric-style command is set for wide mode, an the metric value in the redistribute command is advertised.

Related Commands

default-information originate	Generate a default route for the IS-IS domain.
distribute-list out	Suppress networks from being advertised in updates. Redistributed routing information is filtered by this command.

redistribute bgp

C-Series	No
E-Series	✓

Redistribute routing information from a BGP process. (new command in Release 6.3.1)

Syntax

redistribute bgp *AS number* [**level-1**| **level-1-2** | **level-2**] [**metric** *metric-value*] [**metric-type** {**external**| **internal**}] [**route-map** *map-name*]

To return to the default values, enter the **no redistribute bgp** command with the appropriate parameters.

Parameters

AS number	Enter a number that corresponds to the Autonomous System number. Range: 1 to 65355
level-1	(OPTIONAL) Routes are independently redistributed into IS-IS Level 1 routes only
level-1-2	(OPTIONAL) Routes are independently redistributed into IS-IS Level 1 and Level 2 routes.
level-2	(OPTIONAL) Routes are independently redistributed into IS-IS as Level 2 routes only. This is the default.
metric *metric-value*	(OPTIONAL) The value used for the redistributed route. You should use a metric value that is consistent with the destination protocol. Range: 0 to 16777215 Default: 0.
metric-type {**external**| **internal**}	(OPTIONAL) The external link type associated with the default route advertised into a routing domain. The two options are: • external • internal
route-map *map-name*	*map-name* is an identifier for a configured route map. The route map should filter imported routes from the source routing protocol to the current routing protocol. If you do not specify a *map-name,* all routes are redistributed. If you specify a keyword, but fail to list route map tags, no routes will be imported.

Defaults

IS-IS Level 2 routes only

Command Modes

ROUTER ISIS (conf-router_isis)

Example

```
Force10(conf)#router is
Force10(conf-router_isis)#redistribute bgp 1 level-1 metric 32 metric-type
external route-map rmap-isis-to-bgp
Force10(conf-router_bgp)#show running-config isis
!
router isis
redistribute bgp 1 level-1 metric 32 metric-type external route-map
rmap-isis-to-bgp
```

Figure 323 redistribute bgp Command Example

Usage Information

BGP to IS-IS redistribution supports "match" options using route maps. The metric value, level, and metric-type of redistributed routes can be set by the redistribution command. More advanced "set" options can be performed using route maps.

redistribute ospf

C-Series	**No**
E-Series	✓

Redistribute routing information from an OSPF process.

Syntax

redistribute ospf *process-id* [**level-1**| **level-1-2** | **level-2**] [**match** {**internal** | **external**}] [**metric** *metric-value*] [**metric-type** {**external** | **internal**}] [**route-map** *map-name*]

To return to the default values, enter the **no redistribute ospf** *process-id* [**level-1**| **level-1-2** | **level-2**] [**match** {**internal** | **external**}] [**metric** *metric-value*][**metric-type** {**external** | **internal**}] [**route-map** *map-name*] command.

Parameters

process-id	Enter a number that corresponds to the OSPF process ID to be redistributed. Range: 1 to 65355
metric *metric-value*	(OPTIONAL) The value used for the redistributed route. You should use a metric value that is consistent with the destination protocol. Range: 0 to 16777215 Default: 0.
metric-type {**external** | **internal**}	(OPTIONAL) The external link type associated with the default route advertised into a routing domain. The two options are: • external • internal
level-1	(OPTIONAL) Routes are independently redistributed into IS-IS as Level 1 routes.

level-1-2	(OPTIONAL) Routes are independently redistributed into IS-IS as Level-1-2 routes.
level-2	(OPTIONAL) Routes are independently redistributed into IS-IS as Level 2 routes. This is the default.
match {**external** | **internal**}	(OPTIONAL) The command used for OSPF to route and redistribute into other routing domains. The values are • **internal** • **external**
route-map *map-name*	*map-name* is an identifier for a configured route map. The route map should filter imported routes from the source routing protocol to the current routing protocol. If you do not specify a *map-name,* all routes are redistributed. If you specify a keyword, but fail to list route map tags, no routes will be imported.

Defaults As above

Command Modes ROUTER ISIS (conf-router_isis)

Command History

Version6.3.1.0	Introduced

Usage Information How a metric value assigned to a redistributed route is advertised depends on how on the configuration of the metric-style command. If the metric-style command is set for narrow mode and the metric value in the redistribute ospf command is set to a number higher than 63, the metric value advertised in LSPs will be 63. If the metric-style command is set for wide mode, an the metric value in the redistribute ospf command is advertised.

router isis

C-Series	No
E-Series	✓

Allows you to enable the IS-IS routing protocol and to specify an IP IS-IS process.

Syntax **router isis** [*tag*]

To disable IS-IS routing, enter **no router isis** [*tag*].

Parameters

tag	(OPTIONAL) This is a unique name for a routing process. A null tag is assumed if the tag option is not specified. The tag name must be unique for all IP router processes for a given router.

Defaults Not configured.

Command Modes ROUTER ISIS (conf-router_isis)

Usage Information

You must configure a network entity title (the net command) to specify the area address and the router system ID.

You must enable routing on one or more interfaces to establish adjacencies and establish dynamic routing.

Only one IS-IS routing process can be configured to perform Level 2 routing. A **level-1-2** designation performs Level 1 and Level 2 routing at the same time.

Related Commands

ip router isis	Configure IS-IS routing processes for IP on interfaces and attach an area designator to the routing process.
net	Configure an IS-IS network entity title (NET) for a routing process.
is-type	Assign a type for a given area.

set-overload-bit

C-Series	**No**
E-Series	✓

Configure the router to set the overload bit in its non-pseudonode LSPs. This prevents other routers from using it as an intermediate hop in their shortest path first (SPF) calculations.

Syntax **set-overload-bit**

To return to the default values, enter **no set-overload-bit**.

Defaults Not set.

Command Mode ROUTER ISIS (conf-router_isis)

Usage Information

Set the overload bit when a router experiences problems, such as a memory shortage due to an incomplete link state database which can result in an incomplete or inaccurate routing table. If you set the overload bit in its LSPs, other routers ignore the unreliable router in their SPF calculations until the router has recovered.

show config

C-Series	No
E-Series	✓

View the changes you made to the IS-IS configuration. Default values are not shown.

Syntax **show config**

Command Modes ROUTER ISIS (conf-router_isis)

Example

```
Force10(conf-router_isis)#sho config
!
router isis
 log-adjacency-changes
 lsp-refresh-interval 800
 net 49.0000.0001.0000.0000.000A.00
```

Figure 324 show config Command Example

show isis database

C-Series	No
E-Series	✓

View the IS-IS link state database.

Syntax **show isis database** [**level-1** | **level-2**] [**local**] [**detail** | **summary**] [*lspid*]

Parameters

level-1	(OPTIONAL) Displays the Level 1 IS-IS link-state database.
level-2	(OPTIONAL) Displays the Level 2 IS-IS link-state database.
local	(OPTIONAL) Displays local link-state database information.
detail	(OPTIONAL) Detailed link-state database information of each LSP displays when specified. If not specified, a summary displays.
summary	(OPTIONAL) Summary of link-state database information displays when specified.
lspid	(OPTIONAL) Display only the specified LSP.

Command Modes EXEC

EXEC privilege

Example

```
Force10#sho is da
IS-IS Level-1 Link State Database
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime ATT/P/OL
0000.0000.000A.00-00* 0x0000000B   0xBCB4        1155 0/0/0
0000.0000.000A.01-00* 0x00000003   0x7C41        1109 0/0/0
0000.0000.000B.00-00  0x00000007   0x34CF        1084 0/0/0
0000.0000.000B.01-00  0x00000002   0x94A0        1090 0/0/0

IS-IS Level-2 Link State Database
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime ATT/P/OL
0000.0000.000A.00-00* 0x0000000F   0x6420        1186 0/0/0
0000.0000.000A.01-00* 0x00000003   0x7C41        1113 0/0/0
0000.0000.000B.00-00  0x0000000B   0xE51B        1091 0/0/0
```

Figure 325 show isis database Command Example

Table 84 show isis database Command Example Fields

Field	Description
IS-IS Level-1/Level-2 Link State Database	Displays the IS-IS link state database for Level 1 or Level 2.
LSPID	Displays the LSP identifier. The first six octets are the System ID of the originating router. The next octet is the pseudonode ID. If this byte is not zero, then the LSP describes system links. If this byte is zero (0), then the LSP describes the state of the originating router. The designated router for a LAN creates and floods a pseudonode LSP and describes the attached systems. The last octet is the LSP number. An LSP will be divided into multiple LSP fragments if there is more data than cannot fit in a single LSP. Each fragment has a unique LSP number. An * after the LSPID indicates that an LSP was originated by the system where this command was issued.
LSP Seq Num	This value is the sequence number for the LSP that allows other systems to determine if they have received the latest information from the source.
LSP Checksum	This is the checksum of the entire LSP packet.
LSP Holdtime	This value is the amount of time, in seconds, that the LSP remains valid. A zero holdtime indicates that this is a purged LSP and is being removed from the link state database. A value between brackets indicates the duration that the purged LSP stays in the database before being removed.
ATT	This value represents the Attach bit. This indicates that the router is a Level 2 router and can reach other areas. Level 1-only routers and Level 1-2 routers that have lost connection to other Level 2 routers use the Attach bit to find the closest Level 2 router. They point a default route to the closest Level 2 router.
P	This value represents the P bit. This bit will always set be zero as Force10 Networks does not support area partition repair.
OL	This value represents the overload bit, determining congestion. If the overload bit is set, other routers will not use this system as a transit router when calculating routes.

show isis hostname

C-Series	No
E-Series	✓

View IS-IS host names configured or learned on the E-Series.

Syntax **show isis hostname**

Command Modes EXEC

EXEC privilege

Example

```
Force10#sho isis hostname
System Id       Dynamic Name   Static Name
 BBBB.BBBB.BBBB F10            B233
*AAAA.AAAA.AAAA Force10        B232
Force10#
```

Figure 326 show isis hostname Command Example

show isis interface

C-Series	No
E-Series	✓

View detailed IS-IS interface status and configuration information.

Syntax **show isis interface** [*interface*]

Parameters

interface	(OPTIONAL) Enter the following keywords and slot/port or number information: • For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For Loopback interface, enter the keyword **loopback** followed by a number from zero (0) to 16383. • For a Port Channel, enter the keyword **port-channel** followed by a number from 1 to 32 for EtherScale, 1 to 255 for TeraScale. • For a SONET interface, enter the keyword **sonet** followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information. • For a VLAN, enter the keyword **vlan** followed by a number from 1 to 4094.

Command Modes EXEC

EXEC privilege

Example

```
Force10>show isis int
GigabitEthernet 0/7 is up, line protocol is up
  MTU 1497, Encapsulation SAP
  Routing Protocol: IS-IS
    Circuit Type: Level-1-2
    Interface Index 37847070, Local circuit ID 1
    Level-1 Metric: 10, Priority: 64, Circuit ID: systest-3.01
            Hello Interval: 10, Hello Multiplier: 3, CSNP Interval: 10
    Number of active level-1 adjacencies: 1
    Level-2 Metric: 10, Priority: 64, Circuit ID: systest-3.01
            Hello Interval: 10, Hello Multiplier: 3, CSNP Interval: 10
    Number of active level-2 adjacencies: 1
    Next IS-IS LAN Level-1 Hello in 2 seconds
    Next IS-IS LAN Level-2 Hello in 1 seconds
    LSP Interval: 33
GigabitEthernet 0/8 is up, line protocol is up
  MTU 1497, Encapsulation SAP
  Routing Protocol: IS-IS
    Circuit Type: Level-1-2
    Interface Index 38371358, Local circuit ID 2
    Level-1 Metric: 10, Priority: 64, Circuit ID: systest-3.02
            Hello Interval: 10, Hello Multiplier: 3, CSNP Interval: 10
    Number of active level-1 adjacencies: 1
    Level-2 Metric: 10, Priority: 64, Circuit ID: systest-3.02
            Hello Interval: 10, Hello Multiplier: 3, CSNP Interval: 10
--More--
```

Figure 327 show isis interface Command Example (Partial)

show isis neighbors

C-Series	**No**
E-Series	✓

View information about neighboring (adjacent) routers.

Syntax **show isis neighbors** [**level-1** | **level-2**] [**detail**] [*interface*]

Parameters

level-1	(OPTIONAL) Displays information about Level 1 IS-IS neighbors.
level-2	(OPTIONAL) Displays information about Level 2 IS-IS neighbors.
detail	(OPTIONAL) Displays detailed information about neighbors.
interface	(OPTIONAL) Identifies the interface type slot/port as one of the following: • For a Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For a Port Channel, enter the keyword **port-channel** followed by a number from 1 to 32 for EtherScale, 1 to 255 for TeraScale. • For a SONET interface, enter the keyword **sonet** followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information. • For a VLAN, enter the keyword **vlan** followed by a number from 1 to 4094.

Command Modes EXEC

EXEC privilege

Example

```
Force10#show isis neighbors
System Id      Interface State     Type Priority Uptime            Circuit Id
systest-4      Gi 8/4    Init/Up   L1L2  64/64   00:00:04/00:00:03 systest-4.01/systest-4.01
systest-4      Gi 8/5    Init/Init L1L2  64/64   00:00:04/00:00:04 systest-4.02/systest-4.02
systest-4      Gi 8/6    Init/Init L1L2  64/64   00:00:04/00:00:04 systest-4.03/systest-4.03
systest-4      Gi 8/7    Init/Init L1L2  64/64   00:00:04/00:00:04 systest-4.04/systest-4.04
systest-4      Gi 8/8    Init/Init L1L2  64/64   00:00:04/00:00:04 systest-4.05/systest-4.05
systest-4      Gi 8/9    Init/Init L1L2  64/64   00:00:03/00:00:03 systest-4.06/systest-4.06
systest-4      Gi 8/10   Init/Init L1L2  64/64   00:00:03/00:00:03 systest-4.07/systest-4.07
systest-4      Gi 8/11   Init/Init L1L2  64/64   00:00:03/00:00:03 systest-4.08/systest-4.08
Force10#
```

Figure 328 show isis neighbors Command Example

Table 85 describes the information in Figure 328.

Table 85 show isis neighbors Command Example Fields

Field	Description
System Id	The value that identifies a system in an area.
Interface	The interface, slot, and port in which the router was discovered.
State	The value providing status about the adjacency state. The valid values are Up and Init.
Type	This value displays the adjacency type.
Priority	IS-IS priority advertised by the neighbor. The neighbor with highest priority becomes the designated router for the interface.
Uptime	Displays the interfaces uptime.
Circuit Id	The neighbor's interpretation of the designated router for the interface.

Usage Information Use this command to confirm that the neighbor adjacencies are operating correctly. If you suspect that they are not, you can verify the specified area addresses of the routers by using the show isis neighbors command.

show isis protocol

View IS-IS routing information.

Syntax **show isis protocol**

C-Series	No
E-Series	✓

Command Modes

EXEC

EXEC privilege

Example

```
Force10#sho isis protocol
IS-IS Router: <Null Tag>
  System Id: AAAA.AAAA.AAAA  IS-Type: level-2
  Manual area address(es):
   47.0004.004d.0001
  Routing for area address(es):
   47.0004.004d.0001
  Interfaces supported by IS-IS:
   GigabitEthernet 0/0
   GigabitEthernet 0/1
  Redistributing:
  Distance: 115
  Generate narrow metrics: level-2
  Accept narrow metrics: level-2
  Generate wide metrics: none
  Accept wide metrics: none
Force10#
```

Figure 329 show isis protocol Command Example

show isis traffic

C-Series	No
E-Series	✓

This command allows you to view IS-IS traffic interface information.

Syntax **show isis traffic** [*interface*]

Parameters

interface	(OPTIONAL) Identifies the interface type slot/port as one of the following: • For a Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For a Port Channel, enter the keyword **port-channel** followed by a number from 1 to 32 for EtherScale, 1 to 255 for TeraScale. • For a SONET interface, enter the keyword **sonet** followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information. • For a VLAN, enter the keyword **vlan** followed by a number from 1 to 4094.

Command Modes

EXEC

EXEC privilege

Example

```
Force10#sho is traffic
 IS-IS: Level-1 Hellos (sent/rcvd) : 0/721
 IS-IS: Level-2 Hellos (sent/rcvd) : 900/943
 IS-IS: PTP Hellos (sent/rcvd)     : 0/0
 IS-IS: Level-1 LSPs sourced (new/refresh) : 0/0
 IS-IS: Level-2 LSPs sourced (new/refresh) : 1/3
 IS-IS: Level-1 LSPs flooded (sent/rcvd) : 0/0
 IS-IS: Level-2 LSPs flooded (sent/rcvd) : 5934/5217
 IS-IS: Level-1 LSPs CSNPs (sent/rcvd) : 0/0
 IS-IS: Level-2 LSPs CSNPs (sent/rcvd) : 472/238
 IS-IS: Level-1 LSPs PSNPs (sent/rcvd) : 0/0
 IS-IS: Level-2 LSPs PSNPs (sent/rcvd) : 10/337
 IS-IS: Level-1 DR Elections : 4
 IS-IS: Level-2 DR Elections : 4
 IS-IS: Level-1 SPF Calculations : 0
 IS-IS: Level-2 SPF Calculations : 389
 IS-IS: LSP checksum errors received : 0
 IS-IS: LSP authentication failures : 0
Force10#
```

Figure 330 show isis traffic Command Example

Table 86 describes the information in Figure 330.

Table 86 show isis traffic Command Example Fields

Item	Description
Level-1/Level-2 Hellos (sent/rcvd)	Displays the number of Hello packets sent and received.
PTP Hellos (sent/rcvd)	Displays the number of point-to-point Hellos sent and received.
Level-1/Level-2 LSPs sourced (new/refresh)	Displays the number of new and refreshed LSPs.
Level-1/Level-2 LSPs flooded (sent/rcvd)	Displays the number of flooded LSPs sent and received.
Level-1/Level-2 LSPs CSNPs (sent/rcvd)	Displays the number of CSNP LSPs sent and received.
Level-1/Level-2 LSPs PSNPs (sent/rcvd)	Displays the number of PSNP LPSs sent and received.
Level-1/Level-2 DR Elections	Displays the number of times designated router elections ran.
Level-1/Level-2 SPF Calculations	Displays the number of shortest path first calculations.
LSP checksum errors received	Displays the number of checksum errors LSPs received.
LSP authentication failures	Displays the number of LSP authentication failures.

spf-interval

C-Series	No
E-Series	✓

Specify the minimum interval between Shortest Path First (SPF) calculations.

Syntax

spf-interval [**level-1 | level-2**] *interval seconds* [*initial_wait_interval seconds* [*second_wait_interval seconds*]]

To restore default values, use the **no spf-interval** [**level-1 | level-2**] *interval seconds* [*initial_wait_interval seconds* [*second_wait_interval seconds*]] command.

Parameters

level-1	(OPTIONAL) Enter the keyword **level-1** to apply the configuration to Level-1 SPF calculations.
level-2	(OPTIONAL) Enter the keyword **level-2** to apply the configuration to Level-2 SPF calculations.
interval seconds	Enter the maximum number of seconds between SPF calculations. Range: 0 to 120 seconds Default: 10 seconds
initial_wait_interval seconds	(OPTIONAL) Enter the initial wait time, in seconds, before running the first SPF calculations. Range: 0 to 120 seconds Default: 5 second
second_wait_interval seconds	(OPTIONAL) Enter the wait interval, in seconds, between the first and second SPF calculations. Range: 0 to 120 seconds Default: 5 seconds

Defaults

Defaults as above

Command Modes

ROUTER ISIS (conf-router-isis)

Command History

Version 7.5.1.0	Expanded to support SPF Throttling Enhancemen

Usage Information

SPF throttling slows down the frequency at which route calculation are performed during network instability. Even though throttling route calculations slows down network convergence, not throttling can result in a network not functioning as expected. If network topology is unstable, throttling slows down the scheduling of route calculations until the topology regains its stability.

The first route calculation is controlled by the initial wait interval and the second calculation is controlled by the second wait interval. Each subsequent wait interval is twice as long as the previous one until the wait interval reaches the maximum wait time specified (*interval seconds*). Once the network calms down and there are no triggers for two times the maximum interval, fast behavior is restored (the initial wait time).

Chapter 41 IPv6 IS-IS Protocol

Platform Specific Feature: IPv6 IS-IS Protocol is supported on E-Series only.

IS-IS (Intermediate System to Intermediate System), developed by the International Organization for Standardization (OSI), is an interior gateway protocol that uses a shortest-path-first algorithm. IS-IS facilitates the communication between open systems, supporting routers passing both IP and OSI traffic.

Force10's implementation of IS-IS support for IPv6 is based on the IETF Draft draft-ietf-isis-ipv6-06.txt. This implementation is best when IPv4 and IPv6 topologies are congruent in the IS-IS domain.

The following commands allow you to enable IPv6 IS-IS on the E-Series.

- address family ipv6 unicast on page 986
- adjacency-check on page 987
- advertise on page 988
- area-password on page 988
- clear config on page 989
- clear isis on page 990
- clns host on page 990
- debug isis on page 991
- debug isis adj-packets on page 992
- debug isis local-updates on page 992
- debug isis snp-packets on page 993
- debug isis spf-triggers on page 994
- debug isis update-packets on page 994
- default-information originate on page 995
- domain-password on page 996
- hello padding on page 996
- hostname dynamic on page 997
- ignore-lsp-errors on page 998

- isis circuit-type on page 998
- isis csnp-interval on page 999
- isis hello-interval on page 1000
- isis hello-multiplier on page 1001
- isis hello padding on page 1002
- isis ipv6 metric on page 1003
- isis network point-to-point on page 1003
- isis password on page 1004
- isis priority on page 1005
- is-type on page 1006
- log-adjacency-changes on page 1006
- lsp-gen-interval on page 1007
- lsp-mtu on page 1008
- lsp-refresh-interval on page 1009
- max-area-addresses on page 1010
- max-lsp-lifetime on page 1010
- maximum-paths on page 1011
- net on page 1012
- passive-interface on page 1012
- ipv6 router isis on page 1013
- set-overload-bit on page 1014
- show config on page 1015
- show isis database detail on page 1015
- show isis hostname on page 1016
- show isis interface on page 1016
- show isis neighbors on page 1017
- show isis protocol on page 1018
- spf-interval on page 1019

address family ipv6 unicast

C-Series	No
E-Series	✓

Enter the Address Family command mode.

Syntax **address family ipv6 unicast**

To exit the Address Family command mode, use the **exit-address-family** command.

Defaults No default behavior or values

Command Modes ADDRESS FAMILY (conf-router_isis-af_ipv6)

Command History

Version 7.5.1.0	Introduced

Example

```
Force10(conf-router_isis)#address-family ipv6 unicast
Force10(conf-router_isis-af_ipv6)#?
adjacency-check         Check ISIS neighbor protocol support
advertise               Control which IP routes flow between L1 and L2
default-information     Control distribution of default information
exit-address-family     Exit from Address Family configuration mode
no                      Negate a command or set its defaults
show                    Show ISIS configuration for this address family

Force10(conf-router_isis-af_ipv6)#
```

adjacency-check

C-Series	**No**
E-Series	✓

Check the IS-IS neighbor protocol support.

Syntax **adjacency-check**

To disable adjacency check, use the **no adjacency-check** command.

Defaults Enabled

Command Modes ADDRESS FAMILY (conf-router_isis-af_ipv6)

Command History

Version 7.5.1.0	Introduced

Usage Information Use this command to enable or disable protocol supported before forming an adjacency. The adjacency-check is enabled by default as the IS-IS protocol specification requires.

advertise

C-Series	No
E-Series	✓

Leak routes between levels (distribute IP prefixes between level 1 and level 2 and vice versa).

Syntax **advertise** {**level1-into-level2** | **level2-into-level1**} *prefix-list-name*

To return to the default, use the **no advertise** {**level1-into-level2** | **level2-into-level1**}[*prefix-list-name*] command.

Parameters

level1-into-level2	Enter the keyword **level1-into-level2** to advertise Level 1 routes into Level 2 LSPs. This is the default.
level2-into-level1	Enter the keyword **level2-into-level1** to advertise Level 2 inter-area routes into Level 1 LSPs. Described in RFC 2966.
prefix-list-name	Enter the name of a configured IP prefix list. Routes meeting the criteria of the IP Prefix list are leaked.

Defaults **level1-into-level2** (that is, Level 1 to Level 2 leaking enabled.)

Command Modes ADDRESS FAMILY IPV6 (conf-router_isis-af_ipv6)

Command History

Version 7.5.1.0	Introduced

Usage Information You cannot disable leaking from one level to another, *however* you can regulate the rate flow from one level to another via an IP Prefix list. If the IP Prefix list is not configured, all routes are leaked.

Additional information can be found in IETF RFC 2966, *Domain-wide Prefix Distribution with Two-Level IS-IS*.

area-password

C-Series	No
E-Series	✓

Configure the authentication password for an area.

Syntax **area-password** [**hmac-md5**] *password*

To delete a password, enter **no area-password**.

Parameters

hmac-md5	(OPTIONAL) Enter the keyword **hmac-md5** to encrypt the password.
password	Enter a 1—16-character length alphanumeric string to prevent unauthorized access or incorrect routing information corrupting the link state database. The password is processed as plain text which only provides limited security.

Defaults

Not configured.

Command Modes

ROUTER ISIS (conf-router_isis)

Command History

Version 7.5.1.0	Introduced

Usage Information

Use the area-password command on routers within an area to prevent the link state database from receiving incorrect routing information from unauthorized routers.

The password configured is injected into Level 1 LSPs, CSNPs, and PSNPs.

Related Commands

domain-password	Allows you to set the authentication password for a routing domain.
isis password	Allows you to configure an authentication password for an interface.

clear config

C-Series	**No**
E-Series	✓

Clear IS-IS configurations that display under the router IS-IS mode of the show running-config command output.

Syntax

clear config

Command Modes

ROUTER ISIS (conf-router_isis)

Command History

Version 7.5.1.0	Introduced

Usage Information

Use caution when you enter this command. Back up your configuration prior to using this command or your IS-IS configuration will be erased.

Related Commands		
	copy	Use this command to save the current configuration to another location.

clear isis

C-Series	No
E-Series	✓

Restart the IS-IS process. All IS-IS data is cleared.

Syntax **clear isis** [*tag*] {* | **database** | **traffic**}

Parameters

tag	(Optional) Enter an alphanumeric string to specify the IS-IS routing tag area.
*	Enter the asterisk (*) to clear all IS-IS information and restarts the IS-IS process. This command removes IS-IS neighbor information and IS-IS LSP database information and the full SPF calculation will be done.
database	Clears IS-IS LSP database information.
traffic	Clears IS-IS counters.

Command Modes EXEC privilege

Command History

Version 7.5.1.0	Introduced

clns host

C-Series	No
E-Series	✓

Define a name-to-network service mapping point (NSAP) mapping that can then be used with commands that require NSAPs and system IDs.

Syntax **clns host** *name nsap*

Parameters

name	Enter an alphanumeric string to identify the name-to-NSAP mapping.
nsap	Enter a specific NSAP address that will be associated with the *name* parameter.

Defaults Not configured

Command Modes ROUTER ISIS (conf-router_isis)

Command History

Version 7.5.1.0	Introduced

Usage Information Use this command to configure a shortcut name that can used instead of entering a long string of numbers associated with an NSAP address.

Related Commands

hostname dynamic	Enables dynamic learning of hostname from routers in the domain and allows the routers to advertise the hostname in LSPs.

debug isis

C-Series	**No**
E-Series	✓

Enable debugging for all IS-IS operations.

Syntax **debug isis**

To disable debugging of IS-IS, enter **no debug isis**.

Command Modes EXEC privilege

Command History

Version 7.5.1.0	Introduced

Usage Information Entering **debug isis** enables all debugging parameters.

Use this command to view all debugging information in one output. To turn off debugging, you normally enter separate **no** forms of each command. Enter the **no debug isis** command to disable all debug messages for IS-IS at once.

debug isis adj-packets

C-Series	No
E-Series	✓

Enable debugging on adjacency-related activity such as hello packets that are sent and received on IS-IS adjacencies.

Syntax **debug isis adj-packets** [*interface*]

To turn off debugging, use the **no debug isis adj-packets** [*interface*] command.

Parameters

interface	(OPTIONAL) Identifies the interface type slot/port as one of the following: • For a Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For a Port Channel, enter the keyword **port-channel** followed by a number from 1 to 255. • For a SONET interface, enter the keyword **sonet** followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information. • For a VLAN, enter the keyword **vlan** followed by a number from 1 to 4094.

Command Modes EXEC privilege

Command History

Version 7.5.1.0	Introduced

debug isis local-updates

C-Series	No
E-Series	✓

Enables debugging on a specific interface and provides diagnostic information to debug IS-IS local update packets.

Syntax **debug isis local-updates** [*interface*]

To turn off debugging, enter the **no debug isis local-updates** [*interface*] command.

Parameters

interface	(OPTIONAL) Identifies the interface type slot/port as one of the following: • For a Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For a Port Channel, enter the keyword **port-channel** followed by a number from 1 to 255. • For a SONET interface, enter the keyword **sonet** followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information. • For a VLAN, enter the keyword **vlan** followed by a number from 1 to 4094.

Command Modes EXEC privilege

Command History

Version 7.5.1.0	Introduced

debug isis snp-packets

C-Series	No
E-Series	✓

Enable debugging on a specific interface and provides diagnostic information to debug IS-IS complete sequence number PDU (CSNP) and partial sequence number PDU (PSNP) packets.

Syntax **debug isis snp-packets** [*interface*]

To turn off debugging, enter the **no debug isis snp-packets** [*interface*] command.

Parameters

interface	(OPTIONAL) Identifies the interface type slot/port as one of the following: • For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For a Port Channel interface, enter **port-channel** followed by a number from 1 to 255. • For a SONET interface, enter the keyword **sonet** followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information. • For a VLAN, enter the keyword **vlan** followed by a number from 1 to 4094.

Command Modes EXEC privilege

Command History

Version 7.5.1.0	Introduced

debug isis spf-triggers

C-Series	No
E-Series	✓

Enable debugging on the events that triggered IS-IS shortest path first (SPF) events for debugging purposes.

Syntax **debug isis spf-triggers**

To turn off debugging, enter **no debug isis spf-triggers**.

Command Modes EXEC privilege

Command History

Version 7.5.1.0	Introduced

debug isis update-packets

C-Series	No
E-Series	✓

Enable debugging on Link State PDUs (LSPs) that are detected by a router.

Syntax **debug isis update-packets** [*interface*]

To turn off debugging, enter the **no debug isis update-packets** [*interface*] command.

Parameters

interface	(OPTIONAL) Identifies the interface type slot/port as one of the following: • For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For a Port Channel interface, enter **port-channel** followed by a number from 1 to 255. • For a SONET interface, enter the keyword **sonet** followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information. • For a VLAN, enter the keyword **vlan** followed by a number from 1 to 4094.

Command Modes EXEC privilege

Command History

Version 7.5.1.0	Introduced

default-information originate

C-Series	No
E-Series	✓

Generate a default route into an IS-IS routing domain and controls the distribution of default information.

Syntax

default-information originate [**always**] [**metric** *metric*] [**route-map** *map-name*]

To disable the generation of a default route into the specified IS-IS routing domain, enter the **no default-information originate** [**always**] [**metric** *metric*] [**route-map** *map-name*] command.

Parameters

always	(OPTIONAL) Enter the keyword **always** to have the default route always advertised
metric *metric*	(OPTIONAL) Enter the keyword **metric** followed by a number to assign to the route. Range: 0 to 16777215
route-map *map-name*	(OPTIONAL) A default route will be generated by the routing process if the route map is satisfied.

Defaults

Not configured.

Command Modes

ADDRESS FAMILY IPV6 (conf-router_isis-af_ipv6)

Command History

Version 7.5.1.0	Introduced

Usage Information

When you use this command to redistribute routes into a routing domain, the router becomes an autonomous system (AS) boundary router. An AS boundary router does not always generate a default route into a routing domain. The router still requires its own default route before it can generate one.

How a metric value assigned to a default route is advertised depends on how on the configuration of the metric. If the metric is set for narrow mode and the metric value in the default-information originate command is set to a number higher than 63, the metric value advertised in LSPs will be 63. If the metric is set for wide mode, their the metric value in the default-information originate command is advertised.

Related Commands

isis ipv6 metric	Configure a metric for an interface
show isis database detail	Display the IS-IS link state database.

domain-password

C-Series	No
E-Series	✓

Set the authentication password for a routing domain.

Syntax **domain-password** [**hmac-md5** | *encryption-type*] *password*

To disable the password, enter **no domain-password**.

Parameters

hmac-md5	(OPTIONAL) Enter the keyword **hmac-md5** to encrypt the password using MD5.
encryption-type	(OPTIONAL) Enter 7 to encrypt the password using DES.
password	Enter an alphanumeric string up to 16 characters long.

Defaults No default password.

Command Modes ROUTER ISIS (conf-router_isis)

Command History

Version 7.5.1.0	Introduced

Usage Information The domain password is inserted in Level 2 link state PDUs (LSPs), complete sequence number PDUs (CSNPs), and partial sequence number PDUs (PSNPs).

Related Commands

area-password	Configure an IS-IS area authentication password.
isis password	Configure the authentication password for an interface.

hello padding

C-Series	No
E-Series	✓

Use to turn ON or OFF padding for LAN and point-to-point hello PDUs or to selectively turn padding ON or OFF for LAN or point-to-point hello PDUs.

Syntax **hello padding** [**multi-point** | **point-to-point**]

To return to default, use **no hello padding** [**multi-point** | **point-to-point**].

Parameters

multi-point	(OPTIONAL) Enter the keyword **multi-point** to pad only LAN hello PDUs.
point-to-point	(OPTIONAL) Enter the keyword **point-to-point** to pad only point-to-point PDUs.

Defaults

Both LAN and point-to-point hello PDUs are padded.

Command Modes

ROUTER ISIS (conf-router_isis)

Command History

Version 7.5.1.0	Introduced

Usage Information

IS-IS hellos are padded to the full maximum transmission unit (MTU) size. Padding IS-IS Hellos (IIHS) to the full MTU provides early error detection of large frame transmission problems or mismatched MTUs on adjacent interfaces.

Related Commands

isis hello padding	Turn ON or OFF hello padding on an interface basis.

hostname dynamic

C-Series	No
E-Series	✓

Enables dynamic learning of hostname from routers in the domain and allows the routers to advertise the hostname in LSPs.

Syntax

hostname dynamic

To disable this command, enter **no hostname dynamic**.

Defaults

Enabled.

Command Modes

ROUTER ISIS (conf-router_isis)

Command History

Version 7.5.1.0	Introduced

Usage Information

Use this command to build name-to-systemID mapping tables through the protocol. All **show** commands that display systems also display the hostname.

Related Commands

cln host	Define a name-to-NSAP mapping.

ignore-lsp-errors

C-Series	**No**
E-Series	✓

Ignore LSPs with bad checksums instead of purging those LSPs.

Syntax

ignore-lsp-errors

To return to the default values, enter **no ignore-lsp-errors**.

Defaults

In IS-IS, the default *deletes* LSPs with internal checksum errors (**no ignore-lsp-errors**).

Command Modes

ROUTER ISIS (conf-router_isis)

Command History

Version 7.5.1.0	Introduced

Usage Information

IS-IS normally purges LSPs with an incorrect data link checksum, causing the LSP source to regenerate the message. A cycle of purging and regenerating LSPs can occur when a network link continues to deliver accurate LSPs even though there is a link causing data corruption. This could cause disruption to your system operation.

isis circuit-type

C-Series	**No**
E-Series	✓

Configure the adjacency type on interfaces.

Syntax **isis circuit-type** {**level-1** | **level-1-2** | **level-2-only**}

To return to the default values, enter **no isis circuit-type**.

Parameters

level-1	You can form a Level 1 adjacency if there is at least one common area address between this system and neighbors. You cannot form Level 2 adjacencies on this interface.
level-1-2	You can form a Level 1 and Level 2 adjacencies when the neighbor is also configured as Level-1-2 and there is at least one common area, if not, then a Level 2 adjacency is established. This is the default.
level-2-only	You can form a Level 2 adjacencies when other Level 2 or Level 1-2 routers and their interfaces are configured for Level 1-2 or Level 2. Level 1 adjacencies cannot be established on this interface.

Defaults level-1-2

Command Modes INTERFACE

Command History

Version 7.5.1.0	Introduced

Usage Information Because the default establishes Level 1 and Level 2 adjacencies, you do not need to configure this command. Routers in an IS-IS system should be configured as a Level 1-only, Level 1-2, or Level 2-only system.

Only configure interfaces as Level 1 or Level 2 on routers that are between areas (for example, a Level 1-2 router) to prevent the software from sending unused hello packets and wasting bandwidth.

isis csnp-interval

C-Series	No
E-Series	✓

Configure the IS-IS complete sequence number PDU (CSNP) interval on an interface.

Syntax **isis csnp-interval** *seconds* [**level-1** | **level-2**]

To return to the default values, enter the **no isis csnp-interval** [*seconds*] [**level-1** | **level-2**] command.

Parameters

seconds	Interval of transmission time between CSNPs on multi-access networks for the designated intermediate system. Range: 0 to 65535 Default: 10
level-1	(OPTIONAL) Independently configures the interval of time between transmission of CSNPs for Level 1.
level-2	(OPTIONAL) Independently configures the interval of time between transmission of CSNPs for Level 2.

Defaults *seconds* = 10; **level-1** (if not otherwise specified)

Command Modes INTERFACE

Command History

Version 7.5.1.0	Introduced

Usage Information The default values of this command are typically satisfactory transmission times for a specific interface on a designated intermediate system. To maintain database synchronization, the designated routers send CSNPs.

Level 1 and Level 2 CSNP intervals can be configured independently.

isis hello-interval

C-Series	No
E-Series	✓

Specify the length of time between hello packets sent.

Syntax **isis hello-interval** *seconds* [**level-1** | **level-2**]

To return to the default values, enter the **no isis hello-interval** [*seconds*] [**level-1** | **level-2**] command.

Parameters

seconds	Allows you to set the length of time between hello packet transmissions. Range: 1 to 65535 Default: 10
level-1	(OPTIONAL) Select this value to configure the hello interval for Level 1. This is the default.
level-2	(OPTIONAL) Select this value to configure the hello interval for Level 2.

Defaults *seconds* = 10; **level-1** (if not otherwise specified)

Command Modes INTERFACE

Command History

Version 7.5.1.0	Introduced

Usage Information Hello packets are held for a length of three times the value of the hello interval. Use a high hello interval seconds to conserve bandwidth and CPU usage. Use a low hello interval seconds for faster convergence (but uses more bandwidth and CPU resources).

Related Commands

isis hello-multiplier	Specifies the number of IS-IS hello packets a neighbor must miss before the router should declare the adjacency as down.

isis hello-multiplier

C-Series	**No**
E-Series	✔

Specify the number of IS-IS hello packets a neighbor must miss before the router declares the adjacency down.

Syntax **isis hello-multiplier** *multiplier* [**level-1** | **level-2**]

To return to the default values, enter **no isis hello-multiplier** [*multiplier*] [**level-1** | **level-2**].

Parameters

multiplier	Specifies an integer that sets the multiplier for hello holding time. Never configure a hello-multiplier lower then the default (3). Range: 3 to 1000 Default: 3
level-1	(OPTIONAL) Select this value to configure the hello multiplier independently for Level 1 adjacencies. This is the default.
level-2	(OPTONAL) Select this value to configure the hello multiplier independently for Level 2 adjacencies.

Defaults *multiplier* =3; **level-1** (if not otherwise specified)

Command Modes INTERFACE

Command History

Version 7.5.1.0	Introduced

Usage Information

The holdtime (the product of the hello-multiplier multiplied by the hello-interval) determines how long a neighbor waits for a hello packet before declaring the neighbor is down so routes can be recalculated.

Related Commands

isis hello-interval	Specify the length of time between hello packets.

isis hello padding

C-Series	**No**
E-Series	✓

Turn ON or OFF padding of hello PDUs from the interface mode.

Syntax **isis hello padding**

To return to the default, use the **no isis hello padding**.

Defaults Padding of hello PDUs is enabled (ON).

Command Modes INTERFACE

Command History

Version 7.5.1.0	Introduced

Usage Information

Hello PDUs are “padded” only when both the global and interface padding options are ON. Turning either one OFF will disable padding for the corresponding interface(s).

Related Commands

hello padding	Turn ON or OFF padding for LAN and point-to-point hello PDUs.

isis ipv6 metric

C-Series	No
E-Series	✓

Assign metric to an interface for use with IPv6 information.

Syntax **isis ipv6 metric** *default-metric* [**level-1** | **level-2**]

To return to the default values, enter **no ipv6 isis metric** [*default-metric*] [**level-1** | **level-2**].

Parameters

default-metric	Metric assigned to the link and used to calculate the cost from each other router via the links in the network to other destinations. You can configure this metric for Level 1 or Level 2 routing. Range:0 to 16777215 Default: 10
level-1	(OPTIONAL) Enter **level-1** to configure the shortest path first (SPF) calculation for Level 1 (intra-area) routing. This is the default.
level-2	(OPTIONAL) Enter **level-2** to configure the SPF calculation for Level 2 (inter-area) routing.

Defaults *default-metric* = 10; **level-1** (if not otherwise specified)

Command Modes INTERFACE

Command History

Version 7.5.1.0	Introduced

Usage Information Force10 Networks recommends configuring metrics on all interfaces. Without configuring this command, the IS-IS metrics are similar to hop-count metrics.

isis network point-to-point

C-Series	No
E-Series	✓

Enable the software to treat a broadcast interface as a point-to-point interface.

Syntax **isis network point-to-point**

To disable the feature, enter **no isis network point-to-point**.

Defaults Not enabled.

Command Modes INTERFACE

Command History

Version 7.5.1.0	Introduced

isis password

C-Series	No
E-Series	✓

Configure an authentication password for an interface.

Syntax **isis password** *password* [**level-1** | **level-2**]

To delete a password, enter the **no isis password** [*password*] [**level-1** | **level-2**] command.

Parameters

encryption-type	(OPTIONAL) Enter 7 to encrypt the password using DES.
password	Assign the interface authentication password.
level-1	(OPTIONAL) Independently configures the authentication password for Level 1. The router acts as a station router for Level 1 routing. This is the default.
level-2	(OPTIONAL) Independently configures the authentication password for Level 2. The router acts as an area router for Level 2 routing.

Defaults No default password. **level-1** (if not otherwise specified)

Command Modes INTERFACE

Command History

Version 7.5.1.0	Introduced

Usage Information To protect your network from unauthorized access, use this command to prevent unauthorized routers from forming adjacencies.

You can assign different passwords for different routing levels by using the **level-1** and **level-2** keywords.

The **no** form of this command disables the password for Level 1 or Level 2 routing, using the respective keywords **level-1** or **level-2**.

This password provides limited security as it is processed as plain text.

isis priority

C-Series	No
E-Series	✔

Set priority of the designated router you select.

Syntax

isis priority *value* [**level-1** | **level-2**]

To return to the default values, enter the **no isis priority** [*value*] [**level-1** | **level-2**] command.

Parameters

value	This value sets the router priority. The higher the value, the higher the priority. Range: 0 to 127 Default: 64
level-1	(OPTIONAL) Specify the priority for Level 1. This is the default.
level-2	(OPTIONAL) Specify the priority for Level 2.

Defaults

value = 64; **level-1** (if not otherwise specified)

Command Modes

INTERFACE

Command History

Version 7.5.1.0	Introduced

Usage Information

You can configure priorities independently for Level 1 and Level 2. Priorities determine which router on a LAN will be the designated router. Priorities are advertised within hellos. The router with the highest priority will become the designated intermediate system (DIS).

Routers with priority of 0 cannot be a designated router. Setting the priority to 0 lowers the chance of this system becoming the DIS, but does not prevent it. If all the routers have priority 0, one with highest MAC address will become DIS even though its priority is 0.

is-type

C-Series	No
E-Series	✓

Configure IS-IS operating level for a router.

Syntax **is-type** {**level-1** | **level-1-2** | **level-2-only**}

To return to the default values, enter **no is-type**.

Parameters

level-1	Allows a router to act as a Level 1 router.
level-1-2	Allows a router to act as both a Level 1 and Level 2 router. This is the default.
level-2-only	Allows a router to act as a Level 2 router.

Defaults **level-1-2**

Command Modes ROUTER ISIS (conf-router_isis)

Command History

Version 7.5.1.0	Introduced

Usage Information The IS-IS protocol automatically determines area boundaries and are able to keep Level 1 and Level 2 routing separate. Poorly planned use of this feature may cause configuration errors, such as accidental area partitioning.

If you are configuring only one area in your network, you do not need to run both Level 1 and Level 2 routing algorithms. The IS type can be configured as Level 1.

log-adjacency-changes

C-Series	No
E-Series	✓

Generate a log messages for adjacency state changes.

Syntax **log-adjacency-changes**

To disable this function, enter **no log-adjacency-changes**.

Defaults Adjacency changes are not logged.

Command Modes ROUTER ISIS (conf-router_isis)

Command History

Version 7.5.1.0	Introduced

Usage Information This command allow you to monitor adjacency state changes, which is useful when you monitor large networks. Messages are logged in the system error message facility.

lsp-gen-interval

C-Series	**No**
E-Series	✓

Set the minimum interval between successive generation of link-state packets (LSPs).

Syntax **lsp-gen-interval** [**level-1** | **level-2**] *interval seconds* [*initial_wait_interval seconds* [*second_wait_interval seconds*]]

To restore default values, use the **no lsp-gen-interval** [**level-1** | **level-2**] *interval seconds* [*initial_wait_interval seconds* [*second_wait_interval seconds*]] command.

Parameters

level-1	(OPTIONAL) Enter the keyword **level-1** to apply the configuration to generation of Level-1 LSPs.
level-2	(OPTIONAL) Enter the keyword **level-2** to apply the configuration to generation of Level-2 LSPs.
interval seconds	Enter the maximum number of seconds between LSP generations. Range: 0 to 120 seconds Default: 5 seconds
initial_wait_interval seconds	(OPTIONAL) Enter the initial wait time, in seconds, before running the first LSP generation. Range: 0 to 120 seconds Default: 1 second
second_wait_interval seconds	(OPTIONAL) Enter the wait interval, in seconds, between the first and second LSP generation. Range: 0 to 120 seconds Default: 5 seconds

Defaults Defaults as above

Command Modes ROUTER ISIS (conf-router_isis)

Command History

Version 7.5.1.0	Introduced

Usage Information LSP throttling slows down the frequency at which LSPs are generated during network instability. Even though throttling LSP generations slows down network convergence, no throttling can result in a network not functioning as expected. If network topology is unstable, throttling slows down the scheduling of LSP generations until the topology regains its stability.

The first generation is controlled by the initial wait interval and the second generation is controlled by the second wait interval. Each subsequent wait interval is twice as long as the previous one until the wait interval reaches the maximum wait time specified (*interval seconds*). Once the network calms down and there are no triggers for two times the maximum interval, fast behavior is restored (the initial wait time).

lsp-mtu

C-Series	No
E-Series	✓

Set the maximum transmission unit (MTU) of IS-IS link-state packets (LSPs). This command only limits the size of LSPs generated by this router.

Syntax **lsp-mtu** *size*

To return to the default values, enter **no lsp-mtu**.

Parameters

size	The maximum LSP size, in bytes. Range: 128 to 1497 for non-jumbo mode; 128 to 9195 for jumbo mode. Default: 1497

Defaults 1497 bytes

Command Modes ROUTER ISIS (conf-router_isis)

Command History

Version 7.5.1.0	Introduced

Usage Information

The link MTU (mtu command) and the LSP MTU size must be the same

Since each device can generate a maximum of 255 LSPs, consider carefully whether the lsp-mtu command should be configured.

lsp-refresh-interval

C-Series	**No**
E-Series	✓

Set the link state PDU (LSP) refresh interval. LSPs must be refreshed before they expire. When the LSPs are not refreshed after a refresh interval, they are kept in a database until their max-lsp-lifetime reaches zero and then LSPs will be purged.

Syntax

lsp-refresh-interval *seconds*

To restore the default refresh interval, enter **no lsp-refresh-interval**.

Parameters

seconds	The LSP refresh interval, in seconds. This value has to be less than the seconds value specified with the max-lsp-lifetime command. Range: 1 to 65535 seconds. Default: 900

Defaults

900 seconds

Command Modes

ROUTER ISIS (conf-router_isis)

Command History

Version 7.5.1.0	Introduced

Usage Information

The refresh interval determines the rate at which route topology information is transmitted preventing the information from becoming obsolete.

The refresh interval must be less than the LSP lifetime specified with the max-lsp-lifetime command. A low value reduces the amount of time that undetected link state database corruption can persist at the cost of increased link utilization. A higher value reduces the link utilization caused by the flooding of refreshed packets.

Related Commands

max-lsp-lifetime	Sets the maximum interval that LSPs persist without being refreshed

max-area-addresses

C-Series	No
E-Series	✓

Use this command to configure the number of area addresses on router.

Syntax **max-area-addresses** *number*

To return to the default values, enter **no max-area-addresses**.

Parameters

number	Set the maximum number of manual area addresses. Range: 3 to 6. Default: 3

Defaults 3 addresses

Command Modes ROUTER ISIS (conf-router_isis)

Command History

Version 7.5.1.0	Introduced

Usage Information This value should be consistent with routers in the same area, or else, the router will form only Level 2 adjacencies. The value should be same among all the routers to form Level 1 adjacencies.

max-lsp-lifetime

C-Series	No
E-Series	✓

Set the maximum time that link-state packets (LSPs) exist without being refreshed.

Syntax **max-lsp-lifetime** *seconds*

To restore the default time, enter **no max-lsp-lifetime**.

Parameters

seconds	The maximum lifetime of LSP in seconds. This value must be greater than the lsp-refresh-interval . The higher the value the longer the LSPs are kept. Range: 1 to 65535 Default: 1200

Defaults 1200 seconds

Command Modes ROUTER ISIS (conf-router_isis)

Command History

Version 7.5.1.0	Introduced

Usage Information Change the maximum LSP lifetime with this command. The maximum LSP lifetime must always be greater than the LSP refresh interval.

The *seconds* parameter enables the router to keep LSPs for the specified length of time. If the value is higher, the overhead is reduced on slower-speed links.

Related Commands

lsp-refresh-interval	Use this command to set the link-state packet (LSP) refresh interval.

maximum-paths

C-Series	**No**
E-Series	✔

Allows you to configure the maximum number of parallel paths allowed in a routing table.

Syntax **maximum-paths** *number*

To return to the default values, enter **no maximum-paths**.

Parameters

number	Enter a number as the maximum number of parallel paths an IP routing installs in a routing table. Range: 1 to 16. Default: 4

Defaults 4

Command Mode ROUTER ISIS (conf-router_isis)

Command History

Version 7.5.1.0	Introduced

net

C-Series	No
E-Series	✓

Use this mandatory command to configure an IS-IS network entity title (NET) for a routing process. If a NET is not configured, the IS-IS process will not start.

Syntax **net** *network-entity-title*

To remove a net, enter **no net** *network-entity-title*.

Parameters

network-entity-title	Specify the area address and system ID for an IS-IS routing process. The first 1 to 13 bytes identify the area address. The next 6 bytes identify the system ID. The last 1 byte is the selector byte, always identified as zero zero (00). This argument can be applied to an address or a name.

Defaults Not configured.

Command Modes ROUTER ISIS (conf-router_isis)

Command History

Version 7.5.1.0	Introduced

passive-interface

C-Series	No
E-Series	✓

Suppress routing updates on an interface. This command stops the router from sending updates on that interface.

Syntax **passive-interface** *interface*

To delete a passive interface configuration, enter the **no passive-interface** *interface* command.

Parameters

interface	Enter the following keywords and slot/port or number information: • For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For Loopback interface, enter the keyword **loopback** followed by a number from zero (0) to 16383. • For a Port Channel interface, enter the keyword **port-channel** followed by a number from 1 to 32 for EtherScale, 1 to 255 for TeraScale. • For a SONET interface, enter the keyword **sonet** followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information. • For a VLAN, enter the keyword **vlan** followed by a number from 1 to 4094.

Defaults Not configured.

Command Modes ROUTER ISIS (conf-router_isis)

Command History

Version 7.5.1.0	Introduced

Usage Information Although the passive interface will neither send nor receive routing updates, the network on that interface will still be included in IS-IS updates sent via other interfaces

ipv6 router isis

C-Series	**No**
E-Series	✓

Enable the IPv6 IS-IS routing protocol and specify an IPv6 IS-IS process.

Syntax **ipv6 router isis** [*tag*]

To disable IS-IS routing, enter **no router isis** [*tag*].

Parameters

tag	(OPTIONAL) This is a unique name for a routing process. A null tag is assumed if the tag option is not specified. The tag name must be unique for all IP router processes for a given router.

Defaults Not configured.

Command Modes ROUTER ISIS (conf-router_isis)

Command History

Version 7.5.1.0	Introduced

Usage Information

You must configure a network entity title (the net command) to specify the area address and the router system ID.

You must enable routing on one or more interfaces to establish adjacencies and establish dynamic routing.

Only one IS-IS routing process can be configured to perform Level 2 routing. A **level-1-2** designation performs Level 1 and Level 2 routing at the same time.

Related Commands

net	Configure an IS-IS network entity title (NET) for a routing process.
is-type	Assign a type for a given area.

set-overload-bit

C-Series	**No**
E-Series	✔

Configure the router to set the overload bit in its non-pseudonode LSPs. This prevents other routers from using it as an intermediate hop in their shortest path first (SPF) calculations.

Syntax

set-overload-bit

To return to the default values, enter **no set-overload-bit**.

Defaults

Not set.

Command Mode

ROUTER ISIS (conf-router_isis)

Command History

Version 7.5.1.0	Introduced

Usage Information

Set the overload bit when a router experiences problems, such as a memory shortage due to an incomplete link state database which can result in an incomplete or inaccurate routing table. If you set the overload bit in its LSPs, other routers ignore the unreliable router in their SPF calculations until the router has recovered.

show config

C-Series	No
E-Series	✓

View the changes you made to the IS-IS configuration. Default values are not shown.

Syntax **show config**

Command Modes ADDRESS FAMILY (conf-router_isis-af_ipv6)

Command History

Version 7.5.1.0	Introduced

show isis database detail

C-Series	No
E-Series	✓

View the IS-IS link state database.

Syntax **show isis database** [**level-1** | **level-2**] [**local**] [**detail** | **summary**] [*lspid*]

Parameters

level-1	(OPTIONAL) Displays the Level 1 IS-IS link-state database.
level-2	(OPTIONAL) Displays the Level 2 IS-IS link-state database.
local	(OPTIONAL) Displays local link-state database information.
detail	(OPTIONAL) Detailed link-state database information of each LSP displays when specified. If not specified, a summary displays.
summary	(OPTIONAL) Summary of link-state database information displays when specified.
lspid	(OPTIONAL) Display only the specified LSP.

Command Modes EXEC

EXEC privilege

Command History

Version 7.5.1.0	Introduced

show isis hostname

C-Series	No
E-Series	✓

View IS-IS host names configured or learned on the E-Series.

Syntax **show isis hostname**

Command Modes EXEC

EXEC privilege

Command History

Version 7.5.1.0	Introduced

Example

```
Force10#sho isis hostname
System Id       Dynamic Name   Static Name
 BBBB.BBBB.BBBB F10            B233
*AAAA.AAAA.AAAA Force10        B232
Force10#
```

Figure 331 show isis hostname Command Example

show isis interface

C-Series	No
E-Series	✓

View detailed IS-IS interface status and configuration information.

Syntax **show isis interface** [*interface*]

Parameters

interface	(OPTIONAL) Enter the following keywords and slot/port or number information: • For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For Loopback interface, enter the keyword **loopback** followed by a number from zero (0) to 16383. • For a Port Channel, enter the keyword **port-channel** followed by a number from 1 to 32 for EtherScale, 1 to 255 for TeraScale. • For a SONET interface, enter the keyword **sonet** followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information. • For a VLAN, enter the keyword **vlan** followed by a number from 1 to 4094.

Command Modes

EXEC

EXEC privilege

Command History

Version 7.5.1.0	Introduced

show isis neighbors

C-Series	No
E-Series	✓

View information about neighboring (adjacent) routers.

Syntax

show isis neighbors [**level-1** | **level-2**] [**detail**] [*interface*]

Parameters

level-1	(OPTIONAL) Displays information about Level 1 IS-IS neighbors.
level-2	(OPTIONAL) Displays information about Level 2 IS-IS neighbors.
detail	(OPTIONAL) Displays detailed information about neighbors.
interface	(OPTIONAL) Identifies the interface type slot/port as one of the following: • For a Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For a Port Channel, enter the keyword **port-channel** followed by a number from 1 to 32 for EtherScale, 1 to 255 for TeraScale. • For a SONET interface, enter the keyword **sonet** followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information. • For a VLAN, enter the keyword **vlan** followed by a number from 1 to 4094.

Command Modes

EXEC

EXEC privilege

Command History

Version 7.5.1.0	Introduced

Example

```
Force10#show isis neighbors
System Id      Interface State     Type Priority Uptime            Circuit Id
systest-4      Gi 8/4    Init/Up   L1L2  64/64   00:00:04/00:00:03 systest-4.01/systest-4.01
systest-4      Gi 8/5    Init/Init L1L2  64/64   00:00:04/00:00:04 systest-4.02/systest-4.02
systest-4      Gi 8/6    Init/Init L1L2  64/64   00:00:04/00:00:04 systest-4.03/systest-4.03
systest-4      Gi 8/7    Init/Init L1L2  64/64   00:00:04/00:00:04 systest-4.04/systest-4.04
systest-4      Gi 8/8    Init/Init L1L2  64/64   00:00:04/00:00:04 systest-4.05/systest-4.05
systest-4      Gi 8/9    Init/Init L1L2  64/64   00:00:03/00:00:03 systest-4.06/systest-4.06
systest-4      Gi 8/10   Init/Init L1L2  64/64   00:00:03/00:00:03 systest-4.07/systest-4.07
systest-4      Gi 8/11   Init/Init L1L2  64/64   00:00:03/00:00:03 systest-4.08/systest-4.08
Force10#
```

Figure 332 show isis neighbors Command Example

Table 87 describes the information in Figure 332.

Table 87 show isis neighbors Command Example Fields

Field	Description
System Id	The value that identifies a system in an area.
Interface	The interface, slot, and port in which the router was discovered.
State	The value providing status about the adjacency state. The valid values are Up and Init.
Type	This value displays the adjacency type.
Priority	IS-IS priority advertised by the neighbor. The neighbor with highest priority becomes the designated router for the interface.
Uptime	Displays the interfaces uptime.
Circuit Id	The neighbor's interpretation of the designated router for the interface.

Usage Information

Use this command to confirm that the neighbor adjacencies are operating correctly. If you suspect that they are not, you can verify the specified area addresses of the routers by using the show isis neighbors command.

show isis protocol

View IS-IS routing information.

C-Series	No
E-Series	✓

Syntax **show isis protocol**

Command Modes EXEC

EXEC privilege

Command History

Version 7.5.1.0	Introduced

Example

```
Force10#sho isis protocol
IS-IS Router: <Null Tag>
  System Id: AAAA.AAAA.AAAA  IS-Type: level-2
  Manual area address(es):
   47.0004.004d.0001
  Routing for area address(es):
   47.0004.004d.0001
  Interfaces supported by IS-IS:
   GigabitEthernet 0/0
   GigabitEthernet 0/1
  Redistributing:
  Distance: 115
  Generate narrow metrics: level-2
  Accept narrow metrics: level-2
  Generate wide metrics: none
  Accept wide metrics: none
Force10#
```

Figure 333 show isis protocol Command Example

spf-interval

C-Series	No
E-Series	✓

Specify the minimum interval between Shortest Path First (SPF) calculations.

Syntax **spf-interval** [**level-1 | level-2**] *interval seconds* [*initial_wait_interval seconds* [*second_wait_interval seconds*]]

To restore default values, use the **no spf-interval** [**level-1 | level-2**] *interval seconds* [*initial_wait_interval seconds* [*second_wait_interval seconds*]] command.

Parameters

level-1	(OPTIONAL) Enter the keyword **level-1** to apply the configuration to Level-1 SPF calculations.
level-2	(OPTIONAL) Enter the keyword **level-2** to apply the configuration to Level-2 SPF calculations.
interval seconds	Enter the maximum number of seconds between SPF calculations. Range: 0 to 120 seconds Default: 10 seconds
initial_wait_interval seconds	(OPTIONAL) Enter the initial wait time, in seconds, before running the first SPF calculations. Range: 0 to 120 seconds Default: 5 second
second_wait_interval seconds	(OPTIONAL) Enter the wait interval, in seconds, between the first and second SPF calculations. Range: 0 to 120 seconds Default: 5 seconds

Defaults

Defaults as above

Command Modes

ROUTER ISIS (conf-router-isis)

Command History

Version 7.5.1.0	Introduced

Usage Information

SPF throttling slows down the frequency at which route calculation are performed during network instability. Even though throttling route calculations slows down network convergence, not throttling can result in a network not functioning as expected. If network topology is unstable, throttling slows down the scheduling of route calculations until the topology regains its stability.

The first route calculation is controlled by the initial wait interval and the second calculation is controlled by the second wait interval. Each subsequent wait interval is twice as long as the previous one until the wait interval reaches the maximum wait time specified (*interval seconds*). Once the network calms down and there are no triggers for two times the maximum interval, fast behavior is restored (the initial wait time).

Chapter 42 BGP

Platform Specific Feature: BGP is supported on E-Series only.

FTOS support Border Gateway Protocol (BGP) and Multiprotocol Border Gateway Protocol (MBGP). For detailed information on configuring BGP, refer to *FTOS Configuration Guide*. This chapter contains the following sections:

- BGP Commands on page 1021
- MBGP Commands on page 1098

BGP Commands

Border Gateway Protocol (BGP) is an external gateway protocol that transmits interdomain routing information within and between Autonomous Systems (AS). BGP version 4 (BGPv4) supports classless interdomain routing and the aggregation of routes and AS paths. Basically, two routers (called neighbors or peers) exchange information including full routing tables and periodically send messages to update those routing tables.

The following commands allow you to configure and enable BGP.

- aggregate-address on page 1024
- bgp always-compare-med on page 1025
- bgp bestpath as-path ignore on page 1025
- bgp bestpath med confed on page 1026
- bgp bestpath med missing-as-best on page 1026
- bgp client-to-client reflection on page 1027
- bgp cluster-id on page 1027
- bgp confederation identifier on page 1028
- bgp confederation peers on page 1029
- bgp dampening on page 1029
- bgp default local-preference on page 1030

- bgp enforce-first-as on page 1031
- bgp fast-external-fallover on page 1032
- bgp graceful-restart on page 1032
- bgp log-neighbor-changes on page 1033
- bgp non-deterministic-med on page 1034
- bgp recursive-bgp-next-hop on page 1034
- bgp router-id on page 1035
- bgp soft-reconfig-backup on page 1035
- capture bgp-pdu neighbor (ipv4)
- capture bgp-pdu max-buffer-size
- clear ip bgp on page 1037
- clear ip bgp dampening on page 1039
- clear ip bgp flap-statistics on page 1039
- debug ip bgp on page 1040
- debug ip bgp dampening on page 1041
- debug ip bgp events on page 1042
- debug ip bgp keepalives on page 1042
- debug ip bgp notifications on page 1043
- debug ip bgp soft-reconfiguration on page 1043
- debug ip bgp updates on page 1044
- default-metric on page 1045
- distance bgp on page 1045
- maximum-paths on page 1046
- neighbor activate on page 1047
- neighbor advertisement-interval on page 1047
- neighbor default-originate on page 1048
- neighbor description on page 1049
- neighbor distribute-list on page 1049
- neighbor ebgp-multihop on page 1050
- neighbor fall-over on page 1051
- neighbor filter-list on page 1051
- neighbor graceful-restart on page 1052
- neighbor maximum-prefix on page 1053
- neighbor next-hop-self on page 1054
- neighbor password on page 1054
- neighbor peer-group (assigning peers) on page 1055
- neighbor peer-group (creating group) on page 1057
- neighbor peer-group passive on page 1057
- neighbor remote-as on page 1058
- neighbor remove-private-as on page 1059

- neighbor route-map on page 1059
- neighbor route-reflector-client on page 1060
- neighbor send-community on page 1061
- neighbor shutdown on page 1061
- neighbor soft-reconfiguration inbound on page 1063
- neighbor timers on page 1064
- neighbor update-source on page 1065
- neighbor weight on page 1066
- network on page 1066
- network backdoor on page 1067
- redistribute on page 1068
- redistribute isis on page 1069
- router bgp on page 1071
- show capture bgp-pdu neighbor (ipv4) on page 1071
- show config on page 1072
- show ip bgp on page 1073
- show ip bgp cluster-list on page 1075
- show ip bgp community on page 1076
- show ip bgp community-list on page 1078
- show ip bgp dampened-paths on page 1079
- show ip bgp filter-list on page 1081
- show ip bgp flap-statistics on page 1082
- show ip bgp inconsistent-as on page 1084
- show ip bgp neighbors on page 1085
- show ip bgp next-hop on page 1089
- show ip bgp paths on page 1089
- show ip bgp paths as-path on page 1091
- show ip bgp paths community on page 1092
- show ip bgp peer-group on page 1093
- show ip bgp regexp on page 1095
- show ip bgp summary on page 1096

aggregate-address

C-Series	No
E-Series	✓

Summarize a range of prefixes to minimize the number of entries in the routing table.

Syntax

aggregate-address *ip-address mask* [**advertise-map** *map-name*] [**as-set**] [**attribute-map** *map-name*] [**summary-only**] [**suppress-map** *map-name*]

Parameters

ip-address mask	Enter the IP address and mask of the route to be the aggregate address. Enter the IP address in dotted decimal format (A.B.C.D) and mask in /prefix format (/x).
advertise-map *map-name*	(OPTIONAL) Enter the keywords **advertise-map** followed by the name of a configured route map to set filters for advertising an aggregate route.
as-set	(OPTIONAL) Enter the keyword **as-set** to generate path attribute information and include it in the aggregate. AS_SET includes AS_PATH and community information from the routes included in the aggregated route.
attribute-map *map-name*	(OPTIONAL) Enter the keywords **attribute-map** followed by the name of a configured route map to modify attributes of the aggregate, excluding AS_PATH and NEXT_HOP attributes.
summary-only	(OPTIONAL) Enter the keyword **summary-only** to advertise only the aggregate address. Specific routes will not be advertised.
suppress-map *map-name*	(OPTIONAL) Enter the keywords **suppress-map** followed by the name of a configured route map to identify which more-specific routes in the aggregate are suppressed.

Defaults

Not configured.

Command Modes

ADDRESS FAMILY — (conf-router_bgp_af)

Usage Information

At least one of the routes included in the aggregate address must be in the BGP routing table for the configured aggregate to become active.

Do not add the **as-set** parameter to the aggregate, if routes within the aggregate are constantly changing as the aggregate will flap to keep track of the changes in the AS_PATH.

In route maps used in the **suppress-map** parameter, routes meeting the **deny** clause are not suppress; in other words, they are allowed. The opposite is true: routes meeting the **permit** clause are suppressed.

If the route is injected via the network command, that route will still appear in the routing table if the summary-only parameter is configured in the aggregate-address command.

The summary-only parameter suppresses all advertisements. If you want to suppress advertisements to only specific neighbors, use the neighbor distribute-list command.

In the show ip bgp command, aggregates contain an ‘a’ in the first column and routes suppressed by the aggregate contain an ‘s’ in the first column.

bgp always-compare-med

C-Series	No
E-Series	✓

Allows you to enable comparison of the MULTI_EXIT_DISC (MED) attributes in the paths from different external ASs.

Syntax **bgp always-compare-med**

To disable comparison of MED, enter **no bgp always-compare-med**.

Defaults Disabled (that is, the software only compares MEDs from neighbors within the same AS).

Command Modes ROUTER BGP

Usage Information Any update without a MED attribute is the least preferred route.

If you enable this command, use the clear ip bgp * command to recompute the best path.

bgp bestpath as-path ignore

C-Series	No
E-Series	✓

Ignore the AS PATH in BGP best path calculations.

Syntax **bgp bestpath as-path ignore**

To return to the default, enter **no bgp bestpath as-path ignore**.

Defaults Disabled (that is, the software considers the AS_PATH when choosing a route as best).

Command Modes ROUTER BGP

Usage Information If you enable this command, use the clear ip bgp * command to recompute the best path.

bgp bestpath med confed

C-Series	No
E-Series	✓

Enable MULTI_EXIT_DISC (MED) attribute comparison on paths learned from BGP confederations.

Syntax **bgp bestpath med confed**

To disable MED comparison on BGP confederation paths, enter **no bgp bestpath med confed**.

Defaults Disabled

Command Modes ROUTER BGP

Usage Information The software compares the MEDs only if the path contains no external autonomous system numbers. If you enable this command, use the clear ip bgp * command to recompute the best path.

bgp bestpath med missing-as-best

C-Series	No
E-Series	✓

During path selection, indicate preference to paths with missing MED (MULTI_EXIT_DISC) over those paths with an advertised MED attribute.

Syntax **bgp bestpath med missing-as-best**

To return to the default selection, use the **no bgp bestpath med missing-as-best** command.

Defaults Disabled

Command Modes ROUTER BGP

Command History

Version 6.3.1.0	Introduced

Usage Information The MED is a 4-byte unsigned integer value and the default behavior is to assume a missing MED as 4294967295. This command causes a missing MED to be treated as 0. During the path selection, paths with a lower MED are preferred over those with a higher MED.

bgp client-to-client reflection

C-Series	No
E-Series	✓

Allows you to enable route reflection between clients in a cluster.

Syntax **bgp client-to-client reflection**

To disable client-to-client reflection, enter **no bgp client-to-client reflection**.

Defaults Enabled when a route reflector is configured.

Command Modes ROUTER BGP

Usage Information Route reflection to clients is not necessary if all client routers are fully meshed.

Related Commands

bgp cluster-id	Assign ID to a BGP cluster with two or more route reflectors.
neighbor route-reflector-client	Configure a route reflector and clients.

bgp cluster-id

C-Series	No
E-Series	✓

Assign a cluster ID to a BGP cluster with more than one route reflector.

Syntax **bgp cluster-id** {*ip-address* | *number*}

To delete a cluster ID, use the **no bgp cluster-id** {*ip-address* | *number*} command.

Parameters

ip-address	Enter an IP address as the route reflector cluster ID.
number	Enter a route reflector cluster ID as a number from 1 to 4294967295.

Defaults Not configured.

Command Modes ROUTER BGP

Usage Information When a BGP cluster contains only one route reflector, the cluster ID is the route reflector's router ID. For redundancy, a BGP cluster may contain two or more route reflectors and you assign a cluster ID with the bgp cluster-id command. Without a cluster ID, the route reflector cannot recognize route updates from the other route reflectors within the cluster.

The default format for displaying the cluster-id is dotted decimal, but if you enter the cluster-id as an integer, it will be displayed as an integer.

Related Commands

bgp client-to-client reflection	Enable route reflection between route reflector and clients.
neighbor route-reflector-client	Configure a route reflector and clients.
show ip bgp cluster-list	View paths with a cluster ID.

bgp confederation identifier

C-Series	**No**
E-Series	✓

Configure an identifier for a BGP confederation.

Syntax **bgp confederation identifier** *as-number*

To delete a BGP confederation identifier, use the **no bgp confederation identifier** *as-number* command.

Parameters

as-number	Enter the AS number. Range: 1 to 65535

Defaults Not configured.

Command Modes ROUTER BGP

Usage Information The autonomous systems configured in this command are visible to the EBGP neighbors. Each autonomous system is fully meshed and contains a few connections to other autonomous systems. The next hop, MED, and local preference information is preserved throughout the confederation.

The FTOS accepts confederation EBGP peers without a LOCAL_PREF attribute. The software sends AS_CONFED_SET and accepts AS_CONFED_SET and AS_CONF_SEQ.

bgp confederation peers

C-Series	No
E-Series	✓

Specify the Autonomous Systems (ASs) that belong to the BGP confederation.

Syntax

bgp confederation peers *as-number* [*...as-number*]

To enter no bgp confederation peer.

Parameters

as-number	Enter the AS number. Range: 1 to 65535
...as-number	(OPTIONAL) Enter up to 16 confederation numbers. Range: 1 to 65535.

Defaults

Not configured.

Command Modes

ROUTER BGP

Usage Information

The Autonomous Systems configured in this command are visible to the EBGP neighbors. Each Autonomous System is fully meshed and contains a few connections to other Autonomous Systems.

After specifying autonomous systems numbers for the BGP confederation, recycle the peers to update their configuration.

Related Commands

bgp confederation identifier	Configure a confederation ID.

bgp dampening

C-Series	No
E-Series	✓

Enable BGP route dampening and configure the dampening parameters.

Syntax

bgp dampening [*half-life reuse suppress max-suppress-time*] [**route-map** *map-name*]

To disable route dampening, use the **no bgp dampening** [*half-life reuse suppress max-suppress-time*] [**route-map** *map-name*] command.

Parameters

half-life	(OPTIONAL) Enter the number of minutes after which the Penalty is decreased. After the router assigns a Penalty of 1024 to a route, the Penalty is decreased by half after the half-life period expires. Range: 1 to 45. Default: 15 minutes
reuse	(OPTIONAL) Enter a number as the reuse value, which is compared to the flapping route's Penalty value. If the Penalty value is less than the reuse value, the flapping route is once again advertised (or no longer suppressed). Range: 1 to 20000. Default: 750
suppress	(OPTIONAL) Enter a number as the suppress value, which is compared to the flapping route's Penalty value. If the Penalty value is greater than the suppress value, the flapping route is no longer advertised (that is, it is suppressed). Range: 1 to 20000. Default: 2000
max-suppress-time	(OPTIONAL) Enter the maximum number of minutes a route can be suppressed. The default is four times the half-life value. Range: 1 to 255. Default: 60 minutes.
route-map *map-name*	(OPTIONAL) Enter the keyword **route-map** followed by the name of a configured route map. Only match commands in the configured route map are supported.

Defaults

Disabled.

Command Modes

ADDRESS FAMILY (conf-router_bgp_af)

Usage Information

If you enter **bgp dampening**, the default values for *half-life*, *reuse*, *suppress*, and *max-suppress-time* are applied. The parameters are position-dependent, therefore, if you configure one parameter, you must configure the parameters in the order they appear in the CLI.

Related Commands

show ip bgp dampened-paths	View the BGP paths

bgp default local-preference

C-Series	No
E-Series	✓

Change the default local preference value for routes exchanged between internal BGP peers.

Syntax **bgp default local-preference** *value*

To return to the default value, enter **no bgp default local-preference**.

Parameters

value	Enter a number to assign to routes as the degree of preference for those routes. When routes are compared, the higher the degree of preference or local preference value, the more the route is preferred. Range: 0 to 4294967295 Default: 100

Defaults 100

Command Modes ROUTER BGP

Usage Information The bgp default local-preference command setting is applied by all routers within the AS. To set the local preference for a specific route, use the set local-preference command in the ROUTE-MAP mode.

Related Commands

set local-preference	Configure a filter to set the BGP LOCAL_PREF attribute.

bgp enforce-first-as

C-Series	**No**
E-Series	✓

Disable (or enable) enforce-first-as check for udates received from EBGP peers.

Syntax **bgp enforce-first-as**

To turn off the default, use the **no bgp enforce-first-as** command.

Defaults Enabled

Command Modes ROUTER BGP

Command History

Version 7.4.1.0	Introduced

Usage Information This is enabled by default, that is for all updates received from EBGP peers, BGP ensures that the first AS of the first AS segment is always the AS of the peer. If not, the update is dropped and a counter is incremented. Use the show ip bgp neighbors command to view the "failed enforce-first-as check counter.

If enforce-first-as is disabled, it can be viewed via the show ip protocols command.

Related Commands

show ip bgp neighbors	View the information exchanged by BGP neighbors
show ip protocols	View Information on routing protocols.

bgp fast-external-fallover

C-Series	No
E-Series	✓

Enable the fast external fallover feature, which immediately resets the BGP session if a link to a directly connected external peer fails.

Syntax **bgp fast-external-fallover**

To disable fast external fallover, enter **no bgp fast-external-fallover**.

Defaults Enabled.

Command Modes ROUTER BGP

Usage Information The bgp fast-external-fallover command appears in the show config command output.

bgp graceful-restart

C-Series	No
E-Series	✓

Enable graceful restart on a BGP neighbor, a BGP node, or designate a local router to support graceful restart as a receiver only.

Syntax **bgp graceful-restart** [**restart-time** *seconds*] [**stale-path-time** *seconds*] [**role receiver-only**]

To return to the default, enter the **no bgp graceful-restart** command.

Parameters

restart-time *seconds*	Enter the keyword **restart-time** followed by the maximum number of seconds needed to restart and bring-up all the peers. Range: 1 to 3600 seconds Default: 120 seconds
stale-path-time *seconds*	Enter the keyword **stale-path-time** followed by the maximum number of seconds to wait before restarting a peer's stale paths. Default: 360 seconds.
role receiver-only	Enter the keyword **role receiver-only** to designate the local router to support graceful restart as a receiver only.

Defaults as above

Command Modes ROUTER-BGP

Usage Information This feature is advertised to BGP neighbors through a capability advertisement. In receiver only mode, BGP saves the advertised routes of peers that support this capability when they restart.

bgp log-neighbor-changes

C-Series	No
E-Series	✓

Enable logging of BGP neighbor resets.

Syntax **bgp log-neighbor-changes**

To disable logging, enter **no bgp log-neighbor-changes**.

Defaults Enabled.

Command Modes ROUTER BGP

Usage Information Use the show logging command in the EXEC mode to view BGP neighbor resets.

The bgp log-neighbor-changes command appears in the show config command output.

Related Commands

show logging	View logging settings and system messages logged to the system.

bgp non-deterministic-med

C-Series	No
E-Series	✓

Compare MEDs of paths from different Autonomous Systems.

Syntax **bgp non-deterministic-med**

To return to the default, enter **no bgp non-deterministic-med**.

Defaults Disabled (that is, paths/routes for the same destination but from different ASs will not have their MEDs compared).

Command Modes ROUTER BGP

Usage Information In non-deterministic mode, paths are compared in the order in which they arrive. This method can lead to FTOS choosing different best paths from a set of paths, depending on the order in which they are received from the neighbors since MED may or may not get compared between adjacent paths. In deterministic mode (**no bgp non-deterministic-med)**, FTOS compares MED between adjacent paths within an AS group since all paths in the AS group are from the same AS.

When you change the path selection from deterministic to non-deterministic, the path selection for existing paths remains deterministic until you enter clear ip bgp command to clear existing paths.

bgp recursive-bgp-next-hop

C-Series	No
E-Series	✓

Enable next-hop resolution through other routes learned by BGP.

Syntax **bgp recursive-bgp-next-hop**

To disable next-hop resolution, use the **no bgp recursive-bgp-next-hop** command.

Defaults Enabled

Command Modes ROUTER BGP

Command History

Version 7.2.10	Introduced

Usage Information

This command is a *knob* to disable BGP next-hop resolution via BGP learned routes. During the next-hop resolution, only the *first* route that the next-hop resolves through is verified for the route's protocol source and is checked if the route is learned from BGP or not.

The **clear ip bgp** command is required for this command to take effect and to keep the BGP database consistent. Execute the **clear ip bgp** command right after executing this command.

Related Commands

clear ip bgp	Description.

bgp router-id

C-Series	No
E-Series	✓

Assign a user-given ID to a BGP router.

Syntax

bgp router-id *ip-address*

To delete a user-assigned IP address, enter **no bgp router-id**.

Parameters

ip-address	Enter an IP address in dotted decimal format to reset only that BGP neighbor.

Defaults

The router ID is the highest IP address of the Loopback interface or, if no Loopback interfaces are configured, the highest IP address of a physical interface on the router.

Command Modes

ROUTER BGP

Usage Information

Peering sessions are reset when you change the router ID of a BGP router.

bgp soft-reconfig-backup

C-Series	No
E-Series	✓

Use this command *only* when route-refresh is *not* negotiated to avoid the peer from resending messages.

Syntax **bgp soft-reconfig-backup**

To return to the default setting, use the **no bgp soft-reconfig-backup** command.

Defaults Off

Command Modes ROUTER BGP

Command History

Version 7.4.1.0	Introduced

Usage Information When soft-reconfiguration is enabled for a neighbor and the **clear ip bgp soft in** is executed, the update database stored in the router is replayed and updates are reevaluated. With this command, the replay and update process is triggered only if route-refresh request is *not* negotiated with the peer. If the request is indeed negotiated (upon execution of **clear ip bgp soft in**), then BGP sends a route-refresh request to the neighbor and receives all of the peer's updates.

Note: This command is supported in BGP Router Configuration mode for IPv4 Unicast address only.

Related Commands

clear ip bgp soft in	Activate inbound policies without resetting the BGP TCP session.

capture bgp-pdu neighbor (ipv4)

C-Series	No
E-Series	✓

Enable capture of an IPv4 BGP neighbor packet.

Syntax **capture bgp-pdu neighbor** *ipv4-address* **direction** {**both** | **rx** | **tx**}

To disable capture of the IPv4 BGP neighbor packet, use the **no capture bgp-pdu neighbor** *ipv4-address* command.

Parameters

ipv4-address	Enter the IPv4 address of the target BGP neighbor.
direction {**both** | **rx** | **tx**}	Enter the keyword **direction** and a direction— either **rx** for inbound, **tx** for outbound, or **both**.

Defaults Not configured.

Command Modes EXEC; EXEC privilege

Command History

Version 7.5.1.0	Introduced

Related Commands

capture bgp-pdu max-buffer-size	Specify a size for the capture buffer.
show capture bgp-pdu neighbor (ipv4)	Display BGP packet capture information for an IPv4 address on the E-Series.
capture bgp-pdu neighbor (ipv6)	Enable capture of an IPv6 BGP neighbor packet.

capture bgp-pdu max-buffer-size

C-Series	No
E-Series	✓

Set the size of the BGP packet capture buffer. This buffer size pertains to both IPv4 and IPv6 addresses.

Syntax **capture bgp-pdu max-buffer-size** *100-102400000*

Parameters

100-102400000	Enter a size for the capture buffer.

Defaults 40960000 bytes.

Command Modes EXEC; EXEC privilege

Command History

Version 7.5.1.0	Introduced

Related Commands

capture bgp-pdu neighbor (ipv4)	Enable capture of an IPv4 BGP neighbor packet.
capture bgp-pdu neighbor (ipv6)	Enable capture of an IPv6 BGP neighbor packet.
show capture bgp-pdu neighbor (ipv4)	Display BGP packet capture information for an IPv6 address on the E-Series.

clear ip bgp

C-Series	No
E-Series	✓

Reset BGP sessions on the E-Series. The soft parameter (BGP Soft Reconfiguration) clears the policies without resetting the TCP connection.

Syntax **clear ip bgp** * | *as-number* | *ip-address* [**flap-statistics** | **soft** [**in** | **out**]]

Parameters

*	Enter an asterisk (*) to reset all BGP sessions.
as-number	Enter the AS number to reset all neighbors belonging to that AS. Range: 1 to 65535
ip-address	Enter an IP address in dotted decimal format to reset all prefixes from that neighbor.
flap-statistics	(OPTIONAL) Enter the keyword **flap-statistics** to reset the flap statistics on all prefixes from that neighbor.
soft	(OPTIONAL) Enter the keyword **soft** to configure and activate policies without resetting the BGP TCP session, that is, BGP Soft Reconfiguration. **Note:** If you enter **clear ip bgp** *ip-address* **soft**, both inbound and outbound policies are reset.
in	(OPTIONAL) Enter the keyword **in** to activate only inbound policies.
out	(OPTIONAL) Enter the keyword **out** to activate only outbound policies.

Command Modes EXEC privilege

Command History

Version 6.5.1.0	Expanded to include the *as-number* option

Related Commands

bgp recursive-bgp-next-hop	Disable next-hop resolution through other routes learned by BGP
bgp soft-reconfig-backup	Turn on BGP Soft Reconfiguration

clear ip bgp peer-group

C-Series	**No**
E-Series	✓

Reset a peer-group's BGP sessions.

Syntax **clear ip bgp peer-group** *peer-group-name*

Parameters

peer-group-name	Enter the peer group name to reset the BGP sessions within that peer group.

Command Modes EXEC privilege

clear ip bgp dampening

C-Series	No
E-Series	✓

Clear information on route dampening and return suppressed route to active state.

Syntax **clear ip bgp dampening** [*ip-address mask*]

Parameters

ip-address mask	(OPTIONAL) Enter an IP address in dotted decimal format and the prefix mask in slash format (/x) to clear dampening information only that BGP neighbor.

Command Modes EXEC privilege

Usage Information After you enter this command, the software deletes history routes and returns suppressed routes to active state.

clear ip bgp flap-statistics

C-Series	No
E-Series	✓

Clear BGP flap statistics, which includes number of flaps and the time of the last flap.

Syntax **clear ip bgp flap-statistics** [*ip-address mask* | **filter-list** *as-path-name* | **regexp** *regular-expression*]

Parameters

ip-address mask	(OPTIONAL) Enter an IP address in dotted decimal format and the prefix mask in slash format (/x) to reset only that prefix.

filter-list *as-path-name*	(OPTIONAL) Enter the keyword **filter-list** followed by the name of a configured AS-PATH list.
regexp *regular-expression*	(OPTIONAL) Enter the keyword **regexp** followed by regular expressions. Use one or a combination of the following: . (period) matches on any single character, including white space * (asterisk) matches on sequences in a pattern (zero or more sequences) + (plus sign) matches on sequences in a pattern (one or more sequences) ? (question mark) matches sequences in a pattern (0 or 1 sequences) [ ] (brackets) matches a range of single-character patterns. ^ (caret) matches the beginning of the input string. (If the caret is used at the beginning of a sequence or range, it matches on everything BUT the characters specified.) $ (dollar sign) matches the end of the output string.

Command Modes EXEC privilege

Usage Information If you enter clear ip bgp flap-statistics without any parameters, all statistics are cleared.

Related Commands

show debugging	View enabled debugging operations.
show ip bgp flap-statistics	View BGP flap statistics.
undebug all	Disable all debugging operations.

debug ip bgp

C-Series	No
E-Series	✓

Allows you to view all information on BGP, including BGP events, keepalives, notifications, and updates.

Syntax **debug ip bgp** [*ip-address* | **peer-group** *peer-group-name*] [**in** | **out**]

To disable all BGP debugging, enter **no debug ip bgp**.

Parameters

ip-address	Enter the IP address of the neighbor in dotted decimal format.
peer-group *peer-group-name*	Enter the keyword **peer-group** followed by the name of the peer group.

in	(OPTIONAL) Enter the keyword **in** to view only information on inbound BGP routes.
out	(OPTIONAL) Enter the keyword **out** to view only information on outbound BGP routes.

Command Modes EXEC privilege

Usage Information To view information on both incoming and outgoing routes, do not include the **in** and **out** parameters in the debugging command. The **in** and **out** parameters cancel each other; for example, if you enter **debug ip bgp in** and then enter **debug ip bgp out**, you will not see information on the incoming routes.

Entering a no debug ip bgp command removes all configured debug commands for BGP.

Related Commands

debug ip bgp events	View information about BGP events.
debug ip bgp keepalives	View information about BGP keepalives.
debug ip bgp notifications	View information about BGP notifications.
debug ip bgp updates	View information about BGP updates.
show debugging	View enabled debugging operations.

debug ip bgp dampening

C-Series	No
E-Series	✓

View information on routes being dampened.

Syntax **debug ip bgp dampening** [**in** | **out**]

To disable debugging, enter **no debug ip bgp dampening**.

Parameters

in	(OPTIONAL) Enter the keyword **in** to view only inbound dampened routes.
out	(OPTIONAL) Enter the keyword **out** to view only outbound dampened routes.

Command Modes EXEC privilege

Usage Information Enter no debug ip bgp command to remove all configured debug commands for BGP.

Related Commands

show debugging	View enabled debugging operations.
show ip bgp dampened-paths	View BGP dampened routes.

debug ip bgp events

C-Series	No
E-Series	✓

Allows you to view information on local BGP state changes and other BGP events.

Syntax **debug ip bgp** [*ip-address* | **peer-group** *peer-group-name*] **events** [**in** | **out**]

To disable debugging, use the **no debug ip bgp** [*ip-address* | **peer-group** *peer-group-name*] **events** command.

Parameters

ip-address	(OPTIONAL) Enter the IP address of the neighbor in dotted decimal format.
peer-group *peer-group-name*	(OPTIONAL) Enter the keyword **peer-group** followed by the name of the peer group.
in	(OPTIONAL) Enter the keyword **in** to view only events on inbound BGP messages.
out	(OPTIONAL) Enter the keyword **out** to view only events on outbound BGP messages.

Command Modes EXEC privilege

Usage Information Enter no debug ip bgp command to remove all configured debug commands for BGP.

debug ip bgp keepalives

C-Series	No
E-Series	✓

Allows you to view information about BGP keepalive messages.

Syntax **debug ip bgp** [*ip-address* | **peer-group** *peer-group-name*] **keepalives** [**in** | **out**]

To disable debugging, use the **no debug ip bgp** [*ip-address* | **peer-group** *peer-group-name*] **keepalives** [**in** | **out**] command.

Parameters

ip-address	(OPTIONAL) Enter the IP address of the neighbor in dotted decimal format.
peer-group *peer-group-name*	(OPTIONAL) Enter the keyword **peer-group** followed by the name of the peer group.

in	(OPTIONAL) Enter the keyword **in** to view only inbound keepalive messages.
out	(OPTIONAL) Enter the keyword **out** to view only outbound keepalive messages.

Command Modes EXEC privilege

Usage Information Enter no debug ip bgp command to remove all configured debug commands for BGP.

debug ip bgp notifications

C-Series	No
E-Series	✓

Allows you to view information about BGP notifications received from neighbors.

Syntax **debug ip bgp** [*ip-address* | **peer-group** *peer-group-name*] **notifications** [**in** | **out**]

To disable debugging, use the **no debug ip bgp** [*ip-address* | **peer-group** *peer-group-name*] **notifications** [**in** | **out**] command.

Parameters

ip-address	(OPTIONAL) Enter the IP address of the neighbor in dotted decimal format.
peer-group *peer-group-name*	(OPTIONAL) Enter the keyword **peer-group** followed by the name of the peer group.
in	(OPTIONAL) Enter the keyword **in** to view BGP notifications received from neighbors.
out	(OPTIONAL) Enter the keyword **out** to view BGP notifications sent to neighbors.

Command Modes EXEC privilege

Usage Information Enter no debug ip bgp command to remove all configured debug commands for BGP.

debug ip bgp soft-reconfiguration

Enable soft-reconfiguration debug.

Syntax **debug ip bgp** {*ip-address* | *peer-group-name*} **soft-reconfiguration**

C-Series	No
E-Series	✓

To disable, use the **no debug ip bgp** {*ip-address* | *peer-group-name*} **soft-reconfiguration** command.

Parameters

ip-address	(OPTIONAL) Enter the IP address of the neighbor in dotted decimal format.
peer-group-name	(OPTIONAL) Enter the name of the peer group to disable or enable all routers within the peer group.

Defaults Disabled

Command Modes EXEC

Command History

Version 7.4.1.0	Introduced

Usage Information This command turns on BGP soft-reconfiguration inbound debugging. If no neighbor is specified, debug is turned on for all neighbors.

debug ip bgp updates

C-Series	No
E-Series	✓

Allows you to view information about BGP updates.

Syntax **debug ip bgp updates** [**in** | **out** | **prefix-list** *prefix-list-name*]

To disable debugging, use the **no debug ip bgp** [*ip-address* | **peer-group** *peer-group-name*] **updates** [**in** | **out**] command.

Parameters

in	(OPTIONAL) Enter the keyword **in** to view only BGP updates received from neighbors.
out	(OPTIONAL) Enter the keyword **out** to view only BGP updates sent to neighbors.
prefix-list *prefix-list-name*	(OPTIONAL) Enter the keyword **prefix-list** followed by the name of an established prefix list. If the prefix list is not configured, the default is *permit* (to allow all routes).

Command Modes EXEC privilege

Usage Information Enter no debug ip bgp command to remove all configured debug commands for BGP.

default-metric

C-Series	No
E-Series	✓

Allows you to change the metrics of redistributed routes to locally originated routes. Use this command with the redistribute command.

Syntax **default-metric** *number*

To return to the default setting, enter **no default-metric**.

Parameters

number	Enter a number as the metric to be assigned to routes from other protocols. Range: 1 to 4294967295.

Defaults 0

Command Modes ROUTER BGP

Usage Information The default-metric command in BGP sets the value of the BGP MULTI_EXIT_DISC (MED) attribute for redistributed routes only.

Related Commands

bgp always-compare-med	Enable comparison of all BGP MED attributes.
redistribute	Redistribute routes from other routing protocols into BGP.

distance bgp

C-Series	No
E-Series	✓

Configure three administrative distances for routes.

Syntax **distance bgp** *external-distance internal-distance local-distance*

To return to default values, enter **no distance bgp**.

Parameters

external-distance	Enter a number to assign to routes learned from a neighbor external to the AS. Range: 1 to 255. Default: 20
internal-distance	Enter a number to assign to routes learned from a router within the AS. Range: 1 to 255. Default: 200
local-distance	Enter a number to assign to routes learned from networks listed in the network command. Range: 1 to 255. Default: 200

Defaults *external-distance* = 20; *internal-distance* = 200; *local-distance* = 200.

Command Modes ROUTER BGP

Caution: Force10 Networks recommends that you do not change the administrative distance of internal routes. Changing the administrative distances may cause routing table inconsistencies.

Usage Information The higher the administrative distance assigned to a route means that your confidence in that route is low. Routes assigned an administrative distance of 255 are not installed in the routing table. Routes from confederations are treated as internal BGP routes.

maximum-paths

C-Series	**No**
E-Series	✓

Configure the maximum number of parallel routes (multipath support) BGP supports.

Syntax **maximum-paths** {**ebgp** | **ibgp**} *number*

To return to the default values, enter **no maximum-paths**.

Parameters

ebgp	Enter the keyword **ebgp** to enable multipath support for External BGP routes.
ibgp	Enter the keyword **ibgp** to enable multipath support for Internal BGP routes.
number	Enter a number as the maximum number of parallel paths. Range: 1 to 16 Default: 1

Defaults 1

Command Modes ROUTER BGP

Usage Information If you enable this command, use the clear ip bgp * command to recompute the best path.

neighbor activate

C-Series	No
E-Series	✓

This command allows the specified neighbor/peer group to be enabled for the current AFI/SAFI.

Syntax **neighbor** [*ip-address* | *peer-group-name*] **activate**

To disable, use the **no neighbor** [*ip-address* | *peer-group-name*] **activate** command.

Parameters

ip-address	(OPTIONAL) Enter the IP address of the neighbor in dotted decimal format.
peer-group-name	(OPTIONAL) Enter the name of the peer group
activate	Enter the keyword **activate** to enable the neighbor/peer group in the new AFI/SAFI.

Defaults Disabled

Command Modes ROUTER BGP

Usage Information By default, when a neighbor/peer group configuration is created in the Router BGP context, it is enabled for the IPv4/Unicast AFI/SAFI. By using **activate** in the new context, the neighbor/peer group is enabled for AFI/SAFI.

neighbor advertisement-interval

C-Series	No
E-Series	✓

Set the advertisement interval between BGP neighbors or within a BGP peer group.

Syntax **neighbor** {*ip-address* | *peer-group-name*} **advertisement-interval** *seconds*

To return to the default value, use the **no neighbor** {*ip-address* | *peer-group-name*} **advertisement-interval** command.

Parameters

ip-address	Enter the IP address of the neighbor in dotted decimal format.
peer-group-name	Enter the name of the peer group to set the advertisement interval for all routers in the peer group.
seconds	Enter a number as the time interval, in seconds, between BGP advertisements. Range: 0 to 600 seconds. Default: 5 seconds for internal BGP peers; 30 seconds for external BGP peers.

Defaults *seconds* = 5 seconds (internal peers); *seconds* = 30 seconds (external peers)

Command Modes ROUTER BGP

neighbor default-originate

C-Series	No
E-Series	✓

Inject the default route to a BGP peer or neighbor.

Syntax **neighbor** {*ip-address* | *peer-group-name*} **default-originate** [**route-map** *map-name*]

To remove a default route, use the **no neighbor** {*ip-address* | *peer-group-name*} **default-originate** command.

Parameters

ip-address	Enter the IP address of the neighbor in dotted decimal format.
peer-group-name	Enter the name of the peer group to set the default route of all routers in that peer group.
route-map *map-name*	(OPTIONAL) Enter the keyword **route-map** followed by the name of a configured route map.

Defaults Not configured.

Command Modes ROUTER BGP

Usage Information If you apply a route map to a BGP peer or neighbor with the neighbor default-originate command configured, the software does not apply the set filters in the route map to that BGP peer or neighbor.

neighbor description

C-Series	No
E-Series	✓

Assign a character string describing the neighbor or group of neighbors (peer group).

Syntax **neighbor** {*ip-address* | *peer-group-name*} **description** *text*

To delete a description, use the **no neighbor** {*ip-address* | *peer-group-name*} **description** command.

Parameters

ip-address	Enter the IP address of the neighbor in dotted decimal format.
peer-group-name	Enter the name of the peer group.
text	Enter a continuous text string up to 80 characters.

Defaults Not configured.

Command Modes ROUTER BGP

neighbor distribute-list

C-Series	No
E-Series	✓

Distribute BGP information via an established prefix list.

Syntax **neighbor** {*ip-address* | *peer-group-name*} **distribute-list** *prefix-list-name* {**in** | **out**}

To delete a neighbor distribution list, use the **no neighbor** {*ip-address* | *peer-group-name*} **distribute-list** *prefix-list-name* {**in** | **out**} command.

Parameters

ip-address	Enter the IP address of the neighbor in dotted decimal format.
peer-group-name	Enter the name of the peer group to apply the distribute list filter to all routers in the peer group.
prefix-list-name	Enter the name of an established prefix list. If the prefix list is not configured, the default is permit (to allow all routes).
in	Enter the keyword **in** to distribute only inbound traffic.
out	Enter the keyword **out** to distribute only outbound traffic.

Defaults Not configured.

Command Modes ROUTER BGP

Usage Information Other BGP filtering commands include: neighbor filter-list, ip as-path access-list, and neighbor route-map.

Related Commands

ip as-path access-list	Configure IP AS-Path ACL.
neighbor filter-list	Assign a AS-PATH list to a neighbor or peer group.
neighbor route-map	Assign a route map to a neighbor or peer group.

neighbor ebgp-multihop

C-Series	**No**
E-Series	✓

Attempt and accept BGP connections to external peers on networks that are not directly connected.

Syntax **neighbor** {*ip-address* | *peer-group-name*} **ebgp-multihop** [*ttl*]

To disallow and disconnect connections, use the **no neighbor** {*ip-address* | *peer-group-name*} **ebgp-multihop** command.

Parameters

ip-address	Enter the IP address of the neighbor in dotted decimal format.
peer-group-name	Enter the name of the peer group.
ttl	(OPTIONAL) Enter the number of hops as the Time to Live (ttl) value. Range: 1 to 255. Default: 255

Defaults Disabled.

Command Modes ROUTER BGP

Usage Information To prevent loops, the neighbor ebgp-multihop command will not install default routes of the multihop peer. Networks not directly connected are not considered valid for best path selection.

neighbor fall-over

C-Series	No
E-Series	✓

Enable or disable fast fall-over for BGP neighbors.

Syntax **neighbor** {*ipv4-address* | *peer-group-name*} **fall-over**

To disable, use the **no neighbor** {*ipv4-address* | *peer-group-name*} **fall-over** command.

Parameters

ipv4-address	Enter the IP address of the neighbor in dotted decimal format.
peer-group-name	Enter the name of the peer group.

Defaults Disabled

Command Modes ROUTER BGP (conf-router)

Command History

Version 7.4.1.0	Introduced

Usage Information When fall-over is enabled, BGP keeps track of IP or IPv6 reachability to the peer remote address and the peer local address. Whenever either address becomes unreachable (i.e, no active route exists in the routing table for peer IP or IPv6 destination/local address), BGP brings down the session with the peer.

Related Commands

show ip bgp neighbors	Display information on the BGP neighbors

neighbor filter-list

C-Series	No
E-Series	✓

Configure a BGP filter based on the AS-PATH attribute.

Syntax **neighbor** {*ip-address* | *peer-group-name*} **filter-list** *as-path-name* {**in** | **out**}

To delete a BGP filter, use the **no neighbor** {*ip-address* | *peer-group-name*} **filter-list** *as-path-name* {**in** | **out**} command.

Parameters

ip-address	Enter the IP address of the neighbor in dotted decimal format.
peer-group-name	Enter the name of the peer group to apply the filter to all routers in the peer group.
as-path-name	Enter the name of an established AS-PATH access list. If the AS-PATH access list is not configured, the default is permit (to allow routes).
in	Enter the keyword **in** to filter inbound BGP routes.
out	Enter the keyword **out** to filter outbound BGP routes.

Defaults Not configured.

Command Modes ROUTER BGP

Usage Information Use the ip as-path access-list command syntax in the CONFIGURATION mode to enter the AS-PATH ACL mode and configure AS-PATH filters to deny or permit BGP routes based on information in their AS-PATH attribute.

Related Commands

ip as-path access-list	Enter AS-PATH ACL mode and configure AS-PATH filters.

neighbor graceful-restart

C-Series	**No**
E-Series	✓

Enable graceful restart on a BGP neighbor.

Syntax **neighbor** {*ip-address* | *peer-group-name*} **graceful-restart** [**restart-time** *seconds*] [**stale-path-time** *seconds*] [**role receiver-only**]

To return to the default, enter the **no bgp graceful-restart** command.

Parameters

ip-address	Enter the IP address of the neighbor in dotted decimal format.
peer-group-name	Enter the name of the peer group to apply the filter to all routers in the peer group.
restart-time *seconds*	Enter the keyword **restart-time** followed by the maximum number of seconds needed to restart and bring-up all the peers. Range: 1 to 3600 seconds Default: 120 seconds
stale-path-time *seconds*	Enter the keyword **stale-path-time** followed by the maximum number of seconds to wait before restarting a peer's stale paths. Default: 360 seconds.
role receiver-only	Enter the keyword **role receiver-only** to designate the local router to support graceful restart as a receiver only.

Defaults as above

Command Modes ROUTER-BGP

Usage Information This feature is advertised to BGP neighbors through a capability advertisement. In receiver only mode, BGP saves the advertised routes of peers that support this capability when they restart.

neighbor maximum-prefix

C-Series	No
E-Series	✓

Control the number of network prefixes received.

Syntax **neighbor** {*ip-address* | *peer-group-name*} **maximum-prefix** *maximum* [*threshold*] [**warning-only**]

To return to the default values, use the **no neighbor** {*ip-address* | *peer-group-name*} **maximum-prefix** *maximum* command.

Parameters

ip-address	Enter the IP address of the neighbor in dotted decimal format.
peer-group-name	Enter the name of the peer group.
maximum	Enter a number as the maximum number of prefixes allowed for this BGP router. Range: 1 to 4294967295.
threshold	(OPTIONAL) Enter a number to be used as a percentage of the *maximum* value. When the number of prefixes reaches this percentage of the *maximum* value, the E-Series software sends a message. Range: 1 to 100 percent. Default: 75
warning-only	(OPTIONAL) Enter the keyword **warning-only** to set the router to send a log message when the maximum value is reached. If this parameter is not set, the router stops peering when the maximum number of prefixes is reached.

Defaults *threshold* = 75

Command Modes ROUTER BGP

Usage Information If the neighbor maximum-prefix is configured and the neighbor receives more prefixes than allowed by the neighbor maximum-prefix command configuration, the neighbor goes down and the show ip bgp summary command displays `(prfxd)` in the State/PfxRcd column for that neighbor. The neighbor remains down until you enter the clear ip bgp command for the neighbor or the peer group to which the neighbor belongs or you enter neighbor shutdown and neighbor no shutdown commands.

Related Commands		
	show ip bgp summary	Displays the current BGP configuration.

neighbor next-hop-self

C-Series	No
E-Series	✓

Allows you to configure the router as the next hop for a BGP neighbor. (This command is used for IBGP).

Syntax **neighbor** {*ip-address* | *peer-group-name*} **next-hop-self**

To return to the default setting, use the **no neighbor** {*ip-address* | *peer-group-name*} **next-hop-self** command.

Parameters		
	ip-address	Enter the IP address of the neighbor in dotted decimal format.
	peer-group-name	Enter the name of the peer group.

Defaults Disabled.

Command Modes ROUTER BGP

Usage Information If the set next-hop command in the ROUTE-MAP mode is configured, its configuration takes precedence over the neighbor next-hop-self command.

neighbor password

C-Series	No
E-Series	✓

Enable Message Digest 5 (MD5) authentication on the TCP connection between two neighbors.

Syntax **neighbor** {*ip-address* | *peer-group-name*} **password** [*encryption-type*] *password*

To delete a password, use the **no neighbor** {*ip-address* | *peer-group-name*} **password** command.

Parameters

ip-address	Enter the IP address of the router to be included in the peer group.
peer-group-name	Enter the name of a configured peer group.
encryption-type	(OPTIONAL) Enter 7 as the encryption type for the *password* entered. 7 means that the password is encrypted and hidden.
password	Enter a text string up to 80 characters long. The first character of the *password* must be a letter. You cannot use spaces in the password.

Defaults

Not configured.

Command Modes

ROUTER BGP

Usage Information

Configure the same password on both BGP peers or a connection does not occur. When you configure MD5 authentication between two BGP peers, each segment of the TCP connection between them is verified and the MD5 digest is checked on every segment sent on the TCP connection.

Configuring a password for a neighbor will cause an existing session to be torn down and a new one established.

If you specify a BGP peer group by using the *peer-group-name* parameter, all the members of the peer group will inherit the characteristic configured with this command.

If you configure a password on one neighbor, but you have not configured a password for the neighboring router, the following message appears on the console while the routers attempt to establish a BGP session between them:

```
%RPM0-P:RP1 %KERN-6-INT: No BGP MD5 from [peer's IP address]
:179 to  [local router's IP address]:65524
```

Also, if you configure different passwords on the two routers, the following message appears on the console:

```
%RPM0-P:RP1 %KERN-6-INT: BGP MD5 password mismatch from
[peer's IP address] : 11502 to [local router's IP address] :179
```

neighbor peer-group (assigning peers)

C-Series	**No**
E-Series	✓

Allows you to assign one peer to a existing peer group.

Syntax

neighbor *ip-address* **peer-group** *peer-group-name*

To delete a peer from a peer group, use the **no neighbor** *ip-address* **peer-group** *peer-group-name* command.

Parameters

ip-address	Enter the IP address of the router to be included in the peer group.
peer-group-name	Enter the name of a configured peer group.

Defaults

Not configured.

Command Modes

ROUTER BGP

Usage Information

You can assign up to 64 peers to one peer group.

When you add a peer to a peer group, it inherits all the peer group's configured parameters. A peer cannot become part of a peer group if any of the following commands are configured on the peer:

- neighbor advertisement-interval
- neighbor distribute-list out
- neighbor filter-list out
- neighbor next-hop-self
- neighbor route-map out
- neighbor route-reflector-client
- neighbor send-community

A neighbor may keep its configuration after it was added to a peer group if the neighbor's configuration is more specific than the peer group's, and the neighbor's configuration does not affect outgoing updates.

A peer group must exist before you add a peer to it. If the peer group is disabled (shutdown) the peers within the group are also disabled (shutdown).

Related Commands

clear ip bgp	Resets BGP sessions.
neighbor peer-group (creating group)	Create a peer group.
show ip bgp peer-group	View BGP peers.
show ip bgp neighbors	View BGP neighbors configurations.

neighbor peer-group (creating group)

C-Series	No
E-Series	✓

Allows you to create a peer group and assign it a name.

Syntax **neighbor** *peer-group-name* **peer-group**

To delete a peer group, use the **no neighbor** *peer-group-name* **peer-group** command.

Parameters

peer-group-name	Enter a text string up to 16 characters long as the name of the peer group.

Defaults Not configured.

Command Modes ROUTER BGP

Usage Information When a peer group is created, it is disabled (shut mode).

Related Commands

neighbor peer-group (assigning peers)	Assign routers to a peer group.
neighbor remote-as	Assign a indirectly connected AS to a neighbor or peer group.
neighbor shutdown	Disable a peer or peer group.

neighbor peer-group passive

C-Series	No
E-Series	✓

Enable passive peering on a BGP peer group, that is, the peer group does not send an OPEN message, but will respond to one.

Syntax **neighbor** *peer-group-name* **peer-group passive**

To delete a passive peer-group, use the **no neighbor** *peer-group-name* **peer-group passive** command.

Parameters

peer-group-name	Enter a text string up to 16 characters long as the name of the peer group.

Defaults Not configured.

Command Modes ROUTER BGP

Usage Information After you configure a peer group as passive, you must assign it a subnet using the neighbor soft-reconfiguration inbound command.

Related Commands

neighbor soft-reconfiguration inbound	Assign a subnet to a dynamically-configured BGP neighbor.

neighbor remote-as

C-Series	**No**
E-Series	✓

Create and specify the remote peer to the BGP neighbor.

Syntax **neighbor** {*ip-address* | *peer-group-name*} **remote-as** *number*

To delete a remote AS entry, use the **no neighbor** {*ip-address* | *peer-group-name*} **remote-as** *number* command.

Parameters

ip-address	Enter the IP address of the neighbor to enter the remote AS in its routing table.
peer-group-name	Enter the name of the peer group to enter the remote AS into routing tables of all routers within the peer group.
number	Enter a number of the AS. Range: 1 to 65535.

Defaults Not configured.

Command Modes ROUTER BGP

Usage Information If the *number* parameter is the same as the AS number used in the router bgp command, the remote AS entry in the neighbor is considered an internal BGP peer entry.

This command creates a peer and the newly created peer is disabled (shutdown).

Related Commands

router bgp	Enter the ROUTER BGP mode and configure routes in an AS.

neighbor remove-private-as

C-Series	No
E-Series	✓

Remove private AS numbers from the AS-PATH of outgoing updates.

Syntax **neighbor** {*ip-address* | *peer-group-name*} **remove-private-as**

To return to the default, use the **no neighbor** {*ip-address* | *peer-group-name*} **remove-private-as** command.

Parameters

ip-address	Enter the IP address of the neighbor to remove the private AS numbers.
peer-group-name	Enter the name of the peer group to remove the private AS numbers

Defaults Disabled (that is, private AS number are not removed).

Command Modes ROUTER BGP

Usage Information Applies to EBGP neighbors only.

If the AS-PATH contains both public and private AS number or contains AS numbers of an EBGP neighbor, the private AS numbers are not removed.

If a confederation contains private AS numbers in its AS-PATH, the software removes the private AS numbers only if they follow the confederation numbers in the AS path.

Private AS numbers are 64512 to 65535.

neighbor route-map

C-Series	No
E-Series	✓

Apply an established route map to either incoming or outbound routes of a BGP neighbor or peer group.

Syntax **neighbor** {*ip-address* | *peer-group-name*} **route-map** *map-name* {**in** | **out**}

To remove the route map, use the **no neighbor** {*ip-address* | *peer-group-name*} **route-map** *map-name* {**in** | **out**} command.

Parameters

ip-address	Enter the IP address of the neighbor in dotted decimal format.
peer-group-name	Enter the name of the peer group.
map-name	Enter the name of an established route map. If the Route map is not configured, the default is deny (to drop all routes).
in	Enter the keyword **in** to filter inbound routes.
out	Enter the keyword **out** to filter outbound routes.

Defaults Not configured.

Command Modes ROUTER BGP

Usage Information When you apply a route map to outbound routes, only routes that match at least one section of the route map are permitted.

If you identify a peer group by name, the peers in that peer group inherit the characteristics in the Route map used in this command. If you identify a peer by IP address, the Route map overwrites either the inbound or outbound policies on that peer.

neighbor route-reflector-client

C-Series	No
E-Series	✓

Configure a neighbor as a member of a route reflector cluster.

Syntax **neighbor** {*ip-address* | *peer-group-name*} **route-reflector-client**

To indicate that the neighbor is not a route reflector client or to delete a route reflector configuration, use the **no neighbor** {*ip-address* | *peer-group-name*} **route-reflector-client** command.

Parameters

ip-address	Enter the IP address of the neighbor in dotted decimal format.
peer-group-name	Enter the name of the peer group. All routers in the peer group receive routes from a route reflector.

Defaults Not configured.

Command Modes ROUTER BGP

Usage Information The first time you enter this command it configures the neighbor as a route reflector and members of the route-reflector cluster. Internal BGP (IBGP) speakers do not need to be fully meshed if you configure a route reflector.

When all clients of a route reflector are disabled, the neighbor is no longer a route reflector.

neighbor send-community

C-Series	No
E-Series	✓

Send a COMMUNITY attribute to a BGP neighbor or peer group. A COMMUNITY attribute indicates that all routes with that attribute belong to the same community grouping.

Syntax **neighbor** {*ip-address* | *peer-group-name*} **send-community**

To disable sending a COMMUNITY attribute, use the **no neighbor** {*ip-address* | *peer-group-name*} **send-community** command.

Parameters

ip-address	Enter the IP address of the peer router in dotted decimal format.
peer-group-name	Enter the name of the peer group to send a COMMUNITY attribute to all routers within the peer group.

Defaults Not configured and COMMUNITY attributes are not sent to neighbors.

Command Modes ROUTER BGP

Usage Information To configure a COMMUNITY attribute, use the set community command in the ROUTE-MAP mode.

neighbor shutdown

C-Series	No
E-Series	✓

Disable a BGP neighbor or peer group.

Syntax **neighbor** {*ip-address* | *peer-group-name*} **shutdown**

To enable a disabled neighbor or peer group, use the **neighbor** {*ip-address* | *peer-group-name*} **no shutdown** command.

Parameters

ip-address	Enter the IP address of the neighbor in dotted decimal format.
peer-group-name	Enter the name of the peer group to disable or enable all routers within the peer group.

Defaults

Enabled (that is, BGP neighbors and peer groups are disabled.)

Command Modes

ROUTER BGP

Usage Information

Peers that are enabled within a peer group are disabled when their peer group is disabled.

The neighbor shutdown command terminates all BGP sessions on the BGP neighbor or BGP peer group. Use this command with caution as it terminates the specified BGP sessions. When a neighbor or peer group is shutdown, use the show ip bgp summary command to confirm its status.

Related Commands

show ip bgp summary	Displays the current BGP configuration.
show ip bgp neighbors	Displays the current BGP neighbors.

neighbor soft-reconfiguration inbound

C-Series	No
E-Series	✓

Enable soft-reconfiguration for BGP.

Syntax

neighbor {*ip-address* | *peer-group-name*} **soft-reconfiguration inbound**

To disable, use the **no neighbor** {*ip-address* | *peer-group-name*} **soft-reconfiguration inbound** command.

Parameters

ip-address	Enter the IP address of the neighbor in dotted decimal format.
peer-group-name	Enter the name of the peer group to disable or enable all routers within the peer group.

Defaults

Disabled

Command Modes

ROUTER BGP

Command History

Version 7.2.10	Introduced

Usage Information

This command enables soft-reconfiguration for the BGP neighbor specified. BGP will store all the updates received by the neighbor but will not reset the peer-session.

Caution: Inbound update storage is a memory-intensive operation. The entire BGP update database from the neighbor is stored in memory *regardless* of the inbound policy results applied on the neighbor.

Note: This command is supported in BGP Router Configuration mode for IPv4 Unicast address only.

Related Commands

show ip bgp neighbors	Display routes received by a neighbor

neighbor subnet

C-Series	No
E-Series	✓

Enable passive peering so that the members of the peer group are dynamic

Syntax **neighbor** *peer-group-name* **subnet** *subnet-number mask*

To remove passive peering, use the **no neighbor** *peer-group-name* **subnet** *subnet-number mask* command.

Parameters

subnet-number	Enter a subnet number in dotted decimal format (A.B.C.D.) as the allowable range of addresses included in the Peer group. To allow all addresses, enter 0.0.0.0/0.
mask	Enter a prefix mask in / prefix-length format (/x).

Defaults Not configured.

Command Modes ROUTER BGP

neighbor timers

C-Series	**No**
E-Series	✓

Set keepalive and hold time timers for a BGP neighbor or a peer group.

Syntax **neighbor** {*ip-address* | *peer-group-name*} **timers** *keepalive holdtime*

To return to the default values, use the **no neighbor** {*ip-address* | *peer-group-name*} **timers** command.

Parameters

ip-address	Enter the IP address of the peer router in dotted decimal format.
peer-group-name	Enter the name of the peer group to set the timers for all routers within the peer group.
keepalive	Enter a number for the time interval, in seconds, between keepalive messages sent to the neighbor routers. Range: 1 to 65535 Default: 60 seconds
holdtime	Enter a number for the time interval, in seconds, between the last keepalive message and declaring the router dead. Range: 3 to 65535 Default: 180 seconds

Defaults *keepalive* = 60 seconds; *holdtime* = 180 seconds.

Command Modes ROUTER BGP

Usage Information Timer values configured with the neighbor timers command override the timer values configured with the any other command.

When two neighbors, configured with different *keepalive* and *holdtime* values, negotiate for new values, the resulting values will be as follows:

- the lower of the *holdtime* values is the new *holdtime* value, and
- whichever is the lower value; one-third of the new *holdtime* value, or the configured *keepalive* value is the new *keepalive* value.

neighbor update-source

C-Series	No
E-Series	✓

Enable the E-Series software to use Loopback interfaces for TCP connections for BGP sessions.

Syntax **neighbor** {*ip-address* | *peer-group-name*} **update-source** *interface*

To use the closest interface, use the **no neighbor** {*ip-address* | *peer-group-name*} **update-source** *interface* command.

Parameters

ip-address	Enter the IP address of the peer router in dotted decimal format.
peer-group-name	Enter the name of the peer group to disable all routers within the peer group.
interface	Enter the keyword **loopback** followed by a number of the loopback interface. Range: 0 to 16383.

Defaults Not configured.

Command Modes ROUTER BGP

Usage Information Loopback interfaces are up constantly and the BGP session may need one interface constantly up to stabilize the session. The neighbor update-source command is not necessary for directly connected internal BGP sessions.

neighbor weight

C-Series	No
E-Series	✓

Assign a weight to the neighbor connection, which is used to determine the best path.

Syntax

neighbor {*ip-address* | *peer-group-name*} **weight** *weight*

To remove a weight value, use the **no neighbor** {*ip-address* | *peer-group-name*} **weight** command.

Parameters

ip-address	Enter the IP address of the peer router in dotted decimal format.
peer-group-name	Enter the name of the peer group to disable all routers within the peer group.
weight	Enter a number as the weight. Range: 0 to 65535 Default: 0

Defaults

0

Command Modes

ROUTER BGP

Usage Information

In the FTOS best path selection process, the path with the highest weight value is preferred.

Note: Reset the neighbor connection (clear ip bgp * command) to apply the weight to the connection and recompute the best path.

If the set weight command is configured in a route map applied to this neighbor, the weight set in that command overrides the weight set in the neighbor weight command.

Related Commands

set weight	Assign a weight to all paths meeting the route map criteria.

network

C-Series	No
E-Series	✓

Specify the networks for the BGP process and enter them in the BGP routing table.

Syntax **network** *ip-address mask* [**route-map** *map-name*]

To remove a network, use the **no network** *ip-address mask* [**route-map** *map-name*] command.

Parameters

ip-address	Enter an IP address in dotted decimal format of the network.
mask	Enter the mask of the IP address in the slash prefix length format (for example, /24). The mask appears in command outputs in dotted decimal format (A.B.C.D).
route-map *map-name*	(OPTIONAL) Enter the keyword **route-map** followed by the name of an established route map. Only the following ROUTE-MAP mode commands are supported: • match ip address • set community • set local-preference • set metric • set next-hop • set origin • set weight If the route map is not configured, the default is deny (to drop all routes).

Defaults Not configured.

Command Modes ROUTER BGP

Usage Information The E-Series software resolves the network address configured by the network command with the routes in the main routing table to ensure that the networks are reachable via non-BGP routes and non-default routes.

Related Commands

redistribute	Redistribute routes into BGP.

network backdoor

C-Series	**No**
E-Series	✓

Specify this IGP route as the preferred route.

Syntax **network** *ip-address mask* **backdoor**

To remove a network, use the **no network** *ip-address mask* **backdoor** command.

Parameters

ip-address	Enter an IP address in dotted decimal format of the network.
mask	Enter the mask of the IP address in the slash prefix length format (for example, /24). The mask appears in command outputs in dotted decimal format (A.B.C.D).

Defaults Not configured.

Command Modes ROUTER BGP

Usage Information Though FTOS does not generate a route due to backdoor config, there is an option for injecting/sourcing a local route in presence of network backdoor config on a learned route.

redistribute

C-Series	**No**
E-Series	✓

Redistribute routes into BGP.

Syntax **redistribute** {**connected** | **static**} [**route-map** *map-name*]

To disable redistribution, use the **no redistribution** {**connected** | **static**} command.

Parameters

connected	Enter the keyword **connected** to redistribute routes from physically connected interfaces.
static	Enter the keyword **static** to redistribute manually configured routes. These routes are treated as incomplete routes.
route-map *map-name*	(OPTIONAL) Enter the keyword **route-map** followed by the name of an established route map. Only the following ROUTE-MAP mode commands are supported: • match ip address • set community • set local-preference • set metric • set next-hop • set origin • set weight If the route map is not configured, the default is deny (to drop all routes).

Defaults Not configured.

Command Modes ROUTER BGP

Usage Information

If you do not configure default-metric command, in addition to the redistribute command, or there is no route map to set the metric, the metric for redistributed static and connected is "0".

To redistribute the default route (0.0.0.0/0) configure the neighbor default-originate command.

Related Commands

neighbor default-originate	Inject the default route.

redistribute isis

C-Series	No
E-Series	✓

Redistribute IS-IS routes into BGP.

Syntax

redistribute isis [*WORD*][**level-1**| **level-1-2** | **level-2**] [**metric** *metric-value*] [**route-map** *map-name*]

To return to the default values, enter the **no redistribute isis** [*WORD*][**level-1**| **level-1-2** | **level-2**] [**metric** *metric-value*] [**route-map** *map-name*] command.

Parameters

WORD	ISO routing area tag
level-1	(OPTIONAL) Enter the keyword **level-1** to independently redistributed into Level 1 routes only.
level-1-2	(OPTIONAL) Enter the keyword **level-1-2** to independently redistributed into Level 1 and Level 2 routes. This is the default.
level-2	(OPTIONAL) Enter the keyword **level-2** to independently redistributed into Level 2 routes only
metric *metric-value*	(OPTIONAL) Enter the keyword **metric** followed by the metric value used for the redistributed route. Use a metric value that is consistent with the destination protocol. Range: 0 to 16777215 Default: 0
route-map *map-name*	Enter the keyword **route-map** followed by the map name that is an identifier for a configured route map. The route map should filter imported routes from the source routing protocol to the current routing protocol. If you do not specify a *map-name,* all routes are redistributed. If you specify a keyword, but fail to list route map tags, no routes will be imported.

Defaults

level-1-2

Command Modes

ROUTER BGP

Command History

Version 6.3.1.0	Introduced

Example

```
Force10(conf)#router bgp 1
Force10(conf-router_bgp)#redistribute isis level-1 metric 44 route-map rmap-is2bgp
Force10(conf-router_bgp)#show running-config bgp
!
router bgp 1
redistribute isis level-1 metric 44 route-map rmap-is2bgp
```

Figure 334 redistribute isis Command Example

Usage Information

IS-IS to BGP redistribution supports matching of **level-1** or **level-2** routes or all routes (default). More advanced match options can be performed using route maps. The metric value of redistributed routes can be set by the redistribution command.

redistribute ospf

C-Series	**No**
E-Series	✓

Redistribute OSPF routes into BGP.

Syntax

redistribute ospf *process-id* [[**match external** {**1** | **2**}] [**match internal**]] [**route-map** *map-name*]

To stop redistribution of OSPF routes, use the **no redistribute ospf** *process-id* command.

Parameters

process-id	Enter the number of the OSPF process. Range: 1 to 65535
match external {**1** | **2**}	(OPTIONAL) Enter the keywords match external to redistribute OSPF external routes. You can specify 1 or 2 to redistribute those routes only.
match internal	(OPTIONAL) Enter the keywords **match internal** to redistribute OSPF internal routes only.
route-map *map-name*	(OPTIONAL) Enter the keywords **route-map** followed by the name of a configured Route map.

Defaults

Not configured.

Command Modes

ROUTER BGP

Usage Information

When you enter redistribute isis *process-id* command without any other parameters, FTOS redistributes all OSPF internal routes, external type 1 routes, and external type 2 routes. This feature is not supported by an RFC.

router bgp

C-Series	No
E-Series	✓

Enter ROUTER BGP mode to configure and enable BGP.

Syntax

router bgp *as-number*

To disable BGP, use the **no router bgp** *as-number* command.

Parameters

as-number	Enter the AS number. Range: 1 to 65535.

Defaults

Not enabled.

Command Modes

CONFIGURATION

Example

```
Force10(conf)#router bgp 3
Force10(conf-router_bgp)#
```

Figure 335 router bgp Command Example

show capture bgp-pdu neighbor (ipv4)

C-Series	No
E-Series	✓

Display BGP packet capture information for an IPv4 address on the E-Series.

Syntax

show capture bgp-pdu neighbor *ipv4-address*

Parameters

ipv4-address	Enter the IPv4 address (in dotted decimal format) of the BGP address to display packet information for that address.

Command Modes

EXEC

EXEC privilege

Command History

Version 7.5.1.0	Introduced

Example

```
Force10(conf-router_bgp)#show capture bgp-pdu neighbor 20.20.20.2

Incoming packet capture enabled for BGP neighbor 20.20.20.2
Available buffer size 40958758, 26 packet(s) captured using 680 bytes
  PDU[1] : len 101, captured 00:34:51 ago
    ffffffff ffffffff ffffffff ffffffff 00650100 00000013 00000000
00000000 419ef06c 00000000
    00000000 00000000 00000000 00000000 0181a1e4 0181a25c 41af92c0
00000000 00000000 00000000
    00000000 00000001 0181a1e4 0181a25c 41af9400 00000000
  PDU[2] : len 19, captured 00:34:51 ago
    ffffffff ffffffff ffffffff ffffffff 00130400
  PDU[3] : len 19, captured 00:34:51 ago
    ffffffff ffffffff ffffffff ffffffff 00130400
 [. . .]

Outgoing packet capture enabled for BGP neighbor 20.20.20.2
Available buffer size 40958758, 27 packet(s) captured using 562 bytes
  PDU[1] : len 41, captured 00:34:52 ago
    ffffffff ffffffff ffffffff ffffffff 00290104 000100b4 14141401
0c020a01 04000100 01020080
    00000000
  PDU[2] : len 19, captured 00:34:51 ago
    ffffffff ffffffff ffffffff ffffffff 00130400
  PDU[3] : len 19, captured 00:34:50 ago
    ffffffff ffffffff ffffffff ffffffff 00130400
 [. . .]
Force10#
```

Figure 336 show capture bgp-pdu neighbor Command Example

Related Commands

capture bgp-pdu neighbor (ipv4)	Enable capture of an IPv4 BGP neighbor packet.
capture bgp-pdu max-buffer-size	Specify a size for the capture buffer.
show capture bgp-pdu neighbor (ipv6)	Display BGP packet capture information for an IPv6 address on the E-Series.

show config

C-Series	**No**
E-Series	✓

View the current ROUTER BGP configuration.

Syntax **show config**

Command Modes ROUTER BGP

Example

```
Force10(conf-router_bgp)#show confi
!
router bgp 45
 neighbor suzanne peer-group
 neighbor suzanne no shutdown
 neighbor sara peer-group
 neighbor sara shutdown
 neighbor 13.14.15.20 peer-group suzanne
 neighbor 13.14.15.20 shutdown
 neighbor 123.34.55.123 peer-group suzanne
 neighbor 123.34.55.123 shutdown
Force10(conf-router_bgp)#
```

Figure 337 show config Command Example

show ip bgp

C-Series	No
E-Series	✓

View the current BGP routing table for the E-Series.

Syntax **show ip bgp** [*network* [*network-mask*] [**longer-prefixes**]]

Parameters

network	(OPTIONAL) Enter the network address (in dotted decimal format) of the BGP network to view information only on that network.
network-mask	(OPTIONAL) Enter the network mask (in slash prefix format) of the BGP network address.
longer-prefixes	(OPTIONAL) Enter the keyword **longer-prefixes** to view all routes with a common prefix.

Command Modes EXEC

EXEC privilege

Usage Information When you enable **bgp non-deterministic-med** command, the **show ip bgp** command output for a BGP route does not list the INACTIVE reason.

Example

```
Force10>show ip bgp
BGP table version is 847562, local router ID is 63.114.8.131
Status codes: s suppressed, d damped, h history, * valid, > best
Path source: I - internal, a - aggregate, c - confed-external, r - redistributed, n - network
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network             Next Hop            Metric        LocPrf    Weight  Path
*>  0.0.0.0/0           63.114.8.33                                      0  18508 i
*   3.0.0.0/8           63.114.8.33                                      0  18508 209 701 80 i
*>                      63.114.8.33                                      0  18508 701 80 i
*>  3.3.0.0/16          0.0.0.0                22                   32768  ?
                        63.114.8.35                                      0  18508 ?
*>  4.0.0.0/8           63.114.8.33                                      0  18508 701 1 i
*>  4.2.49.12/30        63.114.8.33                                      0  18508 209 i
*   4.17.250.0/24       63.114.8.33                                      0  18508 209 1239 13716 i
*>                      63.114.8.33                                      0  18508 701 1239 13716 i
*   4.21.132.0/23       63.114.8.33                                      0  18508 209 6461 16422 i
*>                      63.114.8.33                                      0  18508 701 6461 16422 i
*>  4.24.118.16/30      63.114.8.33                                      0  18508 209 i
*>  4.24.145.0/30       63.114.8.33                                      0  18508 209 i
*>  4.24.187.12/30      63.114.8.33                                      0  18508 209 i
*>  4.24.202.0/30       63.114.8.33                                      0  18508 209 i
*>  4.25.88.0/30        63.114.8.33                                      0  18508 209 3561 3908 i
*>  5.0.0.0/9           63.114.8.33             0                        0  18508 ?
*>  5.0.0.0/10          63.114.8.33             0                        0  18508 ?
*>  5.0.0.0/11          63.114.8.33             0                        0  18508 ?
--More--
```

Figure 338 show ip bgp Command Example (Partial)

Table 88 defines the information displayed in Figure 338

Table 88 show ip bgp Command Example Fields

Field	Description
Network	Displays the destination network prefix of each BGP route.
Next Hop	Displays the next hop address of the BGP router. If 0.0.0.0 is listed in this column, then local routes exist in the routing table.
Metric	Displays the BGP route's metric, if assigned.
LocPrf	Displays the BGP LOCAL_PREF attribute for the route.
Weight	Displays the route's weight
Path	Lists all the ASs the route passed through to reach the destination network.

Related Commands

show ip bgp community	View BGP communities.
neighbor maximum-prefix	Control number of network prefixes received.

show ip bgp cluster-list

C-Series	No
E-Series	✓

View BGP neighbors in a specific cluster.

Syntax **show ip bgp cluster-list** [*cluster-id*]

Parameters

cluster-id	(OPTIONAL) Enter the cluster id in dotted decimal format.

Command Modes EXEC

EXEC privilege

Example

```
Force10#show ip bgp cluster-list
BGP table version is 64444683, local router ID is 120.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best
Path source: I - internal, a - aggregate, c - confed-external, r - redistributed, n
- network
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network            Next Hop            Metric     LocPrf Weight Path
* I 10.10.10.1/32      192.68.16.1              0        100      0 i
* I                    192.68.16.1              0        100      0 i
*>I                    192.68.16.1              0        100      0 i
* I                    192.68.16.1              0        100      0 i
* I                    192.68.16.1              0        100      0 i
* I                    192.68.16.1              0        100      0 i
* I 10.19.75.5/32      192.68.16.1              0        100      0 ?
* I                    192.68.16.1              0        100      0 ?
*>I                    192.68.16.1              0        100      0 ?
* I                    192.68.16.1              0        100      0 ?
* I                    192.68.16.1              0        100      0 ?
* I                    192.68.16.1              0        100      0 ?
* I 10.30.1.0/24       192.68.16.1              0        100      0 ?
* I                    192.68.16.1              0        100      0 ?
*>I                    192.68.16.1              0        100      0 ?
* I                    192.68.16.1              0        100      0 ?
* I                    192.68.16.1              0        100      0 ?
* I                    192.68.16.1              0        100      0 ?
```

Figure 339 show ip bgp cluster-list Command Example (Partial)

Table 89 defines the information displayed in Figure 339.

Table 89 show ip bgp cluster-list Command Fields

Field	Description
Network	Displays the destination network prefix of each BGP route.
Next Hop	Displays the next hop address of the BGP router. If 0.0.0.0 is listed in this column, then local routes exist in the routing table.
Metric	Displays the BGP route's metric, if assigned.
LocPrf	Displays the BGP LOCAL_PREF attribute for the route.

Table 89 show ip bgp cluster-list Command Fields (continued)

Field	Description
Weight	Displays the route's weight
Path	Lists all the ASs the route passed through to reach the destination network.

show ip bgp community

C-Series	No
E-Series	✓

View information on all routes with Community attributes or view specific BGP community groups.

Syntax **show ip bgp community** [*community-number*] [**local-as**] [**no-export**] [**no-advertise**]

Parameters

community-number	Enter the community number in AA:NN format where AA is the AS number (2 bytes) and NN is a value specific to that autonomous system. You can specify up to eight community numbers to view information on those community groups.
local-AS	Enter the keywords **local-AS** to view all routes with the COMMUNITY attribute of NO_EXPORT_SUBCONFED. All routes with the NO_EXPORT_SUBCONFED (0xFFFFFF03) community attribute must not be advertised to external BGP peers.
no-advertise	Enter the keywords **no-advertise** to view all routes containing the well-known community attribute of NO_ADVERTISE. All routes with the NO_ADVERTISE (0xFFFFFF02) community attribute must not be advertised to other BGP peers.
no-export	Enter the keywords **no-export** to view all routes containing the well-known community attribute of NO_EXPORT. All routes with the NO_EXPORT (0xFFFFFF01) community attribute must not be advertised outside a BGP confederation boundary.

Command Modes EXEC

EXEC privilege

Usage Information To view the total number of COMMUNITY attributes found, use the show ip bgp summary command. The text line above the route table states the number of COMMUNITY attributes found.

Example

```
Force10>show ip bgp community
BGP table version is 3762622, local router ID is 63.114.8.48
Status codes: s suppressed, d damped, h history, * valid, > best
Path source: I - internal, a - aggregate, c - confed-external, r - redistributed, n - network
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric        LocPrf    Weight  Path
* i 3.0.0.0/8        205.171.0.16                        100         0  209 701 80 i
*>i 4.2.49.12/30     205.171.0.16                        100         0  209 i
* i 4.21.132.0/23    205.171.0.16                        100         0  209 6461 16422 i
*>i 4.24.118.16/30   205.171.0.16                        100         0  209 i
*>i 4.24.145.0/30    205.171.0.16                        100         0  209 i
*>i 4.24.187.12/30   205.171.0.16                        100         0  209 i
*>i 4.24.202.0/30    205.171.0.16                        100         0  209 i
*>i 4.25.88.0/30     205.171.0.16                        100         0  209 3561 3908 i
*>i 6.1.0.0/16       205.171.0.16                        100         0  209 7170 1455 i
*>i 6.2.0.0/22       205.171.0.16                        100         0  209 7170 1455 i
*>i 6.3.0.0/18       205.171.0.16                        100         0  209 7170 1455 i
*>i 6.4.0.0/16       205.171.0.16                        100         0  209 7170 1455 i
*>i 6.5.0.0/19       205.171.0.16                        100         0  209 7170 1455 i
*>i 6.8.0.0/20       205.171.0.16                        100         0  209 7170 1455 i
*>i 6.9.0.0/20       205.171.0.16                        100         0  209 7170 1455 i
*>i 6.10.0.0/15      205.171.0.16                        100         0  209 7170 1455 i
*>i 6.14.0.0/15      205.171.0.16                        100         0  209 7170 1455 i
*>i 6.133.0.0/21     205.171.0.16                        100         0  209 7170 1455 i
*>i 6.151.0.0/16     205.171.0.16                        100         0  209 7170 1455 i
--More--
```

Figure 340 show ip bgp community Command Example (Partial)

The show ip bgp community command without any parameters lists BGP routes with at least one BGP community attribute and the output is the same as for the show ip bgp command output.

Table 90 show ip bgp community Command Example Fields

Field	Description
Network	Displays the destination network prefix of each BGP route.
Next Hop	Displays the next hop address of the BGP router. If 0.0.0.0 is listed in this column, then local routes exist in the routing table.
Metric	Displays the BGP route's metric, if assigned.
LocPrf	Displays the BGP LOCAL_PREF attribute for the route.
Weight	Displays the route's weight
Path	Lists all the ASs the route passed through to reach the destination network.

show ip bgp community-list

C-Series	No
E-Series	✓

View routes that are affected by a specific community list.

Syntax **show ip bgp community-list** *community-list-name* [**exact-match**]

Parameters

community-list-name	Enter the name of a configured IP community list. (max 16 chars)
exact-match	Enter the keyword for an exact match of the communities.

Command Modes EXEC

EXEC privilege

Example

```
Force10#show ip bgp community-list pass
BGP table version is 0, local router ID is 10.101.15.13
Status codes: s suppressed, d damped, h history, * valid, > best
Path source: I - internal, a - aggregate, c - confed-external, r - redistributed, n - network
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network             Next Hop            Metric        LocPrf    Weight  Path
Force10#
```

Figure 341 show ip bgp community-list Command Example

The show ip bgp community-list command without any parameters lists BGP routes matching the Community List and the output is the same as for the show ip bgp command output.

Table 91 show ip bgp community-list Command Example Fields

Field	Description
Network	Displays the destination network prefix of each BGP route.
Next Hop	Displays the next hop address of the BGP router. If 0.0.0.0 is listed in this column, then local routes exist in the routing table.
Metric	Displays the BGP route's metric, if assigned.
LocPrf	Displays the BGP LOCAL_PREF attribute for the route.
Weight	Displays the route's weight
Path	Lists all the ASs the route passed through to reach the destination network.

show ip bgp dampened-paths

C-Series	No
E-Series	✓

View BGP routes that are dampened (non-active).

Syntax **show ip bgp dampened-paths**

Command Modes EXEC

EXEC privilege

Example

```
Force10>show ip bgp damp
BGP table version is 210708, local router ID is 63.114.8.2
Status codes: s suppressed, d damped, h history, * valid, > best
Path source: I - internal, a - aggregate, c - confed-external, r - redistributed, n - network
Origin codes: i - IGP, e - EGP, ? - incomplete
    Network            From            Reuse     Path
Force10>
```

Figure 342 show ip bgp dampened-paths Command Example

Table 92 defines the information displayed in Figure 342.

Table 92 show ip bgp dampened-paths Command Example

Field	Description
Network	Displays the network ID to which the route is dampened.
From	Displays the IP address of the neighbor advertising the dampened route.
Reuse	Displays the hour:minutes:seconds until the dampened route is available.
Path	Lists all the ASs the dampened route passed through to reach the destination network.

show ip bgp detail

C-Series	No
E-Series	✓

Display BGP internal information for IPv4 Unicast address family.

Syntax **show ip bgp detail**

Defaults Defaults.

Command Modes EXEC

EXEC privilege

Command History

Version 7.5.1.0	Introduced

Example

```
R2#show ip bgp detail

Detail information for BGP Node
bgpNdP 0x41a17000 : NdTmrP 0x41a17000 : NdKATmrP 0x41a17014 : NdTics 74857 :
NhLocAS 1 : NdState 2 : NdRPMPrim 1 : NdListSoc 13
NdAuto 1 : NdEqCost 1 : NdSync 0 : NdDefOrg 0
NdV6ListSoc 14 NdDefDid 0 : NdConfedId 0 : NdMedConfed 0 : NdMedMissVal -1 :
NdIgnrIllId 0 : NdRRC2C 1 : NdClstId 33686273 : NdPaTblP 0x41a19088
NdASPTblP 0x41a19090 : NdCommTblP 0x41a19098 : NhOptTransTblP 0x41a190a0 :
NdRRClsTblP 0x41a190a8
NdPktPA 0 : NdLocCBP 0x41a6f000 : NdTmpPAP 0x419efc80 : NdTmpASPAP 0x41a25000 :
NdTmpCommP 0x41a25800
NdTmpRRClP 0x41a4b000 : NdTmpOptP 0x41a4b800 : NdTmpNHP  : NdOrigPAP 0
NdOrgNHP 0 : NdModPathP 0x419efcc0 : NdModASPAP 0x41a4c000 : NdModCommP 0x41a4c800
NdModOptP 0x41a4d000 : NdModNHP  : NdComSortBufP 0x41a19110 : NdComSortHdP
0x41a19d04 : NdUpdAFMsk 0 : AFRstSet 0x41a1a298 : NHopDfrdHdP 0x41a1a3e0 :

NumNhDfrd 0 : CfgHdrAFMsk 1
AFChkNetTmrP 0x41ee705c :  AFRtDamp 0 : AlwysCmpMed 0 : LocrHld 10 : LocrRem 10 :
softReconfig 0x41a1a58c
DefMet 0 : AutoSumm 1 : NhopsP 0x41a0d100 : Starts 0 : Stops 0 : Opens 0
Closes 0 : Fails 0 : Fatals 0 : ConnExps 0 : HldExps 0 : KeepExps 0
RxOpens 0 : RxKeeps 0 : RxUpds 0 : RxNotifs 0 : TxUpds 0 : TxNotifs 0
BadEvts 0 : SynFails 0 : RxeCodeP 0x41a1b6b8 : RxHdrCodeP 0x41a1b6d4 : RxOpCodeP
0x41a1b6e4
RxUpdCodeP 0x41a1b704 : TxEcodeP 0x41a1b734 : TxHdrcodeP 0x41a1b750 : TxOpCodeP
0x41a1b760
TxUpdCodeP 0x41a1b780 : TrEvt 0 : LocPref 100 : tmpPathP 0x41a1b7b8 : LogNbrChgs 1
RecursiveNH 1 : PgCfgId 0 : KeepAlive 0 : HldTime 0 : DioHdl 0 : AggrValTmrP
0x41ee7024
UpdNetTmrP 0 : RedistTmrP 0x41ee7094 : PeerChgTmrP 0 : CleanRibTmrP 0x41ee7104
PeerUpdTmrP 0x41ee70cc : DfrdNHTmrP 0x41ee7174 : DfrdRtselTmrP 0x41ee713c :
FastExtFallover 1 : FastIntFallover 0 : Enforce1stAS 1
PeerIdBitsP 0x41967120 : softOutSz 16 : RibUpdCtxCBP 0
UpdPeerCtxCBP 0 : UpdPeerCtxAFI 0 : TcpioCtxCB 0 : RedistBlk 1
NextCBPurg 1101119536 : NumPeerToPurge 0 : PeerIBGPCnt 0 : NonDet 0 : DfrdPathSel 0
BGPRst 0 : NumGrCfg 1 : DfrdTmestmp 0 : SnmpTrps 0 : IgnrBestPthASP 0
RstOn 1 : RstMod 1 : RstRole 2 : AFFalgs 7 : RstInt 120 : MaxeorExtInt 361
FixedPartCrt 1 : VarParCrt 1
Packet Capture max allowed length 40960000 : current length 0

Peer Grp List
Nbr List
Confed Peer List
Address Family specific Information
AFIndex 0
NdSpFlag 0x41a190b0 : AFRttP 0x41a0d200 : NdRTMMkrP 0x41a19d28 : NdRTMAFTblVer 0 :
NdRibCtxAddr 1101110688
NdRibCtxAddrLen 255 : NdAFPrefix 0 : NdAfNLRIP 0 : NdAFNLRILen 0 : NdAFWPtrP 0
NdAFWLen 0 : NdAfNH  : NdAFRedRttP 0x41a0d400 : NdRecCtxAdd 1101110868
NdRedCtxAddrLen 255 : NdAfRedMkrP 0x41a19e88 : AFAggRttP 0x41a0d600 : AfAggCtxAddr
1101111028 : AfAggrCtxAddrLen 255
AfNumAggrPfx 0 : AfNumAggrASSet 0 : AfNumSuppmap 0 : AfNumAggrValidPfx 0 :
AfMPathRttP 0x41a0d700
MpathCtxAddr 1101111140 : MpathCtxAddrlen 255 : AfEorSet 0x41a19f98 : NumDfrdPfx 0
AfActPeerHd 0x41a1a3a4 : AfExtDist 1101112312 : AfIntDist 200 : AfLocDist 200
AfNumRRc 0 : AfRR 0 : AfNetRttP 0x41a0d300 : AfNetCtxAddr 1101112392 :
AfNetCtxAddrlen 255
AfNwCtxAddr 1101112443 : AfNwCtxAddrlen 255 : AfNetBKDrRttP 0x41a0d500 :
AfNetBKDRCnt 0 : AfDampHLife 0
AfDampReuse 0 : AfDampSupp 0 : AfDampMaxHld 0 : AfDampCeiling 0 : AfDampRmapP
```

show ip bgp filter-list

C-Series	No
E-Series	✓

View the routes that match the filter lists.

Syntax **show ip bgp filter-list** *as-path-name*

Parameters

as-path-name	Enter the name of an AS-PATH.

Command Modes EXEC

EXEC privilege

Example

```
Force10#show ip bgp filter-list hello
BGP table version is 80227, local router ID is 120.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best
Path source: I - internal, a - aggregate, c - confed-external, r - redistributed, n -
network
Origin codes: i - IGP, e - EGP, ? - incomplete

     Network            Next Hop            Metric     LocPrf Weight Path
* I 6.1.5.0/24         192.100.11.2         20000        9999      0 ?
* I                    192.100.8.2          20000        9999      0 ?
* I                    192.100.9.2          20000        9999      0 ?
* I                    192.100.10.2         20000        9999      0 ?
*>I                    6.1.5.1              20000        9999      0 ?
* I                    6.1.6.1              20000        9999      0 ?
* I                    6.1.20.1             20000        9999      0 ?
* I 6.1.6.0/24         192.100.11.2         20000        9999      0 ?
* I                    192.100.8.2          20000        9999      0 ?
* I                    192.100.9.2          20000        9999      0 ?
* I                    192.100.10.2         20000        9999      0 ?
*>I                    6.1.5.1              20000        9999      0 ?
* I                    6.1.6.1              20000        9999      0 ?
* I                    6.1.20.1             20000        9999      0 ?
* I 6.1.20.0/24        192.100.11.2         20000        9999      0 ?
* I                    192.100.8.2          20000        9999      0 ?
* I                    192.100.9.2          20000        9999      0 ?
* I                    192.100.10.2         20000        9999      0 ?
Force10#
```

Figure 343 show ip bgp filter-list Command Example

Table 93 defines the information displayed in Figure 343.

Table 93 show ip bgp filter-list Command Fields

Field	Description
Path source codes	Lists the path sources shown to the right of the last AS number in the Path column: • i = internal route entry • a = aggregate route entry • c = external confederation route entry • n = network route entry • r = redistributed route entry
Next Hop	Displays the next hop address of the BGP router. If 0.0.0.0 is listed in this column, then local routes exist in the routing table.
Metric	Displays the BGP route's metric, if assigned.
LocPrf	Displays the BGP LOCAL_PREF attribute for the route.
Weight	Displays the route's weight
Path	Lists all the ASs the route passed through to reach the destination network.

show ip bgp flap-statistics

C-Series	No
E-Series	✓

View flap statistics on BGP routes.

Syntax **show ip bgp flap-statistics** [*ip-address* [*mask*]] [**filter-list** *as-path-name*] [**regexp** *regular-expression*]

Parameters

ip-address	(OPTIONAL) Enter the IP address (in dotted decimal format) of the BGP network to view information only on that network.
mask	(OPTIONAL) Enter the network mask (in slash prefix (/x) format) of the BGP network address.

filter-list *as-path-name*	(OPTIONAL) Enter the keyword **filter-list** followed by the name of a configured AS-PATH ACL.
regexp *regular-expression*	Enter a regular expression then use one or a combination of the following characters to match: • **.** = (period) any single character (including a white space) • ***** = (asterisk) the sequences in a pattern (0 or more sequences) • **+** = (plus) the sequences in a pattern (1 or more sequences) • **?** = (question mark) sequences in a pattern (either 0 or 1 sequences). **You must enter an escape sequence (CTRL+v) prior to entering the ? regular expression.** • **[ ]** = (brackets) a range of single-character patterns. • **^** = (caret) the beginning of the input string. If the caret is used at the beginning of a sequence or range, it matches on everything BUT the characters specified. • **$** = (dollar sign) the end of the output string.

Command Modes

EXEC

EXEC privilege

Example

```
Force10>show ip bgp flap
BGP table version is 210851, local router ID is 63.114.8.2
Status codes: s suppressed, d damped, h history, * valid, > best
Path source: I - internal, a - aggregate, c - confed-external, r - redistributed, n - network
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network             From            Flaps Duration Reuse     Path
Force10>
```

Figure 344 show ip bgp flap-statistics Command Example

Table 94 defines the information displayed in Figure 344.

Table 94 show ip bgp flap-statistics Command Example Fields

Field	Description
Network	Displays the network ID to which the route is flapping.
From	Displays the IP address of the neighbor advertising the flapping route.
Flaps	Displays the number of times the route flapped.
Duration	Displays the hours:minutes:seconds since the route first flapped.
Reuse	Displays the hours:minutes:seconds until the flapped route is available.
Path	Lists all the ASs the flapping route passed through to reach the destination network.

show ip bgp inconsistent-as

C-Series	No
E-Series	✓

View routes with inconsistent originating Autonomous System (AS) numbers, that is, prefixes that are announced from the same neighbor AS but with a different AS-Path.

Syntax **show ip bgp inconsistent-as**

Command Modes EXEC

EXEC privilege

Example

```
Force10>show ip bgp inconsistent-as
BGP table version is 280852, local router ID is 10.1.2.100
Status codes: s suppressed, d damped, h history, * valid, > best
Path source: I - internal, c - confed-external, r - redistributed, n - network
Origin codes: i - IGP, e - EGP, ? - incomplete

     Network          Next Hop            Metric     LocPrf Weight Path
*    3.0.0.0/8        63.114.8.33                           0 18508 209 7018 80  i
*                     63.114.8.34                           0 18508 209 7018 80  i
*                     63.114.8.60                           0 18508 209 7018 80  i
*>                     63.114.8.33                              0 18508 701 80  i
*>   3.18.135.0/24     63.114.8.60                           0 18508 209 7018  ?
*                     63.114.8.34                           0 18508 209 7018  ?
*                     63.114.8.33                           0 18508 701 7018  ?
*                     63.114.8.33                           0 18508 209 7018  ?
*>   4.0.0.0/8         63.114.8.60                            0 18508 209 1  i
*                     63.114.8.34                            0 18508 209 1  i
*                     63.114.8.33                            0 18508 701 1  i
*                     63.114.8.33                            0 18508 209 1  i
*    6.0.0.0/20        63.114.8.60                           0 18508 209 3549  i
*                     63.114.8.34                           0 18508 209 3549  i
*>                     63.114.8.33              0             0 18508  ?
*                     63.114.8.33                           0 18508 209 3549  i
*    9.2.0.0/16        63.114.8.60                            0 18508 209 701  i
*                     63.114.8.34                            0 18508 209 701  i
--More--
```

Figure 345 show ip bgp inconsistent-as Command Example (Partial)

Table 95 defines the information displayed in Figure 345.

Table 95 show ip bgp inconsistent-as Command Example Fields

Fields	Description
Network	Displays the destination network prefix of each BGP route.
Next Hop	Displays the next hop address of the BGP router. If 0.0.0.0 is listed in this column, then local routes exist in the routing table.
Metric	Displays the BGP route's metric, if assigned.
LocPrf	Displays the BGP LOCAL_PREF attribute for the route.

Table 95 show ip bgp inconsistent-as Command Example Fields

Fields	Description
Weight	Displays the route's weight
Path	Lists all the ASs the route passed through to reach the destination network.

show ip bgp neighbors

C-Series	**No**
E-Series	✓

Allows you to view the information exchanged by BGP neighbors.

Syntax

show ip bgp neighbors [*ip-address* [**advertised-routes** | **dampened-routes** | **detail** | **flap-statistics** | **routes** | {**received-routes** [*network* [*network-mask*]]} | {**denied-routes** [*network* [*network-mask*]]}]

Parameters

ip-address	(OPTIONAL) Enter the IP address of the neighbor to view only BGP information exchanged with that neighbor.
advertised-routes	(OPTIONAL) Enter the keywords **advertised-routes** to view only the routes the neighbor sent.
dampened-routes	(OPTIONAL) Enter the keyword **dampened-routes** to view information on dampened routes from the BGP neighbor.
detail	(OPTIONAL) Enter the keyword **detail** to view neighbor-specific internal information for the IPv4 Unicast address family.
flap-statistics	(OPTIONAL) Enter the keyword **flap-statistics** to view flap statistics on the neighbor's routes.
routes	(OPTIONAL) Enter the keywords **routes** to view only the neighbor's feasible routes.
received-routes [*network* [*network-mask*]	(OPTIONAL) Enter the keywords **received-routes** followed by either the network address (in dotted decimal format) or the network mask (in slash prefix format) to view all information received from neighbors. **Note**: neighbor soft-reconfiguration inbound must be configured prior to viewing all the information received from the neighbors.
denied-routes [*network* [*network-mask*]	(OPTIONAL) Enter the keywords **denied-routes** followed by either the network address (in dotted decimal format) or the network mask (in slash prefix format) to view all information on routes denied via neighbor inbound filters.

Command Modes

EXEC

EXEC privilege

Command History

Version 7.5.1.0	Added **detail** option and output now displays default MED value
Version 7.4.1.0	Added received and denied route options
Version 6.3.10	The output is changed to display the total number of advertised prefixes

Example 1

```
Force10#show ip bgp neighbors

BGP neighbor is 100.10.10.2, remote AS 200, external link
  BGP version 4, remote router ID 192.168.2.101
  BGP state ESTABLISHED, in this state for 00:16:12
  Last read 00:00:12, last write 00:00:03
  Hold time is 180, keepalive interval is 60 seconds
Received 1404 messages, 0 in queue
    3 opens, 1 notifications, 1394 updates
    6 keepalives, 0 route refresh requests
  Sent 48 messages, 0 in queue
    3 opens, 2 notifications, 0 updates
    43 keepalives, 0 route refresh requests
Minimum time between advertisement runs is 30 seconds
  Minimum time before advertisements start is 0 seconds

  Capabilities received from neighbor for IPv4 Unicast :
    MULTIPROTO_EXT(1)
    ROUTE_REFRESH(2)
    CISCO_ROUTE_REFRESH(128)

  Capabilities advertised to neighbor for IPv4 Unicast :
    MULTIPROTO_EXT(1)
    ROUTE_REFRESH(2)
    ROUTE_REFRESH(2)
    GRACEFUL_RESTART(64)
    CISCO_ROUTE_REFRESH(128)

  Route map for incoming advertisements is test
  Maximum prefix set to 4 with threshold 75

  For address family: IPv4 Unicast
  BGP table version 34, neighbor version 34
  5 accepted prefixes consume 20 bytes
  Prefix advertised 0, denied 4, withdrawn 0

Prefixes accepted 1 (consume 4 bytes), withdrawn 0 by peer
  Prefixes advertised 0, rejected 0, withdrawn 0 from peer

  Connections established 2; dropped 1
  Last reset 00:18:21, due to Maximum prefix limit reached
```

Figure 346 show ip bgp neighbors Command Example (Partial)

Table 96 defines the information displayed in Figure 346

Example 2

```
Force10>show ip bgp neighbors 192.14.1.5 advertised-routes

BGP table version is 74103, local router ID is 33.33.33.33
Status codes: s suppressed, S stale, d damped, h history, * valid, > best
Path source: I - internal, a - aggregate, c - confed-external, r - redistributed,
n - network
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network            Next Hop            Metric     LocPrf Weight Path
*>r 1.10.1.0/24        0.0.0.0               5000             32768 ?
*>r 1.11.0.0/16        0.0.0.0               5000             32768 ?
.....
.....
*>I 223.94.249.0/24    223.100.4.249            0        100      0 ?
*>I 223.94.250.0/24    223.100.4.250            0        100      0 ?
*>I 223.100.0.0/16     223.100.255.254          0        100      0 ?
Total number of prefixes: 74102
```

Figure 347 show ip bgp neighbors advertised-routes Command Example

Example 3

```
Force10#show ip bgp neighbors 100.10.10.2 received-routes
BGP table version is 13, local router ID is 120.10.10.1
Status codes: s suppressed, S stale, d damped, h history, * valid, > best
Path source: I - internal, a - aggregate, c - confed-external, r - redistributed
n - network, D - denied, S - stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network            Next Hop            Metric     LocPrf Weight Path
D   70.70.21.0/24      100.10.10.2                         0      0 100 200 ?
D   70.70.22.0/24      100.10.10.2                         0      0 100 200 ?
D   70.70.23.0/24      100.10.10.2                         0      0 100 200 ?
D   70.70.24.0/24      100.10.10.2                         0      0 100 200 ?
*>  70.70.25.0/24      100.10.10.2                         0      0 100 200 ?
*>  70.70.26.0/24      100.10.10.2              0          0      0 100 200 ?
*>  70.70.27.0/24      100.10.10.2              0          0      0 100 200 ?
*>  70.70.28.0/24      100.10.10.2              0          0      0 100 200 ?
*>  70.70.29.0/24      100.10.10.2              0          0      0 100 200 ?
Force10#
```

Figure 348 show ip bgp neighbors received-routes Command Example

Example 4

```
Force10#show ip bgp  neighbors  100.10.10.2 denied-routes
4 denied paths using 205 bytes of memory
BGP table version is 34, local router ID is 100.10.10.2
Status codes: s suppressed, S stale, d damped, h history, * valid, > best
Path source: I - internal, a - aggregate, c - confed-external, r - redistributed
             n - network,  D - denied,  S - stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network            Next Hop            Metric     LocPrf Weight Path
D   70.70.21.0/24      100.10.10.2                         0      0 100 200 ?
D   70.70.22.0/24      100.10.10.2                         0      0 100 200 ?
D   70.70.23.0/24      100.10.10.2                         0      0 100 200 ?
D   70.70.24.0/24      100.10.10.2                         0      0 100 200 ?
Force10#
```

Figure 349 show ip bgp neighbors denied-routes Command Example

Table 96 show ip bgp neighbors Command Fields

Lines beginning with	Description
BGP neighbor	Displays the BGP neighbor address and its AS number. The last phrase in the line indicates whether the link between the BGP router and its neighbor is an external or internal one. If they are located in the same AS, then the link is internal; otherwise the link is external.
BGP version	Displays the BGP version (always version 4) and the remote router ID.
BGP state	Displays the neighbor's BGP state and the amount of time in hours:minutes:seconds it has been in that state.
Last read	This line displays the following information: • last read is the time (hours:minutes:seconds) the router read a message from its neighbor • hold time is the number of seconds configured between messages from its neighbor • keepalive interval is the number of seconds between keepalive messages to help ensure that the TCP session is still alive.

Table 96 show ip bgp neighbors Command Fields (continued)

Lines beginning with	Description
Received messages	This line displays the number of BGP messages received, the number of notifications (error messages) and the number of messages waiting in a queue for processing.
Sent messages	The line displays the number of BGP messages sent, the number of notifications (error messages) and the number of messages waiting in a queue for processing.
Received updates	This line displays the number of BGP updates received and sent.
Soft reconfiguration	This line indicates that soft reconfiguration inbound is configured.
Minimum time	Displays the minimum time, in seconds, between advertisements.
(list of inbound and outbound policies)	Displays the policy commands configured and the names of the Route map, AS-PATH ACL or Prefix list configured for the policy.
For address family:	Displays IPv4 Unicast as the address family.
BGP table version	Displays the which version of the primary BGP routing table the router and the neighbor are using.
accepted prefixes	Displays the number of network prefixes accepted by the router and the amount of memory used to process those prefixes.
Prefix advertised	Displays the number of network prefixes advertised, the number rejected and the number withdrawn from the BGP routing table.
Connections established	Displays the number of TCP connections established and dropped between the two peers to exchange BGP information.
Last reset	Displays the amount of time since the peering session was last reset. Also states if the peer resets the peering session. If the peering session was never reset, the word never is displayed.
Local host:	Displays the peering address of the local router and the TCP port number.
Foreign host:	Displays the peering address of the neighbor and the TCP port number.

Related Commands

show ip bgp	View the current BGP routing table.

show ip bgp next-hop

C-Series	No
E-Series	✓

View all next hops (via learned routes only) with current reachability and flap status. This command only displays one path, even if the next hop is reachable by multiple paths.

Syntax **show ip bgp next-hop**

Command Modes EXEC

EXEC privilege

Example

```
Force10>show ip bgp next-hop
 Next-hop        Via                        RefCount  Cost  Flaps Time Elapsed
 63.114.8.33     63.114.8.33, Gi 12/22        240984     0      0 00:18:25
 63.114.8.34     63.114.8.34, Gi 12/22        135152     0      0 00:18:13
 63.114.8.35     63.114.8.35, Gi 12/22             1     0      0 00:18:07
 63.114.8.60     63.114.8.60, Gi 12/22        135155     0      0 00:18:11
Force10>
```

Figure 350 show ip bgp next-hop Command Example

Table 97 defines the information displayed in Figure 350.

Table 97 show ip bgp next-hop Command Fields

Field	Description
Next-hop	Displays the next-hop IP address.
Via	Displays the IP address and interface used to reach the next hop.
RefCount	Displays the number of BGP routes using this next hop.
Cost	Displays the cost associated with using this next hop.
Flaps	Displays the number of times the next hop has flapped.
Time Elapsed	Displays the time elapsed since the next hop was learned. If the route is down, then this field displays time elapsed since the route went down.

show ip bgp paths

C-Series	No
E-Series	✓

View all the BGP path attributes in the BGP database.

Syntax **show ip bgp paths** [**regexp** *regular-expression*]

Parameters

regexp *regular-expression*	Enter a regular expression then use one or a combination of the following characters to match: • **.** = (period) any single character (including a white space) • ***** = (asterisk) the sequences in a pattern (0 or more sequences) • **+** = (plus) the sequences in a pattern (1 or more sequences) • **?** = (question mark) sequences in a pattern (either 0 or 1 sequences). **You must enter an escape sequence (CTRL+v) prior to entering the ? regular expression.** • **[ ]** = (brackets) a range of single-character patterns. • **^** = (caret) the beginning of the input string. If the caret is used at the beginning of a sequence or range, it matches on everything BUT the characters specified. • **$** = (dollar sign) the end of the output string.

Command Modes EXEC

EXEC privilege

Example

```
Force10#show ip bgp path
Total 16 Paths
Address       Hash Refcount Metric Path
0x1efe7e5c      15     10000        32 ?
0x1efe7e1c      71     10000        23 ?
0x1efe7ddc     127     10000        22 ?
0x1efe7d9c     183     10000        43 ?
0x1efe7d5c     239     10000        42 ?
0x1efe7c9c     283         6        {102 103} ?
0x1efe7b1c     287       336 20000  ?
0x1efe7d1c     295     10000        13 ?
0x1efe7c5c     339         6        {92 93} ?
0x1efe7cdc     351     10000        12 ?
0x1efe7c1c     395         6        {82 83} ?
0x1efe7bdc     451         6        {72 73} ?
0x1efe7b5c     491        78     0  ?
0x1efe7adc     883         2   120  i
0x1efe7e9c     983     10000        33 ?
0x1efe7b9c    1003         6     0  i
Force10#
```

Figure 351 show ip bgp paths Command Example (Partial)

Table 98 defines the information displayed in Figure 351.

Table 98 show ip bgp paths Command Fields

Field	Description
Total	Displays the total number of BGP path attributes.
Address	Displays the internal address where the path attribute is stored.
Hash	Displays the hash bucket where the path attribute is stored.
Refcount	Displays the number of BGP routes using this path attribute.

Table 98 show ip bgp paths Command Fields (continued)

Field	Description
Metric	Displays the MED attribute for this path attribute.
Path	Displays the AS path for the route, with the origin code for the route listed last. Numbers listed between braces {} are AS_SET information.

show ip bgp paths as-path

C-Series	No
E-Series	✔

View all unique AS-PATHs in the BGP database

Syntax **show ip bgp paths as-path**

Command Modes EXEC

EXEC privilege

Example

```
Force10#show ip bgp paths as-path
Total 13 AS-Paths
Address       Hash Refcount AS-Path
0x1ea3c1ec     251         1 42
0x1ea3c25c     251         1 22
0x1ea3c1b4     507         1 13
0x1ea3c304     507         1 33
0x1ea3c10c     763         1 {92 93}
0x1ea3c144     763         1 {102 103}
0x1ea3c17c     763         1 12
0x1ea3c2cc     763         1 32
0x1ea3c09c     764         1 {72 73}
0x1ea3c0d4     764         1 {82 83}
0x1ea3c224    1019         1 43
0x1ea3c294    1019         1 23
0x1ea3c02c    1021         4
Force10#
```

Figure 352 show ip bgp paths as-path Command Example (partial)

Table 99 defines the information displayed in Figure 352.

Table 99 show ip bgp paths community Command Fields

Field	Description
Address	Displays the internal address where the path attribute is stored.
Hash	Displays the hash bucket where the path attribute is stored.

Table 99 show ip bgp paths community Command Fields

Field	Description
Refcount	Displays the number of BGP routes using these AS-Paths.
AS-Path	Displays the AS paths for this route, with the origin code for the route listed last. Numbers listed between braces {} are AS_SET information.

show ip bgp paths community

C-Series	No
E-Series	✔

View all unique COMMUNITY numbers in the BGP database.

Syntax **show ip bgp paths community**

Command Modes EXEC

EXEC privilege

Example

```
E1200-BGP>show ip bgp paths community
Total 293 Communities
Address        Hash Refcount Community
0x1ec88a5c        3         4 209:209 209:6059 209:31272 3908:900 19092:300
0x1e0f10ec       15         4 209:209 209:3039 209:31272 3908:900 19092:300
0x1c902234       37         2 209:209 209:7193 209:21362 3908:900 19092:300
0x1f588cd4       41        24 209:209 209:6253 209:21362 3908:900 19092:300
0x1e805884       46         2 209:209 209:21226 286:777 286:3033 1899:3033
64675:21092
0x1e433f4c       46         8 209:209 209:5097 209:21362 3908:900 19092:300
0x1f173294       48        16 209:209 209:21226 286:40 286:777 286:3040 5606:40
12955:5606
0x1c9f8e24       50         6 209:209 209:4069 209:21362 3908:900 19092:300
0x1c9f88e4       53         4 209:209 209:3193 209:21362 3908:900 19092:300
0x1f58a944       57         6 209:209 209:2073 209:21362 3908:900 19092:300
0x1ce6be44       80         2 209:209 209:999 209:40832
0x1c6e2374       80         2 209:777 209:41528
0x1f58ad6c       82        46 209:209 209:41528
0x1c6e2064       83         2 209:777 209:40832
0x1f588ecc       85       570 209:209 209:40832
0x1f57cc0c       98         2 209:209 209:21226 286:3031 13646:1044 13646:1124
13646:1154 13646:1164 13646:1184 13646:1194 13646:1204 13646:1214 13646:1224
13646:1234 13646:1244 13646:1254 13646:1264 13646:3000
0x1d65b2ac      117         6 209:209 209:999 209:31272
0x1f5854ac      119        18 209:209 209:21226 286:108 286:111 286:777 286:3033
517:5104
```

Figure 353 show ip bgp paths community Command Example (partial)

Table 100 defines the information displayed in Figure 353.

Table 100 show ip bgp paths community Command Fields

Field	Description
Address	Displays the internal address where the path attribute is stored.
Hash	Displays the hash bucket where the path attribute is stored.
Refcount	Displays the number of BGP routes using these communities.
Community	Displays the community attributes in this BGP path.

show ip bgp peer-group

C-Series	No
E-Series	✔

Allows you to view information on the BGP peers in a peer group.

Syntax **show ip bgp peer-group** [*peer-group-name* [**detail** | **summary**]]

Parameters

peer-group-name	(OPTIONAL) Enter the name of a peer group to view information about that peer group only.
detail	(OPTIONAL) Enter the keyword **detail** to view detailed status information of the peers in that peer group.
summary	(OPTIONAL) Enter the keyword **summary** to view status information of the peers in that peer group. The output is the same as that found in show ip bgp summary command

Command Modes

EXEC

EXEC privilege

Command History

Version 7.5.1.0	Modified: Added **detail** option.

Example

```
Force10#show ip bgp peer-group


Peer-group RT-PEERS
Description: ***peering-with-RT***
BGP version 4
Minimum time between advertisement runs is 30 seconds

For address family: IPv4 Unicast
BGP neighbor is RT-PEERS
Number of peers in this group 20
Peer-group members (* - outbound optimized):
  12.1.1.2*
  12.1.1.3*
  12.1.1.4*
  12.1.1.5*
  12.1.1.6*
  12.2.1.2*
  12.2.1.3*
  12.2.1.4*
  12.2.1.5*
  12.2.1.6*
  12.3.1.2*
  12.3.1.3*
  12.3.1.4*
  12.3.1.5*
  12.3.1.6*
  12.4.1.2*
  12.4.1.3*
  12.4.1.4*
  12.4.1.5*
  12.4.1.6*
```

Figure 354 show ip bgp peer-group Command Example (Partial)

Table 101 defines the information displayed in Figure 354.

Table 101 show ip bgp peer-group Command Fields

Line beginning with	Description
Peer-group	Displays the peer group's name.
Administratively shut	Displays the peer group's status if the peer group is not enabled. If the peer group is enabled, this line is not displayed.
BGP version	Displays the BGP version supported.
Minimum time	Displays the time interval between BGP advertisements.
For address family	Displays IPv4 Unicast as the address family.
BGP neighbor	Displays the name of the BGP neighbor.
Number of peers	Displays the number of peers currently configured for this peer group.
Peer-group members:	Lists the IP addresses of the peers in the peer group. If the address is outbound optimized, a * is displayed next to the IP address.

Related Commands

neighbor peer-group (assigning peers)	Assign peer to a peer-group.
neighbor peer-group (creating group)	Create a peer group.
show ip bgp peer-group (multicast)	View information on the BGP peers in a peer group.

show ip bgp regexp

C-Series	No
E-Series	✓

Allows you to view the subset of BGP routing table matching the regular expressions specified.

Syntax **show ip bgp regexp** *regular-expression* [*character*]

Parameters

regular-expression [*character*]	Enter a regular expression then use one or a combination of the following characters to match: • **.** = (period) any single character (including a white space) • ***** = (asterisk) the sequences in a pattern (0 or more sequences) • **+** = (plus) the sequences in a pattern (1 or more sequences) • **?** = (question mark) sequences in a pattern (either 0 or 1 sequences). **You must enter an escape sequence (CTRL+v) prior to entering the ? regular expression.** • **[ ]** = (brackets) a range of single-character patterns. • **^** = (caret) the beginning of the input string. If the caret is used at the beginning of a sequence or range, it matches on everything BUT the characters specified. • **$** = (dollar sign) the end of the output string.

Command Modes EXEC

EXEC privilege

Example

```
Force10#show ip bgp regexp ^2914+
BGP table version is 3700481, local router ID is 63.114.8.35
Status codes: s suppressed, S stale, d damped, h history, * valid, > best
Path source: I - internal, a - aggregate, c - confed-external, r - redistributed, n - network
Origin codes: i - IGP, e - EGP, ? - incomplete
    Network          Next Hop            Metric     LocPrf Weight Path
*>I 3.0.0.0/8        1.1.1.2                  0        100      0 2914 1239 80 i
*>I 4.0.0.0/8        1.1.1.2                  0        100      0 2914 3356 i
*>I 4.17.225.0/24    1.1.1.2                  0        100      0 2914 11853 11853 11853 11853 11853 6496
*>I 4.17.226.0/23    1.1.1.2                  0        100      0 2914 11853 11853 11853 11853 11853 6496
*>I 4.17.251.0/24    1.1.1.2                  0        100      0 2914 11853 11853 11853 11853 11853 6496
*>I 4.17.252.0/23    1.1.1.2                  0        100      0 2914 11853 11853 11853 11853 11853 6496
*>I 4.19.2.0/23      1.1.1.2                  0        100      0 2914 701 6167 6167 6167 i
*>I 4.19.16.0/23     1.1.1.2                  0        100      0 2914 701 6167 6167 6167 i
*>I 4.21.80.0/22     1.1.1.2                  0        100      0 2914 174 4200 16559 i
*>I 4.21.82.0/24     1.1.1.2                  0        100      0 2914 174 4200 16559 i
*>I 4.21.252.0/23    1.1.1.2                  0        100      0 2914 701 6389 8063 19198 i
*>I 4.23.180.0/24    1.1.1.2                  0        100      0 2914 3561 6128 30576 i
*>I 4.36.200.0/21    1.1.1.2                  0        100      0 2914 14742 11854 14135 i
*>I 4.67.64.0/22     1.1.1.2                  0        100      0 2914 11608 19281 i
*>I 4.78.32.0/21     1.1.1.2                  0        100      0 2914 3491 29748 i
*>I 6.1.0.0/16       1.1.1.2                  0        100      0 2914 701 668 i
*>I 6.2.0.0/22       1.1.1.2                  0        100      0 2914 701 668 i
*>I 6.3.0.0/18       1.1.1.2                  0        100      0 2914 701 668 i
```

Figure 355 show ip bgp regexp Command Example (Partial)

Table 102 defines the information displayed in Figure 355.

Table 102 show ip bgp regexp Command Example Fields

Field	Description
Network	Displays the destination network prefix of each BGP route.
Next Hop	Displays the next hop address of the BGP router. If 0.0.0.0 is listed in this column, then non-BGP routes exist in the router's routing table.
Metric	Displays the BGP router's metric, if assigned.
LocPrf	Displays the BGP LOCAL_PREF attribute for the route.
Weight	Displays the route's weight
Path	Lists all the AS paths the route passed through to reach the destination network.

show ip bgp summary

C-Series	No
E-Series	✓

Allows you to view the status of all BGP connections.

Syntax **show ip bgp summary**

Command Modes EXEC

EXEC privilege

Example

```
Force10#show ip bgp summary
BGP router identifier 120.10.10.1, local AS number 100
BGP table version is 34, main routing table version 34
9 network entrie(s) using 1372 bytes of memory
5 paths using 380 bytes of memory
4 denied paths using 164 bytes of memory
BGP-RIB over all using 385 bytes of memory
2 BGP path attribute entrie(s) using 168 bytes of memory
1 BGP AS-PATH entrie(s) using 39 bytes of memory
1 BGP community entrie(s) using 43 bytes of memory
2 neighbor(s) using 7232 bytes of memory

Neighbor        AS     MsgRcvd  MsgSent     TblVer  InQ  OutQ Up/Down  State/Pfx

100.10.10.2     200         46       41         34    0     0 00:14:33         5
120.10.10.2     300         40       47         34    0     0 00:37:10         0
Force10#
```

Figure 356 show ip bgp summary Command Example

Table 103 describes the information in Figure 356.

Table 103 show ip bgp summary Command Fields

Field	Description
BGP router identifier	Displays the local router ID and the AS number.
BGP table version	Displays the BGP table version and the main routing table version.
network entries	Displays the number of network entries and route paths and the amount of memory used to process those entries.
paths	Displays the number of paths and the amount of memory used.
denied paths	Displays the number of denied paths and the amount of memory used.
BGP path attribute entries	Displays the number of BGP path attributes and the amount of memory used to process them.
BGP AS-PATH entries	Displays the number of BGP AS_PATH attributes processed and the amount of memory used to process them.
BGP community entries	Displays the number of BGP COMMUNITY attributes processed and the amount of memory used to process them. The show ip bgp community command provides more details on the COMMUNITY attributes.
Dampening enabled	Displayed only when dampening is enabled. Displays the number of paths designated as history, dampened, or penalized.
Neighbor	Displays the BGP neighbor address.
AS	Displays the AS number of the neighbor.
MsgRcvd	Displays the number of BGP messages that neighbor received.
MsgSent	Displays the number of BGP messages that neighbor sent.
TblVer	Displays the version of the BGP table that was sent to that neighbor.
InQ	Displays the number of messages from that neighbor waiting to be processed.
OutQ	Displays the number of messages waiting to be sent to that neighbor. If a number appears in parentheses, the number represents the number of messages waiting to be sent to the peer group.

Table 103 show ip bgp summary Command Fields

Field	Description
Up/Down	Displays the amount of time (in hours:minutes:seconds) that the neighbor is in the Established stage. If the neighbor has never moved into the Established stage, the word never is displayed.
State/Pfxrcd	If the neighbor is in Established stage, the number of network prefixes received. If a maximum limit was configured with the neighbor maximum-prefix command, (prfxd) appears in this column. If the neighbor is not in Established stage, the current stage is displayed (Idle, Connect, Active, OpenSent, OpenConfirm) When the peer is transitioning between states and clearing the routes received, the phrase (Purging) may appear in this column. If the neighbor is disabled, the phrase (Admin shut) appears in this column.

MBGP Commands

Multiprotocol BGP (MBGP) is an enhanced BGP that enables multicast routing policy throughout the Internet and connecting multicast topologies between BGP and autonomous systems (AS). FTOS MBGP is implemented as per IETF RFC 1858. The MBGP commands are:

- address family on page 1099
- aggregate-address on page 1100
- bgp dampening on page 1101
- clear ip bgp ipv4 multicast on page 1102
- clear ip bgp dampening on page 1102
- clear ip bgp flap-statistics on page 1103
- debug ip bgp dampening on page 1103
- debug ip bgp dampening on page 1103
- debug ip bgp dampening on page 1103
- debug ip bgp peer-group updates on page 1104
- debug ip bgp updates on page 1104
- distance bgp on page 1105
- neighbor activate on page 1106
- neighbor advertisement-interval on page 1106
- neighbor default-originate on page 1107

- neighbor distribute-list on page 1108
- neighbor filter-list on page 1108
- neighbor maximum-prefix on page 1109
- neighbor next-hop-self on page 1110
- neighbor remove-private-AS on page 1111
- neighbor route-map on page 1111
- neighbor route-reflector-client on page 1112
- network on page 1113
- redistribute on page 1114
- redistribute ospf on page 1115
- show ip bgp ipv4 multicast on page 1115
- show ip bgp cluster-list on page 1117
- show ip bgp community on page 1117
- show ip bgp community-list on page 1118
- show ip bgp dampened-paths on page 1118
- show ip bgp filter-list on page 1119
- show ip bgp flap-statistics on page 1119
- show ip bgp inconsistent-as on page 1120
- show ip bgp ipv4 multicast neighbors on page 1120
- show ip bgp peer-group on page 1123
- show ip bgp summary on page 1124

address family

C-Series	No
E-Series	✓

This command changes the context to SAFI (Subsequent Address Family Identifier).

Syntax **address family ipv4 multicast**

To remove SAFI context, use the **no address family ipv4 multicast** command.

Parameters

ipv4	Enter the keyword **ipv4** to specify the address family as IPV4.
multicast	Enter the keyword **multicast** to specify multicast as SAFI.

Defaults IPv4 Unicast

Command Modes ROUTER BGP (conf-router_bgp)

Usage Information

All subsequent commands will apply to this address family once this command is executed. You can exit from this AFI/SAFI to the IPv4 Unicast (the default) family by entering **exit** and returning to the Router BGP context.

aggregate-address

C-Series	No
E-Series	✓

Summarize a range of prefixes to minimize the number of entries in the routing table.

Syntax

aggregate-address *ip-address mask* [**advertise-map** *map-name*] [**as-set**] [**attribute-map** *map-name*] [**summary-only**] [**suppress-map** *map-name*]

Parameters

ip-address mask	Enter the IP address and mask of the route to be the aggregate address. Enter the IP address in dotted decimal format (A.B.C.D) and mask in /prefix format (/x).
advertise-map *map-name*	(OPTIONAL) Enter the keywords **advertise-map** followed by the name of a configured route map to set filters for advertising an aggregate route.
as-set	(OPTIONAL) Enter the keyword **as-set** to generate path attribute information and include it in the aggregate. AS_SET includes AS_PATH and community information from the routes included in the aggregated route.
attribute-map *map-name*	(OPTIONAL) Enter the keywords **attribute-map** followed by the name of a configured route map to modify attributes of the aggregate, excluding AS_PATH and NEXT_HOP attributes.
summary-only	(OPTIONAL) Enter the keyword **summary-only** to advertise only the aggregate address. Specific routes will not be advertised.
suppress-map *map-name*	(OPTIONAL) Enter the keywords **suppress-map** followed by the name of a configured route map to identify which more-specific routes in the aggregate are suppressed.

Defaults

Not configured.

Command Modes

ROUTER BGP Address Family (conf-router_bgp_af)

Usage Information

At least one of the routes included in the aggregate address must be in the BGP routing table for the configured aggregate to become active.

Do not add the **as-set** parameter to the aggregate. If routes within the aggregate are constantly changing, the aggregate will flap to keep track of the changes in the AS_PATH.

In route maps used in the **suppress-map** parameter, routes meeting the **deny** clause are not suppress; in other words, they are allowed. The opposite is true: routes meeting the **permit** clause are suppressed.

If the route is injected via the network command, that route will still appear in the routing table if the summary-only parameter is configured in the aggregate-address command.

The summary-only parameter suppresses all advertisements. If you want to suppress advertisements to only specific neighbors, use the neighbor distribute-list command.

bgp dampening

C-Series	**No**
E-Series	✔

Enable MBGP route dampening.

Syntax **bgp dampening** [*half-life time*] [**route-map** *map-name*]

To disable route dampening, use the **no bgp dampening** [*half-life time*] [**route-map** *map-name*] command.

Parameters

half-life time	(OPTIONAL) Enter the number of minutes after which the Penalty is decreased. After the router assigns a Penalty of 1024 to a route, the Penalty is decreased by half, after the half-life period expires. Range: 1 to 45. Default: 15 minutes
route-map *map-name*	(OPTIONAL) Enter the keyword **route-map** followed by the name of a configured route map. Only match commands in the configured route map are supported.

Defaults Disabled.

Command Modes ROUTER BGP Address Family (conf-router_bgp_af)

clear ip bgp ipv4 multicast

C-Series	No
E-Series	✓

Reset MBGP sessions.

Syntax **clear ip bgp ipv4 multicast** * *ip-address* [**dampening** | **flap-statistics**] **peer-group**]

Parameters

*	Enter the character * to clear all peers.
ip-address	Enter an IP address in dotted decimal format to clear the prefixes from that neighbor.
dampening	(OPTIONAL) Enter the keyword **dampening** to clear route flap dampening information.
flap-statistics	(OPTIONAL) Enter the keyword **flap-statistics** to reset the flap statistics on all prefixes from that neighbor.
peer-group	(OPTIONAL) Enter the keyword **peer-group** to clear all members of a peer-group.

Command Modes EXEC privilege

clear ip bgp dampening

C-Series	No
E-Series	✓

Clear information on route dampening.

Syntax **clear ip bgp dampening ipv4 multicast** *network network-mask*

Parameters

dampening	Enter the keyword **dampening** to clear route flap dampening information.
network	(OPTIONAL) Enter the network address in dotted decimal format (A.B.C.D).
network-mask	(OPTIONAL) Enter the network mask in slash prefix format (/x).

Command Modes EXEC privilege

clear ip bgp flap-statistics

C-Series	No
E-Series	✓

Clear BGP flap statistics, which includes number of flaps and the time of the last flap.

Syntax **clear ip bgp ipv4 multicast flap-statistics Network | filter-list** *list* **|regexp** *regexp*

Parameters

Network	(OPTIONAL) Enter the network address to clear flap statistics in dotted decimal format (A.B.C.D).
filter-list *list*	(OPTIONAL) Enter the keyword **filter-list** followed by the name of a configured AS-PATH list (max 16 characters).
regexp *regexp*	(OPTIONAL) Enter the keyword **regexp** followed by regular expressions. Use one or a combination of the following: . (period) matches on any single character, including white space * (asterisk) matches on sequences in a pattern (zero or more sequences) + (plus sign) matches on sequences in a pattern (one or more sequences) ? (question mark) matches sequences in a pattern (0 or 1 sequences) [ ] (brackets) matches a range of single-character patterns. ^ (caret) matches the beginning of the input string. (If the caret is used at the beginning of a sequence or range, it matches on everything BUT the characters specified.) $ (dollar sign) matches the end of the output string.

Command Modes EXEC privilege

debug ip bgp dampening

C-Series	No
E-Series	✓

View information on routes being dampened.

Syntax **debug ip bgp ipv4 multicast dampening**

To disable debugging, enter **no debug ip bgp ipv4 multicast dampening**

Parameters

dampening	Enter the keyword **dampening** to clear route flap dampening information.

Command Modes EXEC privilege

debug ip bgp peer-group updates

C-Series	No
E-Series	✓

View information about BGP peer-group updates.

debug ip bgp peer-group *peer-group-name* **updates** [**in** | **out**]

To disable debugging, enter **no debug ip bgp peer-group** *peer-group-name* **updates** [**in** | **out**] command.

Parameters

peer-group *peer-group-name*	Enter the keyword **peer-group** followed by the name of the peer-group.
updates	Enter the keyword **updates** to view BGP update information.
in	(OPTIONAL) Enter the keyword **in** to view only BGP updates received from neighbors.
out	(OPTIONAL) Enter the keyword **out** to view only BGP updates sent to neighbors.

Command Modes

EXEC

EXEC privilege

debug ip bgp updates

C-Series	No
E-Series	✓

View information about BGP updates.

debug ip bgp updates [**in** | **out**]

To disable debugging, enter **no debug ip bgp updates** [**in** | **out**] command.

Parameters

updates	Enter the keyword **updates** to view BGP update information.
in	(OPTIONAL) Enter the keyword **in** to view only BGP updates received from neighbors.
out	(OPTIONAL) Enter the keyword **out** to view only BGP updates sent to neighbors.

Command Modes

EXEC privilege

Defaults Disabled.

distance bgp

C-Series	No
E-Series	✓

Define an administrative distance for routes.

Syntax **distance bgp** *external-distance internal-distance local-distance*

To return to default values, enter **no distance bgp**.

Parameters

external-distance	Enter a number to assign to routes learned from a neighbor external to the AS. Range: 1 to 255. Default: 20
internal-distance	Enter a number to assign to routes learned from a router within the AS. Range: 1 to 255. Default: 200
local-distance	Enter a number to assign to routes learned from networks listed in the network command. Range: 1 to 255. Default: 200

Defaults *external-distance* = 20; *internal-distance* = 200; *local-distance* = 200.

Command Modes ROUTER BGP (conf-router_bgp_af)

Caution: Force10 Networks recommends that you do not change the administrative distance of internal routes. Changing the administrative distances may cause routing table inconsistencies.

Usage Information The higher the administrative distance assigned to a route means that your confidence in that route is low. Routes assigned an administrative distance of 255 are not installed in the routing table. Routes from confederations are treated as internal BGP routes.

neighbor activate

C-Series	No
E-Series	✓

This command allows the specified neighbor/peer group to be enabled for the current AFI/SAFI.

Syntax **neighbor** [*ip-address* | *peer-group-name*] **activate**

To disable, use the **no neighbor** [*ip-address* | *peer-group-name*] **activate** command.

Parameters

ip-address	(OPTIONAL) Enter the IP address of the neighbor in dotted decimal format.
peer-group-name	(OPTIONAL) Enter the name of the peer group
activate	Enter the keyword **activate** to enable the neighbor/peer group in the new AFI/SAFI.

Defaults Disabled

Command Modes ROUTER BGP Address Family (conf-router_bgp_af)

Usage Information By default, when a neighbor/peer group configuration is created in the Router BGP context, it is enabled for the IPv4/Unicast AFI/SAFI. By using **activate** in the new context, the neighbor/peer group is enabled for AFI/SAFI.

Related Commands

address family	Changes the context to SAFI

neighbor advertisement-interval

C-Series	No
E-Series	✓

Set the advertisement interval between BGP neighbors or within a BGP peer group.

Syntax **neighbor** {*ip-address* | *peer-group-name*} **advertisement-interval** *seconds*

To return to the default value, use the **no neighbor** {*ip-address* | *peer-group-name*} **advertisement-interval** command.

Parameters

ip-address	Enter the IP address of the neighbor in dotted decimal format.

peer-group-name	Enter the name of the peer group to set the advertisement interval for all routers in the peer group.
seconds	Enter a number as the time interval, in seconds, between BGP advertisements. Range: 0 to 600 seconds. Default: 5 seconds for internal BGP peers; 30 seconds for external BGP peers.

Defaults *seconds* = 5 seconds (internal peers); *seconds* = 30 seconds (external peers)

Command Modes ROUTER BGP Address Family (conf-router_bgp_af)

neighbor default-originate

C-Series	**No**
E-Series	✓

Inject the default route to a BGP peer or neighbor.

Syntax **neighbor** {*ip-address* | *peer-group-name*} **default-originate** [**route-map** *map-name*]

To remove a default route, use the **no neighbor** {*ip-address* | *peer-group-name*} **default-originate** command.

Parameters

ip-address	Enter the IP address of the neighbor in dotted decimal format.
peer-group-name	Enter the name of the peer group to set the default route of all routers in that peer group.
route-map *map-name*	(OPTIONAL) Enter the keyword **route-map** followed by the name of a configured route map.

Defaults Not configured.

Command Modes ROUTER BGP Address Family (conf-router_bgp_af)

neighbor distribute-list

C-Series	No
E-Series	✓

Distribute BGP information via an established prefix list.

Syntax **neighbor** [*ip-address* | *peer-group-name*] **distribute-list** *prefix-list-name* [**in** | **out**]

To delete a neighbor distribution list, use the **no neighbor** [*ip-address* | *peer-group-name*] **distribute-list** *prefix-list-name* [**in** | **out**] command.

Parameters

ip-address	Enter the IP address of the neighbor in dotted decimal format.
peer-group-name	Enter the name of the peer group to apply the distribute list filter to all routers in the peer group.
prefix-list-name	Enter the name of an established prefix list. If the prefix list is not configured, the default is permit (to allow all routes).
in	Enter the keyword **in** to distribute only inbound traffic.
out	Enter the keyword **out** to distribute only outbound traffic.

Defaults Not configured.

Command Modes ROUTER BGP Address Family (conf-router_bgp_af)

Usage Information Other BGP filtering commands include: neighbor filter-list, ip as-path access-list, and neighbor route-map.

Related Commands

ip as-path access-list	Configure IP AS-Path ACL.
neighbor filter-list	Assign a AS-PATH list to a neighbor or peer group.
neighbor route-map	Assign a route map to a neighbor or peer group.

neighbor filter-list

C-Series	No
E-Series	✓

Configure a BGP filter based on the AS-PATH attribute.

Syntax **neighbor** [*ip-address* | *peer-group-name*] **filter-list aspath** *access-list-name* [**in** | **out**]

To delete a BGP filter, use the **no neighbor** [*ip-address* | *peer-group-name*] **filter-list aspath** *access-list-name* [**in** | **out**] command.

Parameters

ip-address	Enter the IP address of the neighbor in dotted decimal format.
peer-group-name	Enter the name of the peer group to apply the filter to all routers in the peer group.
access-list-name	Enter the name of an established AS-PATH access list. If the AS-PATH access list is not configured, the default is permit (to allow routes).
in	Enter the keyword **in** to filter inbound BGP routes.
out	Enter the keyword **out** to filter outbound BGP routes.

Defaults Not configured.

Command Modes ROUTER BGP Address Family (conf-router_bgp_af)

Usage Information Use the ip as-path access-list command syntax in the CONFIGURATION mode to enter the AS-PATH ACL mode and configure AS-PATH filters to deny or permit BGP routes based on information in their AS-PATH attribute.

Related Commands

ip as-path access-list	Enter AS-PATH ACL mode and configure AS-PATH filters.

neighbor maximum-prefix

C-Series	**No**
E-Series	✓

Control the number of network prefixes received.

Syntax **neighbor** *ip-address* | *peer-group-name* **maximum-prefix** *maximum* [*threshold*] [**warning-only**]

To return to the default values, use the **no neighbor** *ip-address* | *peer-group-name* **maximum-prefix** *maximum* command.

Parameters

ip-address	(OPTIONAL) Enter the IP address of the neighbor in dotted decimal format.
peer-group-name	(OPTIONAL) Enter the name of the peer group.
maximum	Enter a number as the maximum number of prefixes allowed for this BGP router. Range: 1 to 4294967295.

threshold	(OPTIONAL) Enter a number to be used as a percentage of the *maximum* value. When the number of prefixes reaches this percentage of the *maximum* value, the E-Series software sends a message. Range: 1 to 100 percent. Default: 75
warning-only	(OPTIONAL) Enter the keyword **warning-only** to set the router to send a log message when the maximum value is reached. If this parameter is not set, the router stops peering when the maximum number of prefixes is reached.

Defaults *threshold* = 75

Command Modes ROUTER BGP Address Family (conf-router_bgp_af)

neighbor next-hop-self

C-Series	No
E-Series	✓

Allows you to configure the router as the next hop for a BGP neighbor.

Syntax **neighbor** *ip-address* | *peer-group-name* **next-hop-self**

To return to the default setting, use the **no neighbor** *ip-address* | *peer-group-name* **next-hop-self** command.

Parameters

ip-address	(OPTIONAL) Enter the IP address of the neighbor in dotted decimal format.
peer-group-name	(OPTIONAL) Enter the name of the peer group.

Defaults Disabled.

Command Modes ROUTER BGP Address Family (conf-router_bgp_af)

Usage Information If the set next-hop command in the ROUTE-MAP mode is configured, its configuration takes precedence over the neighbor next-hop-self command.

neighbor remove-private-AS

C-Series	No
E-Series	✓

Remove private AS numbers from the AS-PATH of outgoing updates.

Syntax **neighbor** *ip-address* | *peer-group-name* **remove-private-as**

To return to the default, use the **no neighbor** *ip-address* | *peer-group-name* **remove-private-as** command.

Parameters

ip-address	(OPTIONAL) Enter the IP address of the neighbor to remove the private AS numbers.
peer-group-name	(OPTIONAL) Enter the name of the peer group to remove the private AS numbers

Defaults Disabled (that is, private AS number are not removed).

Command Modes ROUTER BGP Address Family (conf-router_bgp_af)

neighbor route-map

C-Series	No
E-Series	✓

Apply an established route map to either incoming or outbound routes of a BGP neighbor or peer group.

Syntax **neighbor** [*ip-address* | *peer-group-name*] **route-map** *map-name* [**in** | **out**]

To remove the route map, use the **no neighbor** [*ip-address* | *peer-group-name*] **route-map** *map-name* [**in** | **out**] command.

Parameters

ip-address	(OPTIONAL) Enter the IP address of the neighbor in dotted decimal format.
peer-group-name	(OPTIONAL) Enter the name of the peer group.
map-name	Enter the name of an established route map. If the Route map is not configured, the default is deny (to drop all routes).
in	Enter the keyword **in** to filter inbound routes.
out	Enter the keyword **out** to filter outbound routes.

Defaults Not configured.

Command Modes ROUTER BGP Address Family (conf-router_bgp_af)

Usage Information When you apply a route map to outbound routes, only routes that match at least one section of the route map are permitted.

If you identify a peer group by name, the peers in that peer group inherit the characteristics in the Route map used in this command. If you identify a peer by IP address, the Route map overwrites either the inbound or outbound policies on that peer.

neighbor route-reflector-client

C-Series	No
E-Series	✓

Configure a neighbor as a member of a route reflector cluster.

Syntax **neighbor** *ip-address* | *peer-group-name* **route-reflector-client**

To indicate that the neighbor is not a route reflector client or to delete a route reflector configuration, use the **no neighbor** *ip-address* | *peer-group-name* **route-reflector-client** command.

Parameters

ip-address	(OPTIONAL) Enter the IP address of the neighbor in dotted decimal format.
peer-group-name	(OPTIONAL) Enter the name of the peer group. All routers in the peer group receive routes from a route reflector.

Defaults Not configured.

Command Modes ROUTER BGP Address Family (conf-router_bgp_af)

Usage Information The first time you enter this command it configures the neighbor as a route reflector and members of the route-reflector cluster. Internal BGP (IBGP) speakers do not need to be fully meshed if you configure a route reflector.

When all clients of a route reflector are disabled, the neighbor is no longer a route reflector.

network

C-Series	No
E-Series	✓

Specify the networks for the BGP process and enter them in the BGP routing table.

Syntax

network *ip-address mask* [**route-map** *map-name*]

To remove a network, use the **no network** *ip-address mask* [**route-map** *map-name*] command.

Parameters

ip-address	Enter an IP address in dotted decimal format of the network.
mask	Enter the mask of the IP address in the slash prefix length format (for example, /24). The mask appears in command outputs in dotted decimal format (A.B.C.D).
route-map *map-name*	(OPTIONAL) Enter the keyword **route-map** followed by the name of an established route map. Only the following ROUTE-MAP mode commands are supported: • match ip address • set community • set local-preference • set metric • set next-hop • set origin • set weight If the route map is not configured, the default is deny (to drop all routes).

Defaults

Not configured.

Command Modes

ROUTER BGP Address Family (conf-router_bgp_af)

Usage Information

The E-Series software resolves the network address configured by the network command with the routes in the main routing table to ensure that the networks are reachable via non-BGP routes and non-default routes.

Related Commands

redistribute	Redistribute routes into BGP.

redistribute

C-Series	No
E-Series	✓

Redistribute routes into BGP.

Syntax

redistribute [**connected** | **static**] [**route-map** *map-name*]

To disable redistribution, use the **no redistribution** [**connected** | **static**] [**route-map** *map-name*] command.

Parameters

connected	Enter the keyword **connected** to redistribute routes from physically connected interfaces.
static	Enter the keyword **static** to redistribute manually configured routes. These routes are treated as incomplete routes.
route-map *map-name*	(OPTIONAL) Enter the keyword **route-map** followed by the name of an established route map. Only the following ROUTE-MAP mode commands are supported: • match ip address • set community • set local-preference • set metric • set next-hop • set origin • set weight If the route map is not configured, the default is deny (to drop all routes).

Defaults

Not configured.

Command Modes

ROUTER BGP Address Family (conf-router_bgp_af)

Usage Information

If you do not configure default-metric command, in addition to the redistribute command, or there is no route map to set the metric, the metric for redistributed static and connected is “0”.

To redistribute the default route (0.0.0.0/0) configure the neighbor default-originate command.

Related Commands

neighbor default-originate	Inject the default route.

redistribute ospf

C-Series	No
E-Series	✓

Redistribute OSPF routes into BGP.

Syntax **redistribute ospf** *process-id* [[**match external** {**1** | **2**}] [**match internal**]] [**route-map** *map-name*]

To stop redistribution of OSPF routes, use the **no redistribute ospf** *process-id* command.

Parameters

process-id	Enter the number of the OSPF process. Range: 1 to 65535
match external {**1** | **2**}	(OPTIONAL) Enter the keywords match external to redistribute OSPF external routes. You can specify 1 or 2 to redistribute those routes only.
match internal	(OPTIONAL) Enter the keywords **match internal** to redistribute OSPF internal routes only.
route-map *map-name*	(OPTIONAL) Enter the keywords **route-map** followed by the name of a configured Route map.

Defaults Not configured.

Command Modes ROUTER BGP Address Family (conf-router_bgp_af)

Usage Information When you enter redistribute ospf *process-id* command without any other parameters, FTOS redistributes all OSPF internal routes, external type 1 routes, and external type 2 routes.

This feature is not supported by an RFC.

show ip bgp ipv4 multicast

C-Series	No
E-Series	✓

View the current MBGP routing table for the E-Series.

Syntax **show ip bgp ipv4 multicast** [**detail** | *network* [*network-mask*] [**length**]]

Parameters

detail	(OPTIONAL) Enter the keyword **detail** to display BGP internal information for the IPv4 Multicast address family.
network	(OPTIONAL) Enter the network address (in dotted decimal format) of the BGP network to view information only on that network.

network-mask	(OPTIONAL) Enter the network mask (in slash prefix format) of the BGP network address.
longer-prefixes	(OPTIONAL) Enter the keyword **longer-prefixes** to view all routes with a common prefix.

Command Modes

EXEC

EXEC privilege

Command History

Version 7.5.1.0	Modified: Added **detail** option.

Example

```
Force10#show ip bgp ipv4 multicast
BGP table version is 14, local router ID is 100.10.10.1
Status codes: s suppressed, S stale, d damped, h history, * valid, > best
Path source: I - internal, a - aggregate, c - confed-external, r - redistributed, n - network
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network            Next Hop            Metric     LocPrf Weight Path
*>I 25.1.0.0/16        25.25.25.25              0        100      0 i
*>I 25.2.0.0/16        25.25.25.26              0        100      0 ?
*>I 25.3.0.0/16        211.1.1.165              0        100      0 ?
*>r 144.1.0.0/16       0.0.0.0                  0             32768 ?
*>r 144.2.0.0/16       100.10.10.10             0             32768 ?
*>r 144.3.0.0/16       211.1.1.135              0             32768 ?
*>n 145.1.0.0/16       0.0.0.0                  0             32768 i
Force10#
```

Figure 357 show ip bgp Command Example

Table 104 defines the information displayed in Figure 357.

Table 104 show ip bgp Command Example Fields

Field	Description
Network	Displays the destination network prefix of each BGP route.
Next Hop	Displays the next hop address of the BGP router. If 0.0.0.0 is listed in this column, then local routes exist in the routing table.
Metric	Displays the BGP route's metric, if assigned.
LocPrf	Displays the BGP LOCAL_PREF attribute for the route.
Weight	Displays the route's weight
Path	Lists all the ASs the route passed through to reach the destination network.

Related Commands

show ip bgp community	View BGP communities.

show ip bgp cluster-list

C-Series	No
E-Series	✓

View BGP neighbors in a specific cluster.

Syntax **show ip bgp ipv4 multicast cluster-list** [*cluster-id*]

Parameters

cluster-id	(OPTIONAL) Enter the cluster id in dotted decimal format.

Command Modes EXEC

EXEC privilege

show ip bgp community

C-Series	No
E-Series	✓

View information on all routes with Community attributes or view specific BGP community groups.

Syntax **show ip bgp ipv4 multicast community** [*community-number*] [**local-as**] [**no-export**] [**no-advertise**]

Parameters

community-number	Enter the community number in AA:NN format where AA is the AS number (2 bytes) and NN is a value specific to that autonomous system. You can specify up to eight community numbers to view information on those community groups.
local-AS	Enter the keywords **local-AS** to view all routes with the COMMUNITY attribute of NO_EXPORT_SUBCONFED. All routes with the NO_EXPORT_SUBCONFED (0xFFFFFF03) community attribute must not be advertised to external BGP peers.
no-advertise	Enter the keywords **no-advertise** to view all routes containing the well-known community attribute of NO_ADVERTISE. All routes with the NO_ADVERTISE (0xFFFFFF02) community attribute must not be advertised to other BGP peers.
no-export	Enter the keywords **no-export** to view all routes containing the well-known community attribute of NO_EXPORT. All routes with the NO_EXPORT (0xFFFFFF01) community attribute must not be advertised outside a BGP confederation boundary.

Command Modes EXEC

EXEC privilege

Usage Information

To view the total number of COMMUNITY attributes found, use the show ip bgp summary command. The text line above the route table states the number of COMMUNITY attributes found.

The show ip bgp community command without any parameters lists BGP routes with at least one BGP community attribute and the output is the same as for the show ip bgp command output.

show ip bgp community-list

C-Series	**No**
E-Series	✓

View routes that are affected by a specific community list.

Syntax **show ip bgp ipv4 multicast community-list** *community-list-name*

Parameters

community-list-name	Enter the name of a configured IP community list.

Command Modes EXEC

EXEC privilege

show ip bgp dampened-paths

C-Series	**No**
E-Series	✓

View BGP routes that are dampened (non-active).

Syntax **show ip bgp ipv4 multicast dampened-paths**

Command Modes EXEC

EXEC privilege

show ip bgp filter-list

C-Series	No
E-Series	✓

View the routes that match the filter lists.

Syntax **show ip bgp ipv4 multicast filter-list** *as-path-name*

Parameters		
	as-path-name	Enter the name of an AS-PATH.

Command Modes EXEC

EXEC privilege

show ip bgp flap-statistics

C-Series	No
E-Series	✓

View flap statistics on BGP routes.

Syntax **show ip bgp ipv4 multicast flap-statistics** [*ip-address* [*mask*]] [**filter-list** *as-path-name*] [**regexp** *regular-expression*]

Parameters		
	ip-address	(OPTIONAL) Enter the IP address (in dotted decimal format) of the BGP network to view information only on that network.
	mask	(OPTIONAL) Enter the network mask (in slash prefix (/x) format) of the BGP network address.
	filter-list *as-path-name*	(OPTIONAL) Enter the keyword **filter-list** followed by the name of a configured AS-PATH ACL.
	regexp *regular-expression*	Enter a regular expression then use one or a combination of the following characters to match: • **.** = (period) any single character (including a white space) • * = (asterisk) the sequences in a pattern (0 or more sequences) • **+** = (plus) the sequences in a pattern (1 or more sequences) • **?** = (question mark) sequences in a pattern (either 0 or 1 sequences). **You must enter an escape sequence (CTRL+v) prior to entering the ? regular expression.** • **[ ]** = (brackets) a range of single-character patterns. • **^** = (caret) the beginning of the input string. If the caret is used at the beginning of a sequence or range, it matches on everything BUT the characters specified. • **$** = (dollar sign) the end of the output string.

Command Modes EXEC

EXEC privilege

show ip bgp inconsistent-as

C-Series	No
E-Series	✓

View routes with inconsistent originating Autonomous System (AS) numbers, that is, prefixes that are announced from the same neighbor AS but with a different AS-Path.

Syntax **show ip bgp ipv4 multicast inconsistent-as**

Command Modes EXEC

EXEC privilege

show ip bgp ipv4 multicast neighbors

C-Series	No
E-Series	✓

Allows you to view the information exchanged by BGP neighbors.

Syntax **show ip bgp ipv4 multicast neighbors** [*ip-address* [**advertised-routes** | **dampened-routes** | **detail** | **flap-statistics** | **routes**]]

Parameters

ip-address	(OPTIONAL) Enter the IP address, in either IPv4 or IPv6 format, of the neighbor to view only BGP information exchanged with that neighbor.
advertised-routes	(OPTIONAL) Enter the keywords **advertised-routes** to view only the routes the neighbor sent.
dampened-routes	(OPTIONAL) Enter the keyword **dampened-routes** to view information on dampened routes from the BGP neighbor.
detail	(OPTIONAL) Display detailed neighbor information.

flap-statistics	(OPTIONAL) Enter the keyword **flap-statistics** to view flap statistics on the neighbor's routes.
routes	(OPTIONAL) Enter the keywords **routes** to view only the neighbor's feasible routes.

Command Modes

EXEC

EXEC privilege

Command History

Version 7.5.1.0	Modified: Added **detail** option; added information to output.

Example

```
Force10#show ip bgp ipv4 multicast neighbors
BGP neighbor is 25.25.25.25, remote AS 6400, internal link
  BGP version 4, remote router ID 25.25.25.25
  BGP state ESTABLISHED, in this state for 00:02:18
  Last read 00:00:16, hold time is 180, keepalive interval is 60 seconds
Received 1404 messages, 0 in queue
    3 opens, 1 notifications, 1394 updates
    6 keepalives, 0 route refresh requests
  Sent 48 messages, 0 in queue
    3 opens, 2 notifications, 0 updates
    43 keepalives, 0 route refresh requests
Minimum time between advertisement runs is 5 seconds
Minimum time before advertisements start is 0 seconds
  Capabilities received from neighbor for IPv4 unicast :
    MULTIPROTO_EXT(1)
    ROUTE_REFRESH(2)
    CISCO_ROUTE_REFRESH(128)
  Capabilities advertised to neighbor for IPv4 Multicast :
    MULTIPROTO_EXT(1)
    ROUTE_REFRESH(2)
    CISCO_ROUTE_REFRESH(128)
  Update source set to Loopback 0
  For address family: IPv4 Multicast
  BGP table version 14, neighbor version 14
  3 accepted prefixes consume 12 bytes
Prefixes accepted 1 (consume 4 bytes), withdrawn 0 by peer
  Prefixes advertised 0, rejected 0, withdrawn 0 from peer
Connections established 2; dropped 1
  Last reset 00:03:17, due to user reset

  Notification History
   'Connection Reset' Sent : 1  Recv: 0

Local host: 100.10.10.1, Local port: 179
Foreign host: 25.25.25.25, Foreign port: 2290

BGP neighbor is 211.1.1.129, remote AS 640, external link
  BGP version 4, remote router ID 0.0.0.0
  BGP state ACTIVE, in this state for 00:00:36
  Last read 00:00:41, hold time is 180, keepalive interval is 60 seconds
  Received 28 messages, 0 notifications, 0 in queue
  Sent 6 messages, 3 notifications, 0 in queue
  Received 18 updates, Sent 6 updates
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds

  For address family: IPv4 Multicast
  BGP table version 14, neighbor version 0
  0 accepted prefixes consume 0 bytes
  Prefix advertised 0, rejected 0, withdrawn 0

  Connections established 3; dropped 3
  Last reset 00:00:37, due to user reset

  Notification History
   'Connection Reset' Sent : 3  Recv: 0
```

Figure 358 show ip bgp neighbors Command Example

Figure 105 defines the information displayed in Figure 358.

Table 105 show ip bgp neighbors Command Fields

Lines beginning with	Description
BGP neighbor	Displays the BGP neighbor address and its AS number. The last phrase in the line indicates whether the link between the BGP router and its neighbor is an external or internal one. If they are located in the same AS, then the link is internal; otherwise the link is external.
BGP version	Displays the BGP version (always version 4) and the remote router ID.
BGP state	Displays the neighbor's BGP state and the amount of time in hours:minutes:seconds it has been in that state.
Last read	This line displays the following information: • last read is the time (hours:minutes:seconds) the router read a message from its neighbor • hold time is the number of seconds configured between messages from its neighbor • keepalive interval is the number of seconds between keepalive messages to help ensure that the TCP session is still alive.
Received messages	This line displays the number of BGP messages received, the number of notifications (error messages) and the number of messages waiting in a queue for processing.
Sent messages	The line displays the number of BGP messages sent, the number of notifications (error messages) and the number of messages waiting in a queue for processing.
Received updates	This line displays the number of BGP updates received and sent.
Minimum time	Displays the minimum time, in seconds, between advertisements.
(list of inbound and outbound policies)	Displays the policy commands configured and the names of the Route map, AS-PATH ACL or Prefix list configured for the policy.
For address family:	Displays IPv4 Unicast as the address family.
BGP table version	Displays the which version of the primary BGP routing table the router and the neighbor are using.
accepted prefixes	Displays the number of network prefixes accepted by the router and the amount of memory used to process those prefixes.
Prefix advertised	Displays the number of network prefixes advertised, the number rejected and the number withdrawn from the BGP routing table.
Connections established	Displays the number of TCP connections established and dropped between the two peers to exchange BGP information.
Last reset	Displays the amount of time since the peering session was last reset. Also states if the peer resets the peering session. If the peering session was never reset, the word never is displayed.

Table 105 show ip bgp neighbors Command Fields (continued)

Lines beginning with	Description
Local host:	Displays the peering address of the local router and the TCP port number.
Foreign host:	Displays the peering address of the neighbor and the TCP port number.

Related Commands

show ip bgp	View the current BGP routing table.

show ip bgp peer-group

C-Series	No
E-Series	✓

Allows you to view information on the BGP peers in a peer group.

Syntax **show ip bgp ipv4 multicast peer-group** [*peer-group-name* [**detail** | **summary**]]

Parameters

peer-group-name	(OPTIONAL) Enter the name of a peer group to view information about that peer group only.
detail	(OPTIONAL) Enter the keyword **detail** to view detailed status information of the peers in that peer group.
summary	(OPTIONAL) Enter the keyword **summary** to view status information of the peers in that peer group. The output is the same as that found in show ip bgp summary command

Command Modes

EXEC

EXEC privilege

Command History

Version 7.5.1.0	Modified: Added **detail** option.

Related Commands

neighbor peer-group (assigning peers)	Assign peer to a peer-group.
neighbor peer-group (creating group)	Create a peer group.
show ip bgp peer-group	View information on the BGP peers in a peer group.

show ip bgp summary

C-Series	No
E-Series	✓

Allows you to view the status of all BGP connections.

Syntax **show ip bgp ipv4 multicast summary**

Command Modes EXEC

EXEC privilege

Example

```
Force10#sho ip bgp ipv4 multicast summary
BGP router identifier 100.10.10.1, local AS number 6400
BGP table version is 14, main routing table version 14
7 network entrie(s) and 7 paths using 972 bytes of memory
2 BGP path attribute entrie(s) using 112 bytes of memory
1 BGP AS-PATH entrie(s) using 35 bytes of memory

Neighbor        AS     MsgRcvd  MsgSent     TblVer  InQ  OutQ Up/Down  State/Pfx

25.25.25.25     6400        21        9         14    0     0 00:02:04         3
211.1.1.129     640         28        6          0    0     0 00:00:21 Active
Force10#
```

Figure 359 show ip bgp summary Command Example

Table 106 defines the information displayed in Figure 359.

Table 106 show ip bgp summary Command Fields

Field	Description
BGP router identifier	Displays the local router ID and the AS number.
BGP table version	Displays the BGP table version and the main routing table version.
network entries	Displays the number of network entries and route paths and the amount of memory used to process those entries.
BGP path attribute entries	Displays the number of BGP path attributes and the amount of memory used to process them.
BGP AS-PATH entries	Displays the number of BGP AS_PATH attributes processed and the amount of memory used to process them.
BGP community entries	Displays the number of BGP COMMUNITY attributes processed and the amount of memory used to process them. The show ip bgp community command provides more details on the COMMUNITY attributes.
Dampening enabled	Displayed only when dampening is enabled. Displays the number of paths designated as history, dampened, or penalized.
Neighbor	Displays the BGP neighbor address.

Table 106 show ip bgp summary Command Fields

Field	Description
AS	Displays the AS number of the neighbor.
MsgRcvd	Displays the number of BGP messages that neighbor received.
MsgSent	Displays the number of BGP messages that neighbor sent.
TblVer	Displays the version of the BGP table that was sent to that neighbor.
InQ	Displays the number of messages from that neighbor waiting to be processed.
OutQ	Displays the number of messages waiting to be sent to that neighbor. If a number appears in parentheses, the number represents the number of messages waiting to be sent to the peer group.
Up/Down	Displays the amount of time (in hours:minutes:seconds) that the neighbor is in the Established stage. If the neighbor has never moved into the Established stage, the word never is displayed.
State/Pfx	If the neighbor is in Established stage, the number of network prefixes received. If a maximum limit was configured with the neighbor maximum-prefix command, (prfxd) appears in this column. If the neighbor is not in Established stage, the current stage is displayed (Idle, Connect, Active, OpenSent, OpenConfirm) When the peer is transitioning between states and clearing the routes received, the phrase (Purging) may appear in this column. If the neighbor is disabled, the phrase (Admin shut) appears in this column.

Chapter 43 IPv6 BGP

Platform Specific Feature: IPv6 BGP is supported on E-Series only.

FTOS support Border Gateway Protocol (BGP) and Multiprotocol Border Gateway Protocol (MBGP). This chapter contains the following sections:

- IPv6 BGP Commands on page 1127
- IPv6 MBGP Commands on page 1189

IPv6 BGP Commands

Border Gateway Protocol (BGP) is an external gateway protocol that transmits interdomain routing information within and between Autonomous Systems (AS). BGP version 4 (BGPv4) supports classless interdomain routing and the aggregation of routes and AS paths. Basically, two routers (called neighbors or peers) exchange information including full routing tables and periodically send messages to update those routing tables.

The following commands allow you to configure and enable BGP.

- aggregate-address on page 1129
- bgp always-compare-med on page 1131
- bgp bestpath as-path ignore on page 1131
- bgp bestpath med confed on page 1132
- bgp bestpath med misssing-as-best on page 1132
- bgp client-to-client reflection on page 1133
- bgp cluster-id on page 1133
- bgp confederation identifier on page 1134
- bgp confederation peers on page 1135
- bgp dampening on page 1136
- bgp default local-preference on page 1137

- bgp fast-external-fallover on page 1137
- bgp graceful-restart on page 1138
- bgp log-neighbor-changes on page 1139
- bgp non-deterministic-med on page 1139
- bgp router-id on page 1140
- capture bgp-pdu neighbor (ipv6) on page 1141
- capture bgp-pdu max-buffer-size on page 1141
- capture bgp-pdu max-buffer-size on page 1141
- clear ip bgp as-number on page 1143
- clear ip bgp ipv6-address on page 1144
- clear ip bgp peer-group on page 1145
- clear ip bgp ipv6 dampening on page 1145
- clear ip bgp ipv6 flap-statistics on page 1146
- debug ip bgp on page 1147
- debug ip bgp ipv6 dampening on page 1148
- debug ip bgp events on page 1148
- debug ip bgp keepalives on page 1149
- debug ip bgp notifications on page 1150
- debug ip bgp updates on page 1150
- default-metric on page 1151
- distance bgp on page 1152
- maximum-paths on page 1153
- neighbor activate on page 1153
- neighbor advertisement-interval on page 1154
- neighbor default-originate on page 1155
- neighbor description on page 1156
- neighbor distribute-list on page 1156
- neighbor ebgp-multihop on page 1157
- neighbor fall-over on page 1158
- neighbor filter-list on page 1159
- neighbor maximum-prefix on page 1159
- neighbor next-hop-self on page 1160
- neighbor password on page 1161
- neighbor peer-group (assigning peers) on page 1162
- neighbor peer-group (creating group) on page 1163
- neighbor peer-group passive on page 1164
- neighbor remote-as on page 1164
- neighbor remove-private-as on page 1165
- neighbor route-map on page 1166
- neighbor route-reflector-client on page 1167

- neighbor send-community on page 1168
- neighbor shutdown on page 1168
- neighbor subnet on page 1169
- neighbor timers on page 1170
- neighbor update-source on page 1171
- neighbor weight on page 1171
- network on page 1172
- network backdoor on page 1173
- redistribute on page 1174
- redistribute ospf on page 1175
- router bgp on page 1176
- show capture bgp-pdu neighbor (ipv6) on page 1176
- show config on page 1177
- show ip bgp ipv6 on page 1178
- show ip bgp cluster-list on page 1178
- show ip bgp community on page 1179
- show ip bgp community-list on page 1179
- show ip bgp dampened-paths on page 1180
- show ip bgp filter-list on page 1180
- show ip bgp ipv6 flap-statistics on page 1181
- show ip bgp inconsistent-as on page 1182
- show ip bgp neighbors on page 1182
- show ip bgp next-hop on page 1183
- show ip bgp paths on page 1184
- show ip bgp paths as-path on page 1185
- show ip bgp paths community on page 1185
- show ip bgp peer-group on page 1185
- show ip bgp regexp on page 1186
- show ip bgp summary on page 1187
- timers bgp on page 1188

aggregate-address

C-Series	No
E-Series	✓

Summarize a range of prefixes to minimize the number of entries in the routing table.

Syntax

aggregate-address *ipv6-address prefix-length* [**advertise-map** *map-name*] [**as-set**] [**attribute-map** *map-name*] [**summary-only**] [**suppress-map** *map-name*]

Parameters

ipv6-address prefix-length	Enter the IPv6 address in the **x:x:x:x::x** format followed by the prefix length in the **/x** format. Range: /0 to /128 The **::** notation specifies successive hexadecimal fields of zeros
advertise-map *map-name*	(OPTIONAL) Enter the keywords **advertise-map** followed by the name of a configured route map to set filters for advertising an aggregate route.
as-set	(OPTIONAL) Enter the keyword **as-set** to generate path attribute information and include it in the aggregate. AS_SET includes AS_PATH and community information from the routes included in the aggregated route.
attribute-map *map-name*	(OPTIONAL) Enter the keywords **attribute-map** followed by the name of a configured route map to modify attributes of the aggregate, excluding AS_PATH and NEXT_HOP attributes.
summary-only	(OPTIONAL) Enter the keyword **summary-only** to advertise only the aggregate address. Specific routes will not be advertised.
suppress-map *map-name*	(OPTIONAL) Enter the keywords **suppress-map** followed by the name of a configured route map to identify which more-specific routes in the aggregate are suppressed.

Defaults

Not configured.

Command Modes

ROUTER BGP (conf-router)

Command History

Version 7.4.1.0	Introduced

Usage Information

At least one of the routes included in the aggregate address must be in the BGP routing table for the configured aggregate to become active.

Do not add the **as-set** parameter to the aggregate, if routes within the aggregate are constantly changing as the aggregate will flap to keep track of the changes in the AS_PATH.

In route maps used in the **suppress-map** parameter, routes meeting the **deny** clause are not suppress; in other words, they are allowed. The opposite is true: routes meeting the **permit** clause are suppressed.

If the route is injected via the network command, that route will still appear in the routing table if the summary-only parameter is configured in the aggregate-address command.

The summary-only parameter suppresses all advertisements. If you want to suppress advertisements to only specific neighbors, use the neighbor distribute-list command.

In the show ip bgp ipv6 command, aggregates contain an ‘a’ in the first column and routes suppressed by the aggregate contain an ‘s’ in the first column.

bgp always-compare-med

C-Series	No
E-Series	✓

Allows you to enable comparison of the MULTI_EXIT_DISC (MED) attributes in the paths from different external ASs.

Syntax **bgp always-compare-med**

To disable comparison of MED, enter **no bgp always-compare-med**.

Defaults Disabled (that is, the software only compares MEDs from neighbors within the same AS).

Command Modes ROUTER BGP (conf-router)

Command History

Version 7.4.1.0	Introduced

Usage Information Any update without a MED attribute is the least preferred route.

If you enable this command, use the capture bgp-pdu max-buffer-size * command to recompute the best path.

bgp bestpath as-path ignore

C-Series	No
E-Series	✓

Ignore the AS PATH in BGP best path calculations.

Syntax **bgp bestpath as-path ignore**

To return to the default, enter **no bgp bestpath as-path ignore**.

Defaults Disabled (that is, the software considers the AS_PATH when choosing a route as best).

Command Modes ROUTER BGP (conf-router)

Command History

Version 7.4.1.0	Introduced

Usage Information If you enable this command, use the capture bgp-pdu max-buffer-size * command to recompute the best path.

bgp bestpath med confed

C-Series	No
E-Series	✓

Enable MULTI_EXIT_DISC (MED) attribute comparison on paths learned from BGP confederations.

Syntax **bgp bestpath med confed**

To disable MED comparison on BGP confederation paths, enter **no bgp bestpath med confed**.

Defaults Disabled.

Command Modes ROUTER BGP (conf-router)

Command History

Version 7.4.1.0	Introduced

Usage Information The software compares the MEDs only if the path contains no external autonomous system numbers.

If you enable this command, use the capture bgp-pdu max-buffer-size * command to recompute the best path.

bgp bestpath med misssing-as-best

C-Series	No
E-Series	✓

During path selection, indicate preference to paths with missing MED (MULTI_EXIT_DISC) over those paths with an advertised MED attribute.

Syntax **bgp bestpath med missing-as-best**

To return to the default selection, use the **no bgp bestpath med missing-as-best** command.

Defaults Disabled

Command Modes ROUTER BGP

Command History

Version 7.4.1.0	Introduced

Usage Information The MED is a 4-byte unsigned integer value and the default behavior is to assume a missing MED as 4294967295. This command causes a missing MED to be treated as 0. During the path selection, paths with a lower MED are preferred over those with a higher MED.

bgp client-to-client reflection

C-Series	No
E-Series	✓

Allows you to enable route reflection between clients in a cluster.

Syntax **bgp client-to-client reflection**

To disable client-to-client reflection, enter **no bgp client-to-client reflection**.

Defaults Enabled when a route reflector is configured.

Command Modes ROUTER BGP (conf-router)

Command History

Version 7.4.1.0	Introduced

Usage Information Route reflection to clients is not necessary if all client routers are fully meshed.

Related Commands

bgp cluster-id	Assign ID to a BGP cluster with two or more route reflectors.
neighbor route-reflector-client	Configure a route reflector and clients.

bgp cluster-id

C-Series	No
E-Series	✓

Assign a cluster ID to a BGP cluster with more than one route reflector.

Syntax **bgp cluster-id** {*ip-address* | *number*}

To delete a cluster ID, use the **no bgp cluster-id** {*ip-address* | *number*} command.

Parameters

ip-address	Enter an IP address as the route reflector cluster ID.
number	Enter a route reflector cluster ID as a number from 1 to 4294967295.

Defaults Not configured.

Command Modes ROUTER BGP (conf-router)

Command History

Version 7.4.1.0	Introduced

Usage Information When a BGP cluster contains only one route reflector, the cluster ID is the route reflector's router ID. For redundancy, a BGP cluster may contain two or more route reflectors and you assign a cluster ID with the bgp cluster-id command. Without a cluster ID, the route reflector cannot recognize route updates from the other route reflectors within the cluster.

The default format for displaying the cluster-id is dotted decimal, but if you enter the cluster-id as an integer, it will be displayed as an integer.

Related Commands

bgp client-to-client reflection	Enable route reflection between route reflector and clients.
neighbor route-reflector-client	Configure a route reflector and clients.
show ip bgp cluster-list	View paths with a cluster ID.

bgp confederation identifier

C-Series	**No**
E-Series	✔

Configure an identifier for a BGP confederation.

Syntax **bgp confederation identifier** *as-number*

To delete a BGP confederation identifier, use the **no bgp confederation identifier** *as-number* command.

Parameters

as-number	Enter the AS number. Range: 1 to 65535

Defaults Not configured.

Command Modes ROUTER BGP (conf-router)

Command History

Version 7.4.1.0	Introduced

Usage Information

The autonomous systems configured in this command are visible to the EBGP neighbors. Each autonomous system is fully meshed and contains a few connections to other autonomous systems. The next hop, MED, and local preference information is preserved throughout the confederation.

FTOS accepts confederation EBGP peers without a LOCAL_PREF attribute. The software sends AS_CONFED_SET and accepts AS_CONFED_SET and AS_CONF_SEQ.

bgp confederation peers

C-Series	**No**
E-Series	✔

Specify the Autonomous Systems (ASs) that belong to the BGP confederation.

Syntax

bgp confederation peers *as-number* [*...as-number*]

To enter no bgp confederation peer.

Parameters

as-number	Enter the AS number. Range: 1 to 65535
...as-number	(OPTIONAL) Enter up to 16 confederation numbers. Range: 1 to 65535.

Defaults

Not configured.

Command Modes

ROUTER BGP (conf-router)

Command History

Version 7.4.1.0	Introduced

Usage Information

The Autonomous Systems configured in this command are visible to the EBGP neighbors. Each Autonomous System is fully meshed and contains a few connections to other Autonomous Systems.

After specifying autonomous systems numbers for the BGP confederation, recycle the peers to update their configuration.

Related Commands

bgp confederation identifier	Configure a confederation ID.

bgp dampening

C-Series	No
E-Series	✓

Enable BGP route dampening and configure the dampening parameters.

Syntax

bgp dampening [*half-life reuse suppress max-suppress-time*] [**route-map** *map-name*]

To disable route dampening, use the **no bgp dampening** [*half-life reuse suppress max-suppress-time*] [**route-map** *map-name*] command.

Parameters

half-life	(OPTIONAL) Enter the number of minutes after which the Penalty is decreased. After the router assigns a Penalty of 1024 to a route, the Penalty is decreased by half after the half-life period expires. Range: 1 to 45. Default: 15 minutes
reuse	(OPTIONAL) Enter a number as the reuse value, which is compared to the flapping route's Penalty value. If the Penalty value is less than the reuse value, the flapping route is once again advertised (or no longer suppressed). Range: 1 to 20000. Default: 750
suppress	(OPTIONAL) Enter a number as the suppress value, which is compared to the flapping route's Penalty value. If the Penalty value is greater than the suppress value, the flapping route is no longer advertised (that is, it is suppressed). Range: 1 to 20000. Default: 2000
max-suppress-time	(OPTIONAL) Enter the maximum number of minutes a route can be suppressed. The default is four times the half-life value. Range: 1 to 255. Default: 60 minutes.
route-map *map-name*	(OPTIONAL) Enter the keyword **route-map** followed by the name of a configured route map. Only match commands in the configured route map are supported.

Defaults

Disabled.

Command Modes

ROUTER BGP (conf-router)

Command History

Version 7.4.1.0	Introduced

Usage Information

If you enter **bgp dampening**, the default values for *half-life*, *reuse*, *suppress*, and *max-suppress-time* are applied. The parameters are position-dependent, therefore, if you configure one parameter, you must configure the parameters in the order they appear in the command.

Related Commands		
	show ip bgp dampened-paths	View the BGP paths

bgp default local-preference

C-Series	No
E-Series	✓

Change the default local preference value for routes exchanged between internal BGP peers.

Syntax **bgp default local-preference** *value*

To return to the default value, enter **no bgp default local-preference**.

Parameters

value	Enter a number to assign to routes as the degree of preference for those routes. When routes are compared, the higher the degree of preference or local preference value, the more the route is preferred. Range: 0 to 4294967295 Default: 100

Defaults 100

Command Modes ROUTER BGP (conf-router)

Command History

Version 7.4.1.0	Introduced

Usage Information The bgp default local-preference command setting is applied by all routers within the AS.

bgp fast-external-fallover

C-Series	No
E-Series	✓

Enable the fast external fallover feature, which immediately resets the BGP session if a link to a directly connected external peer fails.

Syntax **bgp fast-external-fallover**

To disable fast external fallover, enter **no bgp fast-external-fallover**.

Defaults Enabled

Command Modes ROUTER BGP (conf-router)

Command History

Version 7.4.1.0	Introduced

Usage Information The bgp fast-external-fallover command appears in the show config command output.

bgp graceful-restart

C-Series	No
E-Series	✔

Enable graceful restart on a BGP neighbor, a BGP node, or designate a local router to support graceful restart as a receiver only.

Syntax **bgp graceful-restart** [**neighbor** *ip-addres* | *peer-group-name*] [**restart-time** *seconds*] [**stale-path-time** *seconds*] [**role receiver-only**]

To return to the default, enter the **no bgp graceful-restart** command.

Parameters

neighbor *ip-address* | *peer-group-name*	Enter the keyword **neighbor** followed by one of the options listed below: • *ip-address* of the neighbor in IP address format of the neighbor • *peer-group-name* of the neighbor peer group.
restart-time *seconds*	Enter the keyword **restart-time** followed by the maximum number of seconds needed to restart and bring up all peers. Range: 1 to 3600 seconds Default: 120 seconds
stale-path-time *seconds*	Enter the keyword **stale-path-time** followed by the maximum number of seconds to wait before restarting a peer's stale paths. Default: 360 seconds.
role receiver-only	Enter the keyword **role receiver-only** to designate the local router to support graceful restart as a receiver only.

Defaults as above

Command Modes ROUTER BGP (conf-router)

Command History

Version 7.4.1.0	Introduced

Usage Information This feature is advertised to BGP neighbors through a capability advertisement. In receiver only mode, BGP saves the advertised routes of peers that support this capability when they restart.

bgp log-neighbor-changes

C-Series	No
E-Series	✓

Enable logging of BGP neighbor resets.

Syntax **bgp log-neighbor-changes**

To disable logging, enter **no bgp log-neighbor-changes**.

Defaults Enabled

Command Modes ROUTER BGP (conf-router)

Command History

Version 7.4.1.0	Introduced

Usage Information The bgp log-neighbor-changes command appears in the show config command output.

Related Commands

show config	View the current configuration

bgp non-deterministic-med

C-Series	No
E-Series	✓

Compare MEDs of paths from different Autonomous Systems.

Syntax **bgp non-deterministic-med**

To return to the default, enter **no bgp non-deterministic-med**.

Defaults Disabled (that is, paths/routes for the same destination but from different ASs will not have their MEDs compared).

Command Modes ROUTER BGP (conf-router)

Command History

Version 7.4.1.0	Introduced

Usage Information In non-deterministic mode, paths are compared in the order in which they arrive. This method can lead to FTOS choosing different best paths from a set of paths, depending on the order in which they are received from the neighbors since MED may or may not get compared between adjacent paths. In deterministic mode (**no bgp non-deterministic-med)**, FTOS compares MED between adjacent paths within an AS group since all paths in the AS group are from the same AS.

When you change the path selection from deterministic to non-deterministic, the path selection for existing paths remains deterministic until you enter capture bgp-pdu max-buffer-size command to clear existing paths.

bgp router-id

C-Series	**No**
E-Series	✓

Assign a user-given ID to a BGP router.

Syntax **bgp router-id** *ip-address*

To delete a user-assigned IP address, enter **no bgp router-id**.

Parameters

ip-address	Enter an IP address in dotted decimal format to reset only that BGP neighbor.

Defaults The router ID is the highest IP address of the Loopback interface or, if no Loopback interfaces are configured, the highest IP address of a physical interface on the router.

Command Modes ROUTER BGP (conf-router)

Command History

Version 7.4.1.0	Introduced

Usage Information Peering sessions are reset when you change the router ID of a BGP router.

capture bgp-pdu neighbor (ipv6)

C-Series	No
E-Series	✓

Enable capture of an IPv6 BGP neighbor packet.

Syntax

capture bgp-pdu neighbor *ipv6-address* **direction** {**both** | **rx** | **tx**}

To disable capture of the IPv6 BGP neighbor packet, use the **no capture bgp-pdu neighbor** *ipv6-address* command.

Parameters

ipv6-address	Enter the IPv6 address of the target BGP neighbor.
direction {**both** | **rx** | **tx**}	Enter the keyword **direction** and a direction— either **rx** for inbound, **tx** for outbound, or **both**.

Defaults

Not configured.

Command Modes

EXEC; EXEC privilege

Command History

Version 7.5.1.0	Introduced

Related Commands

capture bgp-pdu max-buffer-size	Enable route reflection between route reflector and clients.
show capture bgp-pdu neighbor (ipv6)	Configure a route reflector and clients.
capture bgp-pdu neighbor (ipv4)	Enable capture of an IPv4 BGP neighbor packet.

capture bgp-pdu max-buffer-size

C-Series	No
E-Series	✓

Set the size of the BGP packet capture buffer. This buffer size pertains to both IPv4 and IPv6 addresses.

Syntax

capture bgp-pdu max-buffer-size *100-102400000*

Parameters

100-102400000	Enter a size for the capture buffer.

Defaults

40960000 bytes

Command Modes

EXEC; EXEC privilege

Command History

Version 7.5.1.0	Introduced

Related Commands

capture bgp-pdu neighbor (ipv6)	Enable capture of an IPv6 BGP neighbor packet.
show capture bgp-pdu neighbor (ipv6)	Configure a route reflector and clients.

clear ip bgp * (asterisk)

C-Series	**No**
E-Series	✓

Reset all BGP sessions in the specified category on the E-Series. The soft parameter (BGP Soft Reconfiguration) clears the policies without resetting the TCP connection.

Syntax **clear ip bgp** * [**ipv4 multicast soft** [**in** | **out**] | **ipv6 unicast soft** [**in** | **out**] | **soft** [**in** | **out**]]

Parameters

*	Enter an asterisk (*) to reset all BGP sessions.
ipv4 multicast soft [**in**	**out**]	(OPTIONAL) This keyword sequence sets options within the a specified IPv4 address family.
ipv6 unicast soft [**in**	**out**]	(OPTIONAL) This keyword sequence sets options within the a specified IPv6 address family.
soft	(OPTIONAL) Enter the keyword **soft** to configure and activate policies without resetting the BGP TCP session, that is, BGP Soft Reconfiguration. **Note:** If you enter **clear ip bgp** *ip6-address* **soft**, both inbound and outbound policies are reset.
in	(OPTIONAL) Enter the keyword **in** to activate only inbound policies.
out	(OPTIONAL) Enter the keyword **out** to activate only outbound policies.

Command Modes EXEC privilege

Command History

Version 7.4.1.0	Introduced

clear ip bgp as-number

C-Series	No
E-Series	✓

Reset BGP sessions on the E-Series. The soft parameter (BGP Soft Reconfiguration) clears the policies without resetting the TCP connection.

Syntax **clear ip bgp** *as-number* [**flap-statistics | ipv4 {multicast {flap-statistics | soft {in | out}} | unicast {flap-statistics | soft {in | out}} | ipv6 unicast {flap-statistics | soft {in | out}| soft** [**in** | **out**]

Parameters

as-number	Enter an autonomous system (AS) number to reset neighbors belonging to that AS. If used without a qualifier, the keyword resets all neighbors belonging to that AS. Range: 1 to 65535
flap-statistics	(OPTIONAL) Enter the keyword **flap-statistics** to clear all flap statistics belonging to that AS or a specified address family within that AS.
ipv4	(OPTIONAL) Enter the keyword **ipv4** to select options for that address family.
ipv6	(OPTIONAL) Enter the keyword **ipv6** to select options for that address family.
unicast	(OPTIONAL) Enter the keyword **unicast** to select the unicast option within the selected address family.
multicast	(OPTIONAL) Enter the keyword **multicast** to select the multicast option within the selected address family.
soft	(OPTIONAL) Enter the keyword **soft** to configure and activate policies without resetting the BGP TCP session, that is, BGP Soft Reconfiguration. **Note:** If you enter **clear ip bgp** *ip6-address* **soft**, both inbound and outbound policies are reset.
in	(OPTIONAL) Enter the keyword **in** to activate only inbound policies.
out	(OPTIONAL) Enter the keyword **out** to activate only outbound policies.

Command Modes EXEC privilege

Command History

Version 7.4.1.0	Introduced

clear ip bgp ipv6-address

C-Series	No
E-Series	✓

Reset BGP sessions specific to an IPv6 address on the E-Series. The soft parameter (BGP Soft Reconfiguration) clears the policies without resetting the TCP connection.

Syntax **clear ip bgp** *ipv6-address* [**flap-statistics | ipv4 {multicast {flap-statistics | soft {in | out}} | unicast {flap-statistics | soft {in | out}} | ipv6 unicast {flap-statistics | soft {in | out}| soft** [**in** | **out**]

Parameters

ipv6-address	Enter an IPv6 address to reset neighbors belonging to that IP. Used without a qualifier, the keyword resets all neighbors belonging to that IP.
flap-statistics	(OPTIONAL) Enter the keyword **flap-statistics** to clear all flap statistics belonging to that AS or a specified address family within that IP.
ipv4	(OPTIONAL) Enter the keyword **ipv4** to select options for that address family.
ipv6	(OPTIONAL) Enter the keyword **ipv6** to select options for that address family.
unicast	(OPTIONAL) Enter the keyword **unicast** to select the unicast option within the selected address family.
multicast	(OPTIONAL) Enter the keyword **multicast** to select the multicast option within the selected address family.
soft	(OPTIONAL) Enter the keyword **soft** to configure and activate policies without resetting the BGP TCP session, that is, BGP Soft Reconfiguration. **Note:** If you enter **clear ip bgp** *ip6-address* **soft**, both inbound and outbound policies are reset.
in	(OPTIONAL) Enter the keyword **in** to activate only inbound policies.
out	(OPTIONAL) Enter the keyword **out** to activate only outbound policies.

Command Modes EXEC privilege

Command History

Version 7.4.1.0	Introduced

clear ip bgp peer-group

C-Series	No
E-Series	✓

Reset a peer-group's BGP sessions.

Syntax **clear ip bgp peer-group** *peer-group-name*

Parameters

peer-group-name	Enter the peer group name to reset the BGP sessions within that peer group.

Command Modes EXEC privilege

Command History

Version 7.4.1.0	Introduced

clear ip bgp ipv6 dampening

C-Series	No
E-Series	✓

Clear information on route dampening and return suppressed route to active state.

Syntax **clear ip bgp ipv6 unicast dampening** [*ipv6-address*]

Parameters

ipv6-address	Enter the IPv6 address in the **x:x:x:x::x** format followed by the prefix length in the **/x** format. Range: /0 to /128 The **::** notation specifies successive hexadecimal fields of zeros

Command Modes EXEC privilege

Command History

Version 7.4.1.0	Introduced

Usage Information After you enter this command, the software deletes history routes and returns suppressed routes to active state.

clear ip bgp ipv6 flap-statistics

C-Series	No
E-Series	✓

Clear BGP flap statistics, which includes number of flaps and the time of the last flap.

Syntax

clear ip bgp ipv6 unicast flap-statistics [*ipv6-address* | **filter-list** *as-path-name* | **regexp** *regular-expression*]

Parameters

ipv6-address	(OPTIONAL) Enter the IPv6 address in the **x:x:x:x::x** format followed by the prefix length in the **/x** format. Range: /0 to /128 The **::** notation specifies successive hexadecimal fields of zeros
filter-list *as-path-name*	(OPTIONAL) Enter the keyword **filter-list** followed by the name of a configured AS-PATH list.
regexp *regular-expression*	(OPTIONAL) Enter the keyword **regexp** followed by regular expressions. Use one or a combination of the following: . (period) matches on any single character, including white space * (asterisk) matches on sequences in a pattern (zero or more sequences) + (plus sign) matches on sequences in a pattern (one or more sequences) ? (question mark) matches sequences in a pattern (0 or 1 sequences) [ ] (brackets) matches a range of single-character patterns. ^ (caret) matches the beginning of the input string. (If the caret is used at the beginning of a sequence or range, it matches on everything BUT the characters specified.) $ (dollar sign) matches the end of the output string.

Command Modes

EXEC privilege

Command History

Version 7.4.1.0	Introduced

Usage Information

If you enter clear ip bgp ipv6 flap-statistics without any parameters, all statistics are cleared.

Related Commands

show ip bgp ipv6 flap-statistics	View BGP flap statistics.

debug ip bgp

C-Series	No
E-Series	✓

Allows you to view all information on BGP, including BGP events, keepalives, notifications, and updates.

Syntax

debug ip bgp [*ipv6-address* | **peer-group** *peer-group-name*] [**in** | **out**]

To disable all BGP debugging, enter **no debug ip bgp**.

Parameters

ipv6-address	(OPTIONAL) Enter the IPv6 address in the **x:x:x:x::x** format followed by the prefix length in the **/x** format. Range: /0 to /128 The **::** notation specifies successive hexadecimal fields of zeros.
peer-group *peer-group-name*	Enter the keyword **peer-group** followed by the name of the peer group.
in	(OPTIONAL) Enter the keyword **in** to view only information on inbound BGP routes.
out	(OPTIONAL) Enter the keyword **out** to view only information on outbound BGP routes.

Command Modes

EXEC privilege

Command History

Version 7.4.1.0	Introduced

Usage Information

To view information on both incoming and outgoing routes, do not include the **in** and **out** parameters in the debugging command. The **in** and **out** parameters cancel each other; for example, if you enter **debug ip bgp in** and then enter **debug ip bgp out**, you will not see information on the incoming routes.

Entering a no debug ip bgp command removes all configured debug commands for BGP.

Related Commands

debug ip bgp events	View information about BGP events.
debug ip bgp keepalives	View information about BGP keepalives.
debug ip bgp notifications	View information about BGP notifications.
debug ip bgp updates	View information about BGP updates.

debug ip bgp ipv6 dampening

C-Series	No
E-Series	✓

View information on IPv6 routes being dampened.

Syntax **debug ip bgp ipv6 unicast dampening** [**in** | **out**]

To disable debugging, enter **no debug ip bgp ipv6 unicast dampening**.

Parameters

in	(OPTIONAL) Enter the keyword **in** to view only inbound dampened routes.
out	(OPTIONAL) Enter the keyword **out** to view only outbound dampened routes.

Command Modes EXEC privilege

Command History

Version 7.4.1.0	Introduced

Usage Information Enter no debug ip bgp command to remove all configured debug commands for BGP.

Related Commands

show ip bgp dampened-paths	View BGP dampened routes.

debug ip bgp events

C-Series	No
E-Series	✓

Allows you to view information on local BGP state changes and other BGP events.

Syntax **debug ip bgp** [*ipv6-address* | **peer-group** *peer-group-name*] **events** [**in** | **out**]

To disable debugging, use the **no debug ip bgp** *ipv6-address* | **peer-group** *peer-group-name*] **events** command.

Parameters

ipv6-address	(OPTIONAL) Enter the IPv6 address in the **x:x:x:x::x** format followed by the prefix length in the **/x** format. Range: /0 to /128 The **::** notation specifies successive hexadecimal fields of zeros.
peer-group *peer-group-name*	(OPTIONAL) Enter the keyword **peer-group** followed by the name of the peer group.

in	(OPTIONAL) Enter the keyword **in** to view only events on inbound BGP messages.
out	(OPTIONAL) Enter the keyword **out** to view only events on outbound BGP messages.

Command Modes EXEC privilege

Command History

Version 7.4.1.0	Introduced

Usage Information Enter the no debug ip bgp command to remove all configured debug commands for BGP.

debug ip bgp keepalives

C-Series	No
E-Series	✓

Allows you to view information about BGP keepalive messages.

Syntax **debug ip bgp** [*ipv6-address* | **peer-group** *peer-group-name*] **keepalives** [**in** | **out**]

To disable debugging, use the **no debug ip bgp** [*ip-address* | **peer-group** *peer-group-name*] **keepalives** [**in** | **out**] command.

Parameters

ipv6-address	(OPTIONAL) Enter the IPv6 address in the **x:x:x:x::x** format followed by the prefix length in the **/x** format. Range: /0 to /128 The **::** notation specifies successive hexadecimal fields of zeros.
peer-group *peer-group-name*	(OPTIONAL) Enter the keyword **peer-group** followed by the name of the peer group.
in	(OPTIONAL) Enter the keyword **in** to view only inbound keepalive messages.
out	(OPTIONAL) Enter the keyword **out** to view only outbound keepalive messages.

Command Modes EXEC privilege

Command History

Version 7.4.1.0	Introduced

Usage Information Enter the no debug ip bgp command to remove all configured debug commands for BGP.

debug ip bgp notifications

C-Series	No
E-Series	✓

Allows you to view information about BGP notifications received from neighbors.

Syntax **debug ip bgp** [*ipv6-address* | **peer-group** *peer-group-name*] **notifications** [**in** | **out**]

To disable debugging, use the **no debug ip bgp** [*ip-address* | **peer-group** *peer-group-name*] **notifications** [**in** | **out**] command.

Parameters

ipv6-address	(OPTIONAL) Enter the IPv6 address in the **x:x:x:x::x** format followed by the prefix length in the **/x** format. Range: /0 to /128 The **::** notation specifies successive hexadecimal fields of zeros.
peer-group *peer-group-name*	(OPTIONAL) Enter the keyword **peer-group** followed by the name of the peer group.
in	(OPTIONAL) Enter the keyword **in** to view BGP notifications received from neighbors.
out	(OPTIONAL) Enter the keyword **out** to view BGP notifications sent to neighbors.

Command Modes EXEC privilege

Command History

Version 7.4.1.0	Introduced

Usage Information Enter the no debug ip bgp command to remove all configured debug commands for BGP.

debug ip bgp updates

C-Series	No
E-Series	✓

Allows you to view information about BGP updates.

Syntax **debug ip bgp** [*ipv6-address* | **peer-group** *peer-group-name* | **ipv6 unicast** [*ipv6-address*]] **updates** [**in** | **out** | **prefix-list** *prefix-list-name*]

To disable debugging, use the **no debug ip bgp** [*ip-address* | **peer-group** *peer-group-name* | **ipv6 unicast** [*ipv6-address*]] **updates** [**in** | **out**] command.

Parameters

ipv6-address	(OPTIONAL) Enter the IPv6 address in the **x:x:x:x::x** format followed by the prefix length in the **/x** format. Range: /0 to /128 The **::** notation specifies successive hexadecimal fields of zeros.
peer-group *peer-group-name*	(OPTIONAL) Enter the keyword **peer-group** followed by the name of the peer group.
ipv6 unicast [*ipv6-address*]	(OPTIONAL) Enter the keyword **ipv6 unicast**, and, optionally, an ipv6 address.
in	(OPTIONAL) Enter the keyword **in** to view only BGP updates received from neighbors.
out	(OPTIONAL) Enter the keyword **out** to view only BGP updates sent to neighbors.

Command Modes EXEC privilege

Command History

Version 7.4.1.0	Introduced

Usage Information Enter the no debug ip bgp command to remove all configured debug commands for BGP.

default-metric

C-Series	**No**
E-Series	✓

Allows you to change the metrics of redistributed routes to locally originated routes. Use this command with the redistribute command.

Syntax **default-metric** *number*

To return to the default setting, enter **no default-metric**.

Parameters

number	Enter a number as the metric to be assigned to routes from other protocols. Range: 1 to 4294967295.

Defaults 0

Command Modes ROUTER BGP (conf-router)

Command History

Version 7.4.1.0	Introduced

Usage Information

The default-metric command in BGP sets the value of the BGP MULTI_EXIT_DISC (MED) attribute for redistributed routes only.

Related Commands

bgp always-compare-med	Enable comparison of all BGP MED attributes.
redistribute	Redistribute routes from other routing protocols into BGP.

distance bgp

C-Series	**No**
E-Series	✓

Configure three administrative distances for routes.

Syntax

distance bgp *external-distance internal-distance local-distance*

To return to default values, enter **no distance bgp**.

Parameters

external-distance	Enter a number to assign to routes learned from a neighbor external to the AS. Range: 1 to 255. Default: 20
internal-distance	Enter a number to assign to routes learned from a router within the AS. Range: 1 to 255. Default: 200
local-distance	Enter a number to assign to routes learned from networks listed in the network command. Range: 1 to 255. Default: 200

Defaults

external-distance = 20; *internal-distance* = 200; *local-distance* = 200.

Command Modes

ADDRESS FAMILY (conf-router_bgpv6_af)

Command History

Version 7.4.1.0	Introduced

Caution: Force10 Networks recommends that you do not change the administrative distance of internal routes. Changing the administrative distances may cause routing table inconsistencies.

Usage Information

The higher the administrative distance assigned to a route means that your confidence in that route is low. Routes assigned an administrative distance of 255 are not installed in the routing table.

Routes from confederations are treated as internal BGP routes.

maximum-paths

C-Series	No
E-Series	✓

Configure the maximum number of parallel routes (multipath support) BGP supports.

Syntax **maximum-paths** {**ebgp** | **ibgp**} *number*

To return to the default values, enter **no maximum-paths**.

Parameters

ebgp	Enter the keyword **ebgp** to enable multipath support for External BGP routes.
ibgp	Enter the keyword **ibgp** to enable multipath support for Internal BGP routes.
number	Enter a number as the maximum number of parallel paths. Range: 1 to 16 Default: 1

Defaults 1

Command Modes ADDRESS FAMILY (conf-router_bgpv6_af)

Command History

Version 7.4.1.0	Introduced

Usage Information If you enable this command, use the capture bgp-pdu max-buffer-size command to recompute the best path.

neighbor activate

C-Series	No
E-Series	✓

This command allows the specified neighbor/peer group to be enabled for the current AFI/SAFI.

Syntax **neighbor** {*ipv6-address* | *peer-group-name*} **activate**

To disable, use the **no neighbor** {*ipv6-address* | *peer-group-name*} **activate** command.

Parameters

ipv6-address	Enter the IPv6 address in the **x:x:x:x::x** format. The **::** notation specifies successive hexadecimal fields of zeros.
peer-group-name	Identify a peer group by name.
activate	Enter the keyword **activate** to enable the identified neighbor or peer group in the new AFI/SAFI.

Defaults Disabled

Command Modes ADDRESS FAMILY (conf-router_bgpv6_af)

Command History

Version 7.4.1.0	Introduced

Usage Information By default, when a neighbor/peer group configuration is created in the Router BGP context, it is enabled for the IPv6/Unicast AFI/SAFI. By using **activate** in the new context, the neighbor/peer group is enabled for AFI/SAFI.

neighbor advertisement-interval

C-Series	**No**
E-Series	✓

Set the advertisement interval between BGP neighbors or within a BGP peer group.

Syntax **neighbor** {*ipv6-address* | *peer-group-name*} **advertisement-interval** *seconds*

To return to the default value, use the **no neighbor** {*ipv6-address* | *peer-group-name*} **advertisement-interval** command.

Parameters

ipv6-address	Enter the IPv6 address in the **x:x:x:x::x** format. The **::** notation specifies successive hexadecimal fields of zeros.
peer-group-name	Enter the name of the peer group to set the advertisement interval for all routers in the peer group.
seconds	Enter a number as the time interval, in seconds, between BGP advertisements. Range: 0 to 600 seconds. Default: 5 seconds for internal BGP peers; 30 seconds for external BGP peers.

Defaults *seconds* = 5 seconds (internal peers); *seconds* = 30 seconds (external peers)

Command Modes ADDRESS FAMILY (conf-router_bgpv6_af)

Command History

Version 7.4.1.0	Introduced

neighbor default-originate

C-Series	No
E-Series	✓

Inject the default route to a BGP peer or neighbor.

Syntax

neighbor {*ipv6-address* | *peer-group-name*} **default-originate** [**route-map** *map-name*]

To remove a default route, use the **no neighbor** {*ipv6-address* | *peer-group-name*} **default-originate** [**route-map** *map-name*] command.

Parameters

ipv6-address	Enter the IPv6 address in the **x:x:x:x::x** format. The **::** notation specifies successive hexadecimal fields of zeros.
peer-group-name	Enter the name of the peer group to set the default route of all routers in that peer group.
route-map *map-name*	(OPTIONAL) Enter the keyword **route-map** followed by the name of a configured route map.

Defaults

Not configured.

Command Modes

ADDRESS FAMILY (conf-router_bgpv6_af)

Command History

Version 7.4.1.0	Introduced

Usage Information

If you apply a route map to a BGP peer or neighbor with the neighbor default-originate command configured, the software does not apply the set filters in the route map to that BGP peer or neighbor.

neighbor description

C-Series	No
E-Series	✓

Assign a character string describing the neighbor or group of neighbors (peer group).

Syntax **neighbor** {*ipv6-address* | *peer-group-name*} **description** *text*

To delete a description, use the **no neighbor** {*ipv6-address* | *peer-group-name*} **description** *text* command.

Parameters

ipv6-address	Enter the IPv6 address in the **x:x:x:x::x** format. The **::** notation specifies successive hexadecimal fields of zeros.
peer-group-name	Enter the name of the peer group.
text	Enter a continuous text string up to 80 characters.

Defaults Not configured.

Command Modes ROUTER BGP (conf-router)

Command History

Version 7.4.1.0	Introduced

neighbor distribute-list

C-Series	No
E-Series	✓

Distribute BGP information via an established prefix list.

Syntax **neighbor** {*ipv6-address* | *peer-group-name*} **distribute-list** *prefix-list-name* {**in** | **out**}

To delete a neighbor distribution list, use the **no neighbor** {*ipv6-address* | *peer-group-name*} **distribute-list** *prefix-list-name* {**in** | **out**} command.

Parameters

ipv6-address	Enter the IPv6 address in the **x:x:x:x::x** format. The **::** notation specifies successive hexadecimal fields of zeros.
peer-group-name	Enter the name of the peer group.
prefix-list-name	Enter the name of an established prefix list. If the prefix list is not configured, the default is permit (to allow all routes).

in	Enter the keyword **in** to distribute only inbound traffic.
out	Enter the keyword **out** to distribute only outbound traffic.

Defaults Not configured.

Command Modes ADDRESS FAMILY (conf-router_bgpv6_af)

Command History

Version 7.4.1.0	Introduced

Usage Information Other BGP filtering commands include: neighbor filter-list and neighbor route-map.

Related Commands

neighbor filter-list	Assign a AS-PATH list to a neighbor or peer group.
neighbor route-map	Assign a route map to a neighbor or peer group.

neighbor ebgp-multihop

C-Series	**No**
E-Series	✓

Attempt and accept BGP connections to external peers on networks that are not directly connected.

Syntax **neighbor** {*ipv6-address* | *peer-group-name*} **ebgp-multihop** [*ttl*]

To disallow and disconnect connections, use the **no neighbor** {*ipv6-address* | *peer-group-name*} **ebgp-multihop** [*ttl*] command.

Parameters

ipv6-address	Enter the IPv6 address in the **x:x:x:x::x** format. The **::** notation specifies successive hexadecimal fields of zeros.
peer-group-name	Enter the name of the peer group.
ttl	(OPTIONAL) Enter the number of hops as the Time to Live (ttl) value. Range: 1 to 255. Default: 255

Defaults Disabled.

Command Modes ROUTER BGP (conf-router)

Command History

Version 7.4.1.0	Introduced

Usage Information

To prevent loops, the neighbor ebgp-multihop command will not install default routes of the multihop peer. Networks not directly connected are not considered valid for best path selection.

neighbor fall-over

C-Series	No
E-Series	✓

Enable or disable fast fall-over for BGP neighbors.

Syntax

neighbor {*ipv6-address* | *peer-group-name*} **fall-over**

To disable, use the **no neighbor** {*ipv6-address* | *peer-group-name*} **fall-over** command.

Parameters

ipv6-address	Enter the IPv6 address in the **x:x:x:x::x** format. The **::** notation specifies successive hexadecimal fields of zeros.
peer-group-name	Enter the name of the peer group.

Defaults

Disabled

Command Modes

ROUTER BGP (conf-router)

Command History

Version 7.4.1.0	Introduced

Usage Information

When fall-over is enabled, BGP keeps track of IP or IPv6 reachability to the peer remote address and the peer local address. Whenever either address becomes unreachable (i.e, no active route exists in the routing table for peer IP or IPv6 destination/local address), BGP brings down the session with the peer.

Related Commands

show ip bgp neighbors	Display information on the BGP neighbors

neighbor filter-list

C-Series	No
E-Series	✓

Configure a BGP filter based on the AS-PATH attribute.

Syntax **neighbor** {*ipv6-address* | *peer-group-name*} **filter-list** *as-path-name* {**in** | **out**}

To delete a BGP filter, use the **no neighbor** {*ipv6-address* | *peer-group-name*} **filter-list** *as-path-name* {**in** | **out**} command.

Parameters

ipv6-address	Enter the IPv6 address in the **x:x:x:x::x** format. The **::** notation specifies successive hexadecimal fields of zeros.
peer-group-name	Enter the name of the peer group to apply the filter to all routers in the peer group.
as-path-name	Enter the name of an established AS-PATH access list. If the AS-PATH access list is not configured, the default is permit (to allow routes). (16 characters maximum)
in	Enter the keyword **in** to filter inbound BGP routes.
out	Enter the keyword **out** to filter outbound BGP routes.

Defaults Not configured.

Command Modes ADDRESS FAMILY (conf-router_bgpv6_af)

Command History

Version 7.4.1.0	Introduced

neighbor maximum-prefix

C-Series	No
E-Series	✓

Control the number of network prefixes received.

Syntax **neighbor** {*ipv6-address* | *peer-group-name*} **maximum-prefix** *maximum* [*threshold*] [**warning-only**]

To return to the default values, use the **no neighbor** {*ipv6-address* | *peer-group-name*} **maximum-prefix** *maximum* [*threshold*] [**warning-only**] command.

Parameters

ipv6-address	Enter the IPv6 address in the **x:x:x:x::x** format. The **::** notation specifies successive hexadecimal fields of zeros.
peer-group-name	Enter the name of the peer group.
maximum	Enter a number as the maximum number of prefixes allowed for this BGP router. Range: 1 to 4294967295.
threshold	(OPTIONAL) Enter a number to be used as a percentage of the *maximum* value. When the number of prefixes reaches this percentage of the *maximum* value, the E-Series software sends a message. Range: 1 to 100 percent. Default: 75
warning-only	(OPTIONAL) Enter the keyword **warning-only** to set the router to send a log message when the maximum value is reached. If this parameter is not set, the router stops peering when the maximum number of prefixes is reached.

Defaults *threshold* = 75

Command Modes ADDRESS FAMILY (conf-router_bgpv6_af)

Command History

Version 7.4.1.0	Introduced

Usage Information If the neighbor maximum-prefix is configured and the neighbor receives more prefixes than allowed by the neighbor maximum-prefix command configuration, the neighbor goes down and the show ip bgp ipv6 summary command displays `(prfxd)` in the State/PfxRcd column for that neighbor. The neighbor remains down until you enter the capture bgp-pdu max-buffer-size command for the neighbor or the peer group to which the neighbor belongs or you enter neighbor shutdown and neighbor no shutdown commands.

Related Commands

show ip bgp summary	Displays the current BGP configuration.

neighbor next-hop-self

C-Series	No
E-Series	✓

Allows you to configure the router as the next hop for a BGP neighbor. (This command is used for IBGP).

Syntax **neighbor** {*ipv6-address* | *peer-group-name*} **next-hop-self**

To return to the default setting, use the **no neighbor** {*ipv6-address* | *peer-group-name*} **next-hop-self** command.

Parameters

ipv6-address	Enter the IPv6 address in the **x:x:x:x::x** format. The **::** notation specifies successive hexadecimal fields of zeros.
peer-group-name	(OPTIONAL)Enter the name of the peer group.

Defaults Disabled.

Command Modes ADDRESS FAMILY (conf-router_bgpv6_af)

Command History

Version 7.4.1.0	Introduced

Usage Information If the set ipv6 next-hop command in the ROUTE-MAP mode is configured, its configuration takes precedence over the neighbor next-hop-self command.

neighbor password

C-Series	**No**
E-Series	✔

Enable Message Digest 5 (MD5) authentication on the TCP connection between two neighbors.

Syntax **neighbor** *ipv6-address* **password** [*encryption-type*] *password*

To delete a password, use the **no neighbor** *ipv6-address* **password** [*encryption-type*] *password* command.

Parameters

ipv6-address	Enter the IPv6 address in the **x:x:x:x::x** format. The **::** notation specifies successive hexadecimal fields of zeros.
encryption-type	(OPTIONAL) Enter 7 as the encryption type for the *password* entered. 7 means that the password is encrypted and hidden.
password	Enter a text string up to 80 characters long. The first character of the *password* must be a letter. You cannot use spaces in the password.

Defaults Not configured

Command Modes ROUTER BGP (conf-router)

Command History

Version 7.4.1.0	Introduced

Usage Information

Configure the same password on both BGP peers or a connection does not occur. When you configure MD5 authentication between two BGP peers, each segment of the TCP connection between them is verified and the MD5 digest is checked on every segment sent on the TCP connection.

Configuring a password for a neighbor will cause an existing session to be torn down and a new one established.

If you specify a BGP peer group by using the *peer-group-name* parameter, all the members of the peer group will inherit the characteristic configured with this command.

neighbor peer-group (assigning peers)

C-Series	**No**
E-Series	✓

Allows you to assign one peer to a existing peer group.

Syntax

neighbor *ipv6-address* **peer-group** *peer-group-name*

To delete a peer from a peer group, use the **no neighbor** *ipv6-address* **peer-group** *peer-group-name* command.

Parameters

ipv6-address	Enter the IPv6 address in the **x:x:x:x::x** format. The **::** notation specifies successive hexadecimal fields of zeros.
peer-group *peer-group-name*	Enter the keyword **peer-group** followed by the name of a configured peer group. (maximum 16 characters)

Defaults

Not configured.

Command Modes

ROUTER BGP (conf-router)

Command History

Version 7.4.1.0	Introduced

Usage Information

You can assign up to 64 peers to one peer group.

When you add a peer to a peer group, it inherits all the peer group's configured parameters. A peer cannot become part of a peer group if any of the following commands are configured on the peer:

- neighbor advertisement-interval
- neighbor distribute-list out
- neighbor filter-list out
- neighbor next-hop-self

- neighbor route-map out
- neighbor route-reflector-client
- neighbor send-community

A neighbor may keep its configuration after it was added to a peer group if the neighbor's configuration is more specific than the peer group's, and the neighbor's configuration does not affect outgoing updates.

A peer group must exist before you add a peer to it. If the peer group is disabled (shutdown) the peers within the group are also disabled (shutdown).

Related Commands

capture bgp-pdu max-buffer-size	Resets BGP sessions.
neighbor peer-group (creating group)	Create a peer group.
show ip bgp peer-group	View BGP peers.
show ip bgp neighbors	View BGP neighbors configurations.

neighbor peer-group (creating group)

C-Series	**No**
E-Series	✓

Allows you to create a peer group and assign it a name.

Syntax **neighbor** *peer-group-name* **peer-group**

To delete a peer group, use the **no neighbor** *peer-group-name* **peer-group** command.

Parameters

peer-group-name	Enter a text string up to 16 characters long as the name of the peer group.

Defaults Not configured.

Command Modes ROUTER BGP (conf-router)

Command History

Version 7.4.1.0	Introduced

Usage Information When a peer group is created, it is disabled (shut mode).

Related Commands

neighbor peer-group (assigning peers)	Assign routers to a peer group.

neighbor remote-as	Assign a indirectly connected AS to a neighbor or peer group.
neighbor shutdown	Disable a peer or peer group.

neighbor peer-group passive

C-Series	No
E-Series	✓

Enable passive peering on a BGP peer group, that is, the peer group does not send an OPEN message, but will respond to one.

Syntax

neighbor *peer-group-name* **peer-group passive**

To delete a passive peer-group, use the **no neighbor** *peer-group-name* **peer-group passive** command.

Parameters

peer-group-name	Enter a text string up to 16 characters long as the name of the peer group.

Defaults

Not configured.

Command Modes

ROUTER BGP (conf-router)

Command History

Version 7.4.1.0	Introduced

Usage Information

After you configure a peer group as passive, you must assign it a subnet using the neighbor subnet command.

Related Commands

neighbor subnet	Assign a subnet to a dynamically-configured BGP neighbor.

neighbor remote-as

C-Series	No
E-Series	✓

Create and specify the remote peer to the BGP neighbor.

Syntax

neighbor {*ipv6-address* | *peer-group-name*} **remote-as** *number*

To delete a remote AS entry, use the **no neighbor** {*ipv6-address* | *peer-group-name*} **remote-as** *number*command.

Parameters

ipv6-address	Enter the IPv6 address in the **x:x:x:x::x** format. The **::** notation specifies successive hexadecimal fields of zeros.
peer-group-name	Enter the name of the peer group to enter the remote AS into routing tables of all routers within the peer group.
number	Enter a number of the AS. Range: 1 to 65535.

Defaults

Not configured.

Command Modes

ROUTER BGP (conf-router)

Command History

Version 7.4.1.0	Introduced

Usage Information

If the *number* parameter is the same as the AS number used in the router bgp command, the remote AS entry in the neighbor is considered an internal BGP peer entry.

This command creates a peer and the newly created peer is disabled (shutdown).

Related Commands

router bgp	Enter the ROUTER BGP mode and configure routes in an AS.

neighbor remove-private-as

C-Series	**No**
E-Series	✓

Remove private AS numbers from the AS-PATH of outgoing updates.

Syntax

neighbor {*ipv6-address* | *peer-group-name*} **remove-private-as**

To return to the default, use the **no neighbor** {*ipv6-address* | *peer-group-name*} **remove-private-as** command.

Parameters

ipv6-address	Enter the IPv6 address in the **x:x:x:x::x** format. The **::** notation specifies successive hexadecimal fields of zeros.
peer-group-name	Enter the name of the peer group to remove the private AS numbers

Defaults Disabled (that is, private AS number are not removed).

Command Modes ADDRESS FAMILY (conf-router_bgpv6_af)

Command History

Version 7.4.1.0	Introduced

Usage Information Applies to EBGP neighbors only.

If the AS-PATH contains both public and private AS number or contains AS numbers of an EBGP neighbor, the private AS numbers are not removed.

If a confederation contains private AS numbers in its AS-PATH, the software removes the private AS numbers only if they follow the confederation numbers in the AS path.

Private AS numbers are 64512 to 65535.

neighbor route-map

C-Series	**No**
E-Series	✓

Apply an established route map to either incoming or outbound routes of a BGP neighbor or peer group.

Syntax **neighbor** {*ipv6-address* | *peer-group-name*} **route-map** *map-name* {**in** | **out**}

To remove the route map, use the **no neighbor** {*ipv6-address* | *peer-group-name*} **route-map** *map-name* {**in** | **out**} command.

Parameters

ipv6-address	Enter the IPv6 address in the **x:x:x:x::x** format. The **::** notation specifies successive hexadecimal fields of zeros.
peer-group-name	Enter the name of the peer group.
map-name	Enter the name of an established route map. If the Route map is not configured, the default is deny (to drop all routes).
in	Enter the keyword **in** to filter inbound routes.
out	Enter the keyword **out** to filter outbound routes.

Defaults Not configured.

Command Modes ADDRESS FAMILY (conf-router_bgpv6_af)

Command History

Version 7.4.1.0	Introduced

Usage Information

When you apply a route map to outbound routes, only routes that match at least one section of the route map are permitted.

If you identify a peer group by name, the peers in that peer group inherit the characteristics in the Route map used in this command. If you identify a peer by IP address, the Route map overwrites either the inbound or outbound policies on that peer.

neighbor route-reflector-client

C-Series	**No**
E-Series	✓

Configure a neighbor as a member of a route reflector cluster.

Syntax

neighbor {*ipv6-address* | *peer-group-name*} **route-reflector-client**

To indicate that the neighbor is not a route reflector client or to delete a route reflector configuration, use the **no neighbor** {*ipv6-address* | *peer-group-name*} **route-reflector-client** command.

Parameters

ipv6-address	Enter the IPv6 address in the **x:x:x:x::x** format. The **::** notation specifies successive hexadecimal fields of zeros.
peer-group-name	Enter the name of the peer group. All routers in the peer group receive routes from a route reflector.

Defaults

Not configured.

Command Modes

ADDRESS FAMILY (conf-router_bgpv6_af)

Command History

Version 7.4.1.0	Introduced

Usage Information

The first time you enter this command it configures the neighbor as a route reflector and members of the route-reflector cluster. Internal BGP (IBGP) speakers do not need to be fully meshed if you configure a route reflector.

When all clients of a route reflector are disabled, the neighbor is no longer a route reflector.

neighbor send-community

C-Series	No
E-Series	✓

Send a COMMUNITY attribute to a BGP neighbor or peer group. A COMMUNITY attribute indicates that all routes with that attribute belong to the same community grouping.

Syntax **neighbor** {*ipv6-address* | *peer-group-name*} **send-community**

To disable sending a COMMUNITY attribute, use the **no neighbor** {*ipv6-address* | *peer-group-name*} **send-community** command.

Parameters

ipv6-address	Enter the IPv6 address in the **x:x:x:x::x** format. The **::** notation specifies successive hexadecimal fields of zeros.
peer-group-name	Enter the name of the peer group to send a COMMUNITY attribute to all routers within the peer group.

Defaults Not configured and COMMUNITY attributes are not sent to neighbors.

Command Modes ADDRESS FAMILY (conf-router_bgpv6_af)

Command History

Version 7.4.1.0	Introduced

neighbor shutdown

C-Series	No
E-Series	✓

Disable a BGP neighbor or peer group.

Syntax **neighbor** {*ipv6-address* | *peer-group-name*} **shutdown**

To enable a disabled neighbor or peer group, use the **no neighbor** {*ipv6-address* | *peer-group-name*} **shutdown** command.

Parameters

ipv6-address	Enter the IPv6 address in the **x:x:x:x::x** format. The **::** notation specifies successive hexadecimal fields of zeros.
peer-group-name	Enter the name of the peer group to disable or enable all routers within the peer group.

Defaults Enabled (that is, BGP neighbors and peer groups are disabled.)

Command Modes ROUTER BGP (conf-router)

Command History

Version 7.4.1.0	Introduced

Usage Information Peers that are enabled within a peer group are disabled when their peer group is disabled.

The neighbor shutdown command terminates all BGP sessions on the BGP neighbor or BGP peer group. Use this command with caution as it terminates the specified BGP sessions. When a neighbor or peer group is shutdown, use the show ip bgp summary command to confirm its status.

Related Commands

show ip bgp summary	Displays the current BGP configuration.
show ip bgp neighbors	Displays the current BGP neighbors.

neighbor subnet

C-Series	**No**
E-Series	✓

Enable passive peering so that the members of the peer group are dynamic

Syntax **neighbor** *peer-group-name* **subnet** *subnet-number mask*

To remove passive peering, use the **no neighbor** *peer-group-name* **subnet** *subnet-number mask* command.

Parameters

subnet-number	Enter a subnet number in dotted decimal format (A.B.C.D.) as the allowable range of addresses included in the Peer group. To allow all addresses, enter 0::0/0.
mask	Enter a prefix mask in / prefix-length format (/x).

Defaults Not configured.

Command Modes ROUTER BGP (conf-router)

Command History

Version 7.4.1.0	Introduced

neighbor timers

C-Series	No
E-Series	✓

Set keepalive and hold time timers for a BGP neighbor or a peer group.

Syntax

neighbor {*ipv6-address* | *peer-group-name*} **timers** *keepalive holdtime*

To return to the default values, use the **no neighbor** {*ipv6-address* | *peer-group-name*} **timers** command.

Parameters

ipv6-address	Enter the IPv6 address in the **x:x:x:x::x** format. The **::** notation specifies successive hexadecimal fields of zeros.
peer-group-name	Enter the name of the peer group to set the timers for all routers within the peer group.
keepalive	Enter a number for the time interval, in seconds, between keepalive messages sent to the neighbor routers. Range: 1 to 65535 Default: 60 seconds
holdtime	Enter a number for the time interval, in seconds, between the last keepalive message and declaring the router dead. Range: 3 to 65535 Default: 180 seconds

Defaults

keepalive = 60 seconds; *holdtime* = 180 seconds.

Command Modes

ROUTER BGP (conf-router)

Command History

Version 7.4.1.0	Introduced

Usage Information

Timer values configured with the neighbor timers command override the timer values configured with the timers bgp command.

When two neighbors, configured with different *keepalive* and *holdtime* values, negotiate for new values, the resulting values will be as follows:

- the lower of the *holdtime* values is the new *holdtime* value, and
- whichever is the lower value; one-third of the new *holdtime* value, or the configured *keepalive* value is the new *keepalive* value.

neighbor update-source

C-Series	No
E-Series	✓

Enable the E-Series software to use Loopback interfaces for TCP connections for BGP sessions.

Syntax **neighbor** {*ipv6-address* | *peer-group-name*} **update-source loopback** *interface*

To use the closest interface, use the **no neighbor** {*ipv6-address* | *peer-group-name*} **update-source loopback** *interface* command.

Parameters

ipv6-address	Enter the IPv6 address in the **x:x:x:x::x** format. The **::** notation specifies successive hexadecimal fields of zeros.
peer-group-name	Enter the name of the peer group to disable all routers within the peer group.
loopback *interface*	Enter the keyword **loopback** followed by a number of the loopback interface. Range: 0 to 16383.

Defaults Not configured.

Command Modes ROUTER BGP (conf-router)

Command History

Version 7.4.1.0	Introduced

Usage Information Loopback interfaces are up constantly and the BGP session may need one interface constantly up to stabilize the session. The neighbor update-source command is not necessary for directly connected internal BGP sessions.

neighbor weight

C-Series	No
E-Series	✓

Assign a weight to the neighbor connection, which is used to determine the best path.

Syntax **neighbor** {*ipv6-address* | *peer-group-name*} **weight** *weight*

To remove a weight value, use the **no neighbor** {*ipv6-address* | *peer-group-name*} **weight** *weight* command.

Parameters

ipv6-address	Enter the IPv6 address in the **x:x:x:x::x** format. The **::** notation specifies successive hexadecimal fields of zeros.
peer-group-name	Enter the name of the peer group to disable all routers within the peer group.
weight	Enter a number as the weight. Range: 0 to 65535 Default: 0

Defaults 0

Command Modes ROUTER BGP (conf-router)

Command History

Version 7.4.1.0	Introduced

Usage Information In the FTOS best path selection process, the path with the highest weight value is preferred.

Note: Reset the neighbor connection (capture bgp-pdu max-buffer-size * command) to apply the weight to the connection and recompute the best path.

network

C-Series	**No**
E-Series	✓

Specify the networks for the BGP process and enter them in the BGP routing table.

Syntax **network** *ipv6-address prefix-length* [**route-map** *map-name*]

To remove a network, use the **no network** *ip-address mask* [**route-map** *map-name*] command.

Parameters

ipv6-address prefix-length	Enter the IPv6 address in the **x:x:x:x::x** format followed by the prefix length in the **/x** format. Range: /0 to /128 The **::** notation specifies successive hexadecimal fields of zeros.

mask	Enter the mask of the IP address in the slash prefix length format (for example, /24). The mask appears in command outputs in dotted decimal format (A.B.C.D).
route-map *map-name*	(OPTIONAL) Enter the keyword **route-map** followed by the name of an established route map. Only the following ROUTE-MAP mode commands are supported: • match ipv6 address • match ipv6 next-hop • match ipv6 route-source • set ipv6 next-hop If the route map is not configured, the default is deny (to drop all routes).

Defaults

Not configured.

Command Modes

ADDRESS FAMILY (conf-router_bgpv6_af)

Command History

Version 7.4.1.0	Introduced

Usage Information

The E-Series software resolves the network address configured by the network command with the routes in the main routing table to ensure that the networks are reachable via non-BGP routes and non-default routes.

Related Commands

redistribute	Redistribute routes into BGP.

network backdoor

C-Series	**No**
E-Series	✓

Specify this IGP route as the preferred route.

Syntax

network *ipv6-address prefix-length* **backdoor**

To remove a network, use the **no network** *ipv6-address prefix-length* **backdoor** command.

Parameters

ipv6-address prefix-length	Enter the IPv6 address in the **x:x:x:x::x** format followed by the prefix length in the **/x** format. Range: /0 to /128 The **::** notation specifies successive hexadecimal fields of zeros.

Defaults Not configured.

Command Modes ADDRESS FAMILY (conf-router_bgpv6_af)

Command History

Version 7.4.1.0	Introduced

Usage Information Though FTOS does not generate a route due to backdoor config, there is an option for injecting/sourcing a local route in presence of network backdoor config on a learned route.

redistribute

C-Series	**No**
E-Series	✔

Redistribute routes into BGP.

Syntax **redistribute** {**connected** | **static**} [**route-map** *map-name*]

To disable redistribution, use the **no redistribution** {**connected** | **static**} command.

Parameters

connected	Enter the keyword **connected** to redistribute routes from physically connected interfaces.
static	Enter the keyword **static** to redistribute manually configured routes. These routes are treated as incomplete routes.
route-map *map-name*	(OPTIONAL) Enter the keyword **route-map** followed by the name of an established route map. Only the following ROUTE-MAP mode commands are supported: • match ipv6 address • match ipv6 next-hop • match ipv6 route-source • set ipv6 next-hop If the route map is not configured, the default is deny (to drop all routes).

Defaults Not configured.

Command Modes ADDRESS FAMILY (conf-router_bgpv6_af)

Command History

Version 7.4.1.0	Introduced

Usage Information If you do not configure default-metric command, in addition to the redistribute command, or there is no route map to set the metric, the metric for redistributed static and connected is “0”.

To redistribute the default route (0**::**0/0) configure the neighbor default-originate command.

Related Commands		
	neighbor default-originate	Inject the default route.

redistribute ospf

C-Series	No
E-Series	✓

Redistribute OSPFv3 routes into BGP.

Syntax **redistribute ospf** *process-id* [[**match external** {**1** | **2**}] [**match internal**]] [**route-map** *map-name*]

To stop redistribution of OSPF routes, use the **no redistribute ospf** *process-id* command.

Parameters

process-id	Enter the number of the OSPFv3 process. Range: 1 to 65535
match external {**1** | **2**}	(OPTIONAL) Enter the keywords match external to redistribute OSPF external routes. You can specify 1 or 2 to redistribute those routes only.
match internal	(OPTIONAL) Enter the keywords **match internal** to redistribute OSPFv3 internal routes only.
route-map *map-name*	(OPTIONAL) Enter the keyword **route-map** followed by the name of an established route map. Only the following ROUTE-MAP mode commands are supported: • match ipv6 address • match ipv6 next-hop • match ipv6 route-source • set ipv6 next-hop If the route map is not configured, the default is deny (to drop all routes).

Defaults Not configured.

Command Modes ADDRESS FAMILY (conf-router_bgpv6_af)

Command History

Version 7.4.1.0	Introduced

Usage Information When you enter redistribute ospf *process-id* command without any other parameters, FTOS redistributes all OSPF internal routes, external type 1 routes, and external type 2 routes.

router bgp

C-Series	No
E-Series	✓

Enter ROUTER BGP mode to configure and enable BGP.

Syntax **router bgp** *as-number*

To disable BGP, use the **no router bgp** *as-number* command.

Parameters

as-number	Enter the AS number. Range: 1 to 65535.

Defaults Not enabled.

Command Modes CONFIGURATION

Command History

Version 7.4.1.0	Introduced

show capture bgp-pdu neighbor (ipv6)

C-Series	No
E-Series	✓

Display BGP packet capture information for an IPv6 address on the E-Series.

Syntax **show capture bgp-pdu neighbor** *ipv6-address*

Parameters

ipv6-address	Enter the IPv6 address (X:X:X:X::X) of a BGP neighbor.

Command Modes EXEC

EXEC privilege

Command History

Version 7.5.1.0	Introduced

Related Commands

capture bgp-pdu neighbor (ipv6)	Enable capture of an IPv6 BGP neighbor packet.
capture bgp-pdu max-buffer-size	Specify a size for the capture buffer.
show capture bgp-pdu neighbor (ipv4)	Display BGP packet capture information for an IPv4 address on the E-Series.

show config

C-Series	No
E-Series	✓

View the current ROUTER BGP configuration.

Syntax **show config**

Command Modes ADDRESS FAMILY (conf-router_bgpv6_af)

Example

```
Force10(conf-router_bgp)#show conf
!
router bgp 18508
 neighbor RR-CLIENT peer-group
 neighbor RR-CLIENT remote-as 18508
 neighbor RR-CLIENT no shutdown
 neighbor RR-CLIENT-PASSIV peer-group passive
 neighbor RR-CLIENT-PASSIV remote-as 18508
 neighbor RR-CLIENT-PASSIV subnet 9000::9:0/120
 neighbor RR-CLIENT-PASSIV no shutdown
 neighbor 1109::33 remote-as 18508
 neighbor 1109::33 update-source Loopback 101
 neighbor 1109::33 no shutdown
 neighbor 2222::220 remote-as 18508
 neighbor 2222::220 route-reflector-client
 neighbor 2222::220 update-source Loopback 100
 neighbor 2222::220 no shutdown
 neighbor 4000::33 remote-as 18508
 neighbor 4000::33 no shutdown
 neighbor 4000::60 remote-as 18508
 neighbor 4000::60 no shutdown
 neighbor 9000::1:2 remote-as 640
 no neighbor 9000::1:2 activate
 neighbor 9000::1:2 no shutdown
 neighbor 9000::4:2 peer-group RR-CLIENT
 neighbor 9000::4:2 no shutdown
 neighbor 9000::5:2 remote-as 1
 neighbor 9000::5:2 no shutdown
 neighbor 9000::6:2 remote-as 2
 neighbor 9000::6:2 no shutdown
 neighbor 9000::7:2 remote-as 3
 neighbor 9000::7:2 no shutdown
 neighbor 9000::8:2 remote-as 18508
 neighbor 9000::8:2 no shutdown
 neighbor 9000::a:2 remote-as 18508
 neighbor 9000::a:2 no shutdown
 neighbor 9000::b:14 remote-as 18508
 neighbor 9000::b:14 no shutdown
 !
 address-family ipv6 unicast
 neighbor RR-CLIENT activate
 neighbor RR-CLIENT route-reflector-client
 neighbor RR-CLIENT-PASSIV activate
 neighbor RR-CLIENT-PASSIV route-reflector-client
 neighbor 1109::33 activate
 neighbor 2222::220 activate
 neighbor 2222::220 route-reflector-client
 neighbor 4000::33 activate
 neighbor 4000::60 activate
 neighbor 9000::1:2 activate
 neighbor 9000::5:2 activate
 neighbor 9000::6:2 activate
 neighbor 9000::7:2 activate
 neighbor 9000::8:2 activate
 neighbor 9000::a:2 activate
 neighbor 9000::b:14 activate
 exit-address-family
```

Figure 360 show config Command Example (Partial)

show ip bgp ipv6

C-Series	No
E-Series	✓

View the current BGP routing table for the E-Series.

Syntax **show ip bgp ipv6 unicast** [*network* [*network-mask*] [**longer-prefixes**]]

Parameters

network	(OPTIONAL) Enter the network address (in dotted decimal format) of the BGP network to view information only on that network.
network-mask	(OPTIONAL) Enter the network mask (in slash prefix format) of the BGP network address.
longer-prefixes	(OPTIONAL) Enter the keyword **longer-prefixes** to view all routes with a common prefix.

Command Modes EXEC

EXEC privilege

Command History

Version 7.4.1.0	Introduced

Usage Information When you enable **bgp non-deterministic-med** command, the **show ip bgp** command output for a BGP route does not list the INACTIVE reason.

show ip bgp cluster-list

C-Series	No
E-Series	✓

View BGP neighbors in a specific cluster.

Syntax **show ip bgp cluster-list** [*cluster-id*]

Parameters

cluster-id	(OPTIONAL) Enter the cluster id in dotted decimal format.

Command Modes EXEC

EXEC privilege

Command History

Version 7.4.1.0	Introduced

show ip bgp community

C-Series	No
E-Series	✓

View information on all routes with Community attributes or view specific BGP community groups.

Syntax

show ip bgp ipv6 unicast community [*community-number*] [**local-as**] [**no-export**] [**no-advertise**]

Parameters

community-number	Enter the community number in AA:NN format where AA is the AS number (2 bytes) and NN is a value specific to that autonomous system. You can specify up to eight community numbers to view information on those community groups.
local-AS	Enter the keywords **local-AS** to view all routes with the COMMUNITY attribute of NO_EXPORT_SUBCONFED. All routes with the NO_EXPORT_SUBCONFED (0xFFFFFF03) community attribute must not be advertised to external BGP peers.
no-advertise	Enter the keywords **no-advertise** to view all routes containing the well-known community attribute of NO_ADVERTISE. All routes with the NO_ADVERTISE (0xFFFFFF02) community attribute must not be advertised to other BGP peers.
no-export	Enter the keywords **no-export** to view all routes containing the well-known community attribute of NO_EXPORT. All routes with the NO_EXPORT (0xFFFFFF01) community attribute must not be advertised outside a BGP confederation boundary.

Command Modes

EXEC

EXEC privilege

Command History

Version 7.4.1.0	Introduced

Usage Information

To view the total number of COMMUNITY attributes found, use the show ip bgp ipv6 summary command. The text line above the route table states the number of COMMUNITY attributes found.

show ip bgp community-list

C-Series	No
E-Series	✓

View routes that are affected by a specific community list.

Syntax **show ip bgp ipv6 unicast community-list** *community-list-name* [**exact-match**]

Parameters

community-list-name	Enter the name of a configured IP community list.
exact-match	(OPTIONAL) Enter **exact-match** to display only for an exact match of the communities.

Command Modes EXEC

EXEC privilege

Command History

Version 7.4.1.0	Introduced

show ip bgp dampened-paths

C-Series	No
E-Series	✓

View BGP routes that are dampened (non-active).

Syntax **show ip bgp ipv6 unicast dampened-paths**

Command Modes EXEC

EXEC privilege

Command History

Version 7.4.1.0	Introduced

show ip bgp filter-list

C-Series	No
E-Series	✓

View the routes that match the filter lists.

Syntax **show ip bgp ipv6 unicast filter-list** *as-path-name*

Parameters		
	as-path-name	Enter the name of an AS-PATH.

Command Modes EXEC

EXEC privilege

Command History		
	Version 7.4.1.0	Introduced

show ip bgp ipv6 flap-statistics

C-Series	No
E-Series	✓

View flap statistics on BGP routes.

Syntax **show ip bgp ipv6 unicast flap-statistics** [*ipv6-address prefix-length*] [**filter-list** *as-path-name*] [**regexp** *regular-expression*]

Parameters		
	ipv6-address prefix-length	Enter the IPv6 address in the **x:x:x:x::x** format followed by the prefix length in the **/x** format. Range: /0 to /128 The **::** notation specifies successive hexadecimal fields of zeros.
	filter-list *as-path-name*	(OPTIONAL) Enter the keyword **filter-list** followed by the name of a configured AS-PATH ACL.
	regexp *regular-expression*	Enter a regular expression then use one or a combination of the following characters to match: • **.** = (period) any single character (including a white space) • * = (asterisk) the sequences in a pattern (0 or more sequences) • **+** = (plus) the sequences in a pattern (1 or more sequences) • **?** = (question mark) sequences in a pattern (either 0 or 1 sequences). **You must enter an escape sequence (CTRL+v) prior to entering the ? regular expression.** • **[ ]** = (brackets) a range of single-character patterns. • **^** = (caret) the beginning of the input string. If the caret is used at the beginning of a sequence or range, it matches on everything BUT the characters specified. • **$** = (dollar sign) the end of the output string.

Command Modes EXEC

EXEC privilege

Command History	
Version 7.4.1.0	Introduced

show ip bgp inconsistent-as

C-Series	No
E-Series	✓

View routes with inconsistent originating Autonomous System (AS) numbers, that is, prefixes that are announced from the same neighbor AS but with a different AS-Path.

Syntax **show ip bgp ipv6 unicast inconsistent-as**

Command Modes EXEC

EXEC privilege

Command History	
Version 7.4.1.0	Introduced

show ip bgp neighbors

C-Series	No
E-Series	✓

Allows you to view the information exchanged by BGP neighbors.

Syntax **show ip bgp neighbors** [*ipv6-address prefix-length* | *ip-address*] [**advertised-routes** | **dampened-routes** | **detail** | **flap-statistics** | **routes**]

Parameters

ipv6-address prefix-length | *ip-address*	Enter the IPv6 address in the **x:x:x:x::x** format followed by the prefix length in the **/x** format. Range: /0 to /128 The **::** notation specifies successive hexadecimal fields of zeros *or* Enter an IP address in dotted decimal format to reset all prefixes from that neighbor.
advertised-routes	(OPTIONAL) Enter the keyword **advertised-routes** to view only the routes the neighbor sent.

dampened-routes	(OPTIONAL) Enter the keyword **dampened-routes** to view information on dampened routes from the BGP neighbor.
detail	(OPTIONAL) Enter the keyword **detail** to view neighbor-specific internal information for the IPv6 address family.
flap-statistics	(OPTIONAL) Enter the keyword **flap-statistics** to view flap statistics on the neighbor's routes.
routes	(OPTIONAL) Enter the keywords **routes** to view only the neighbor's feasible routes.

Command Modes

EXEC

EXEC privilege

Command History

Version 7.5.1.0	Modified: Added **detail** option.
Version 7.4.1.0	Introduced

Related Commands

show ip bgp ipv6	View the current BGP routing table.

show ip bgp next-hop

C-Series	**No**
E-Series	✓

View all next hops (via learned routes only) with current reachability and flap status. This command only displays one path, even if the next hop is reachable by multiple paths.

Syntax **show ip bgp next-hop**

Command Modes

EXEC

EXEC privilege

Command History

Version 7.4.1.0	Introduced

Example

```
Force10#show ip bgp next-hop
 Next-hop        Via                        RefCount  Cost  Flaps Time Elapsed
 9000::5:2       9000::5:2, Gi 8/38                2     0      0 00:23:22
 9000::6:2       9000::6:2, Gi 8/38                2     0      0 00:23:22
 9000::7:2       9000::7:2, Gi 8/38                2     0      0 00:23:22
 9000::8:2       9000::8:2, Gi 8/38                2     0      0 00:23:22
 9000::9:2       9000::9:2, Gi 8/38             6000     0      0 00:23:16
 9000::a:2       9000::a:2, Gi 8/38                2     0      0 00:23:22
Force10#
```

Figure 361 show ip bgp next-hop Command Example

show ip bgp paths

C-Series	No
E-Series	✓

View all the BGP path attributes in the BGP database.

Syntax **show ip bgp paths** [**regexp** *regular-expression*]

Parameters

regexp *regular-expression*	Enter a regular expression then use one or a combination of the following characters to match: • **.** = (period) any single character (including a white space) • * = (asterisk) the sequences in a pattern (0 or more sequences) • **+** = (plus) the sequences in a pattern (1 or more sequences) • **?** = (question mark) sequences in a pattern (either 0 or 1 sequences). **You must enter an escape sequence (CTRL+v) prior to entering the ? regular expression.** • **[ ]** = (brackets) a range of single-character patterns. • **^** = (caret) the beginning of the input string. If the caret is used at the beginning of a sequence or range, it matches on everything BUT the characters specified. • **$** = (dollar sign) the end of the output string.

Command Modes EXEC

EXEC privilege

Command History

Version 7.4.1.0	Introduced

show ip bgp paths as-path

C-Series	No
E-Series	✓

View all unique AS-PATHs in the BGP database

Syntax **show ip bgp paths as-path**

Command Modes EXEC

EXEC privilege

Command History

Version 7.4.1.0	Introduced

show ip bgp paths community

C-Series	No
E-Series	✓

View all unique COMMUNITY numbers in the BGP database.

Syntax **show ip bgp paths community**

Command Modes EXEC

EXEC privilege

Command History

Version 7.4.1.0	Introduced

show ip bgp peer-group

C-Series	No
E-Series	✓

Allows you to view information on the BGP peers in a peer group.

Syntax **show ip bgp peer-group** [*peer-group-name* [**summary**]]

Parameters

peer-group-name	(OPTIONAL) Enter the name of a peer group to view information about that peer group only.
summary	(OPTIONAL) Enter the keyword **summary** to view status information of the peers in that peer group. The output is the same as that found in show ip bgp summary command

Command Modes

EXEC

EXEC privilege

Command History

Version 7.4.1.0	Introduced

Example

```
Force10#show ip bgp peer-group

Peer-group RR-CLIENT, remote AS 18508
  BGP version 4
  Minimum time between advertisement runs is 5 seconds

  For address family: IPv4 Unicast
  BGP neighbor is RR-CLIENT, peer-group internal,
  Number of peers in this group 1
  Peer-group members (* - outbound optimized):
    9000::4:

Peer-group RR-CLIENT-PASSIV, remote AS 18508
  BGP version 4
  Minimum time between advertisement runs is 5 seconds

  For address family: IPv4 Unicast
  BGP neighbor is RR-CLIENT-PASSIV, peer-group internal,
  Number of peers in this group 1
  Peer-group members (* - outbound optimized):
    9000::9:2*
Force10#
```

Figure 362 show ip bgp peer-group Command Example

show ip bgp regexp

C-Series	**No**
E-Series	✓

Allows you to view the subset of BGP routing table matching the regular expressions specified.

Syntax **show ip bgp regexp** *regular-expression* [*character*]

Parameters	*regular-expression* [*character*]	Enter a regular expression then use one or a combination of the following characters to match: • **.** = (period) any single character (including a white space) • ***** = (asterisk) the sequences in a pattern (0 or more sequences) • **+** = (plus) the sequences in a pattern (1 or more sequences) • **?** = (question mark) sequences in a pattern (either 0 or 1 sequences). **You must enter an escape sequence (CTRL+v) prior to entering the ? regular expression.** • **[ ]** = (brackets) a range of single-character patterns. • **^** = (caret) the beginning of the input string. If the caret is used at the beginning of a sequence or range, it matches on everything BUT the characters specified. • **$** = (dollar sign) the end of the output string.

Command Modes

EXEC

EXEC privilege

Command History

Version 7.4.1.0	Introduced

show ip bgp summary

C-Series	**No**
E-Series	✓

Allows you to view the status of all BGP connections.

Syntax **show ip bgp summary**

Command Modes

EXEC

EXEC privilege

Command History

Version 7.4.1.0	Introduced

Example

```
Force10# show ip bgp summary
BGP router identifier 55.55.55.55, local AS number 18508
BGP table version is 0, main routing table version 0
6 BGP path attribute entrie(s) using 392 bytes of memory
6 BGP AS-PATH entrie(s) using 294 bytes of memory
6 BGP community entrie(s) using 234 bytes of memory

Neighbor        AS     MsgRcvd  MsgSent     TblVer  InQ  OutQ Up/Down  State/Pfx

1109::33        18508        0        0          0    0     0 never    Active
2222::220       18508        0        0          0    0     0 never    Active
4000::33        18508        0        0          0    0     0 never    Active
4000::60        18508        0        0          0    0     0 never    Active
9000::4:2       18508        0        0          0    0     0 never    Active
9000::5:2       1           35       32          0    0     0 00:16:42          0
9000::6:2       2           35       32          0    0     0 00:16:39          0
9000::7:2       3           35       32          0    0     0 00:16:41          0
9000::8:2       18508       35       32          0    0     0 00:16:42          0
9000::9:2       18508       44       19          0    0     0 00:16:41          0
9000::a:2       18508       35       32          0    0     0 00:16:43          0
9000::b:14      18508       29       29          0    0     0 00:13:01          0
Force10#
```

Figure 363 show ip bgp summary Command Example

timers bgp

C-Series	No
E-Series	✔

Allows you to adjust the BGP network timers for all neighbors.

Syntax **timers bgp** *keepalive holdtimer*

To return to the default values, use the **no timers bgp** command.

Parameters

keepalive	Enter the time interval in seconds between which the E-Series sends keepalive messages. Range: 1 to 65535 Default: 60 seconds
holdtimer	Enter the time interval in seconds which the E-Series waits since the last keepalive message before declaring a BGP peer dead. Range: 3 to 65535 Default: 180 seconds

Defaults *keepalive* = 60 seconds; *holdtimer* = 180 seconds

Command Modes ROUTER BGP (conf-router)

Command History

Version 7.4.1.0	Introduced

Related Commands		
	neighbor timers	Adjust BGP timers for a specific peer or peer group.

IPv6 MBGP Commands

Multiprotocol BGP (MBGP) is an enhanced BGP that enables multicast routing policy throughout the Internet and connecting multicast topologies between BGP and autonomous systems (AS). FTOS MBGP is implemented as per IETF RFC 1858. The MBGP commands are:

- address family on page 1190
- aggregate-address on page 1190
- bgp dampening on page 1192
- clear ip bgp ipv6 unicast on page 1192
- clear ip bgp ipv6 unicast dampening on page 1193
- clear ip bgp ipv6 unicast flap-statistics on page 1194
- debug ip bgp ipv6 unicast dampening on page 1194
- debug ip bgp ipv6 unicast peer-group updates on page 1195
- debug ip bgp ipv6 unicast updates on page 1196
- distance bgp on page 1196
- neighbor activate on page 1197
- neighbor advertisement-interval on page 1198
- neighbor default-originate on page 1199
- neighbor distribute-list on page 1199
- neighbor filter-list on page 1200
- neighbor maximum-prefix on page 1201
- neighbor next-hop-self on page 1202
- neighbor remove-private-AS on page 1202
- neighbor route-map on page 1203
- neighbor route-reflector-client on page 1204
- network on page 1204
- redistribute on page 1205
- show ip bgp ipv6 unicast on page 1206
- show ip bgp ipv6 unicast cluster-list on page 1208
- show ip bgp ipv6 unicast community on page 1208
- show ip bgp ipv6 unicast community-list on page 1209
- show ip bgp ipv6 unicast dampened-paths on page 1210

- show ip bgp ipv6 unicast detail on page 1210
- show ip bgp ipv6 unicast filter-list on page 1211
- show ip bgp ipv6 unicast flap-statistics on page 1212
- show ip bgp ipv6 unicast inconsistent-as on page 1213
- show ip bgp ipv6 unicast neighbors on page 1213
- show ip bgp ipv6 unicast peer-group on page 1216
- show ip bgp ipv6 unicast summary on page 1217

address family

C-Series	No
E-Series	✓

This command changes the context to SAFI (Subsequent Address Family Identifier).

Syntax **address family ipv6 unicast**

To remove SAFI context, use the **no address family ipv6 unicast** command.

Parameters

ipv6	Enter the keyword **ipv6** to specify the address family as IPv6.
unicast	Enter the keyword **unicast** to specify multicast as SAFI.

Defaults IPv6 Unicast

Command Modes ROUTER BGP (conf-router_bgpv6-af)

Command History

Version 7.4.1.0	Introduced

Usage Information All subsequent commands will apply to this address family once this command is executed. You can exit from this AFI/SAFI to the IPv6 Unicast (the default) family by entering **exit** and returning to the Router BGP context.

aggregate-address

C-Series	No
E-Series	✓

Summarize a range of prefixes to minimize the number of entries in the routing table.

Syntax

aggregate-address *ipv6-address prefix-length* [**advertise-map** *map-name*] [**as-set**] [**attribute-map** *map-name*] [**summary-only**] [**suppress-map** *map-name*]

Parameters

ipv6-address prefix-length	Enter the IPv6 address in the **x:x:x:x::x** format followed by the prefix length in the **/x** format. Range: /0 to /128 The **::** notation specifies successive hexadecimal fields of zeros.
advertise-map *map-name*	(OPTIONAL) Enter the keywords **advertise-map** followed by the name of a configured route map to set filters for advertising an aggregate route.
as-set	(OPTIONAL) Enter the keyword **as-set** to generate path attribute information and include it in the aggregate. AS_SET includes AS_PATH and community information from the routes included in the aggregated route.
attribute-map *map-name*	(OPTIONAL) Enter the keywords **attribute-map** followed by the name of a configured route map to modify attributes of the aggregate, excluding AS_PATH and NEXT_HOP attributes.
summary-only	(OPTIONAL) Enter the keyword **summary-only** to advertise only the aggregate address. Specific routes will not be advertised.
suppress-map *map-name*	(OPTIONAL) Enter the keywords **suppress-map** followed by the name of a configured route map to identify which more-specific routes in the aggregate are suppressed.

Defaults

Not configured.

Command Modes

ROUTER BGP Address Family (conf-router_bgpv6-af)

Command History

Version 7.4.1.0	Introduced

Usage Information

At least one of the routes included in the aggregate address must be in the BGP routing table for the configured aggregate to become active.

Do not add the **as-set** parameter to the aggregate. If routes within the aggregate are constantly changing, the aggregate will flap to keep track of the changes in the AS_PATH.

In route maps used in the **suppress-map** parameter, routes meeting the **deny** clause are not suppress; in other words, they are allowed. The opposite is true: routes meeting the **permit** clause are suppressed.

If the route is injected via the network command, that route will still appear in the routing table if the summary-only parameter is configured in the aggregate-address command.

The summary-only parameter suppresses all advertisements. If you want to suppress advertisements to only specific neighbors, use the neighbor distribute-list command.

bgp dampening

C-Series	No
E-Series	✓

Enable MBGP route dampening.

Syntax **bgp dampening** [*half-life time*] [**route-map** *map-name*]

To disable route dampening, use the **no bgp dampening** [*half-life time*] [**route-map** *map-name*] command.

Parameters

half-life time	(OPTIONAL) Enter the number of minutes after which the Penalty is decreased. After the router assigns a Penalty of 1024 to a route, the Penalty is decreased by half, after the half-life period expires. Range: 1 to 45. Default: 15 minutes
route-map *map-name*	(OPTIONAL) Enter the keyword **route-map** followed by the name of a configured route map. Only match commands in the configured route map are supported.

Defaults Disabled.

Command Modes ROUTER BGP Address Family (conf-router_bgpv6-af)

Command History

Version 7.4.1.0	Introduced

clear ip bgp ipv6 unicast

C-Series	No
E-Series	✓

Reset MBGP sessions.

Syntax **clear ip bgp ipv6 unicast** * *ipv6-address prefix-length* [**dampening** | **flap-statistics**] **peer-group**]

Parameters

*	Enter the character * to clear all peers.
ipv6-address prefix-length	Enter the IPv6 address in the **x:x:x:x::x** format followed by the prefix length in the **/x** format. Range: /0 to /128 The **::** notation specifies successive hexadecimal fields of zeros

dampening	(OPTIONAL) Enter the keyword **dampening** to clear route flap dampening information.
flap-statistics	(OPTIONAL) Enter the keyword **flap-statistics** to reset the flap statistics on all prefixes from that neighbor.
peer-group	(OPTIONAL) Enter the keyword **peer-group** to clear all members of a peer-group.

Command Modes EXEC privilege

Command History

Version 7.4.1.0	Introduced

clear ip bgp ipv6 unicast dampening

C-Series	**No**
E-Series	✓

Clear information on route dampening.

Syntax **clear ip bgp dampening ipv6 unicast** *network network-mask*

Parameters

dampening	Enter the keyword **dampening** to clear route flap dampening information.
network	(OPTIONAL) Enter the network address in dotted decimal format (A.B.C.D).
network-mask	(OPTIONAL) Enter the network mask in slash prefix format (/x).

Command Modes EXEC privilege

Command History

Version 7.4.1.0	Introduced

clear ip bgp ipv6 unicast flap-statistics

C-Series	No
E-Series	✓

Clear BGP flap statistics, which includes number of flaps and the time of the last flap.

Syntax **clear ip bgp ipv6 unicast flap-statistics Network | filter-list** *list* |**regexp** *regexp*

Parameters

Network	(OPTIONAL) Enter the network address to clear flap statistics in dotted decimal format (A.B.C.D).
filter-list *list*	(OPTIONAL) Enter the keyword **filter-list** followed by the name of a configured AS-PATH list (max 16 characters).
regexp *regexp*	(OPTIONAL) Enter the keyword **regexp** followed by regular expressions. Use one or a combination of the following: . (period) matches on any single character, including white space * (asterisk) matches on sequences in a pattern (zero or more sequences) + (plus sign) matches on sequences in a pattern (one or more sequences) ? (question mark) matches sequences in a pattern (0 or 1 sequences) [ ] (brackets) matches a range of single-character patterns. ^ (caret) matches the beginning of the input string. (If the caret is used at the beginning of a sequence or range, it matches on everything BUT the characters specified.) $ (dollar sign) matches the end of the output string.

Command Modes EXEC privilege

Command History

Version 7.4.1.0	Introduced

debug ip bgp ipv6 unicast dampening

C-Series	No
E-Series	✓

View information on routes being dampened.

Syntax **debug ip bgp ipv6 unicast dampening**

To disable debugging, enter **no debug ip bgp ipv6 unicast dampening**

Parameters		
	dampening	Enter the keyword **dampening** to clear route flap dampening information.

Command Modes EXEC privilege

Command History

Version 7.4.1.0	Introduced

debug ip bgp ipv6 unicast peer-group updates

C-Series	No
E-Series	✓

View information about BGP peer-group updates.

debug ip bgp ipv6 unicast peer-group *peer-group-name* **updates** [**in** | **out**]

To disable debugging, enter **no debug ip bgp ipv6 unicast peer-group** *peer-group-name* **updates** [**in** | **out**] command.

Parameters		
	peer-group *peer-group-name*	Enter the keyword **peer-group** followed by the name of the peer-group.
	updates	Enter the keyword **updates** to view BGP update information.
	in	(OPTIONAL) Enter the keyword **in** to view only BGP updates received from neighbors.
	out	(OPTIONAL) Enter the keyword **out** to view only BGP updates sent to neighbors.

Command Modes EXEC privilege

Command History

Version 7.4.1.0	Introduced

debug ip bgp ipv6 unicast updates

C-Series	No
E-Series	✓

View information about BGP updates.

debug ip bgp ipv6 unicast *ipv6-address prefix-length* **updates** [**in** | **out**]

To disable debugging, enter **no debug ip bgp ipv6 unicast** *ipv6-address prefix-length* **updates** [**in** | **out**] command.

Parameters

ipv6-address prefix-length	Enter the IPv6 address in the **x:x:x:x::x** format followed by the prefix length in the **/x** format. Range: /0 to /128 The **::** notation specifies successive hexadecimal fields of zeros
updates	Enter the keyword **updates** to view BGP update information.
in	(OPTIONAL) Enter the keyword **in** to view only BGP updates received from neighbors.
out	(OPTIONAL) Enter the keyword **out** to view only BGP updates sent to neighbors.

Command Modes EXEC privilege

Command History

Version 7.4.1.0	Introduced

Defaults Disabled.

distance bgp

C-Series	No
E-Series	✓

Define an administrative distance for routes.

Syntax **distance bgp** *external-distance internal-distance local-distance*

To return to default values, enter **no distance bgp**.

Parameters

external-distance	Enter a number to assign to routes learned from a neighbor external to the AS. Range: 1 to 255. Default: 20
internal-distance	Enter a number to assign to routes learned from a router within the AS. Range: 1 to 255. Default: 200
local-distance	Enter a number to assign to routes learned from networks listed in the network command. Range: 1 to 255. Default: 200

Defaults *external-distance* = 20; *internal-distance* = 200; *local-distance* = 200.

Command Modes ROUTER BGP Address Family (conf-router_bgpv6-af)

Command History

Version 7.4.1.0	Introduced

Caution: Force10 Networks recommends that you do not change the administrative distance of internal routes. Changing the administrative distances may cause routing table inconsistencies.

Usage Information The higher the administrative distance assigned to a route means that your confidence in that route is low. Routes assigned an administrative distance of 255 are not installed in the routing table. Routes from confederations are treated as internal BGP routes.

neighbor activate

C-Series	**No**
E-Series	✓

This command allows the specified neighbor/peer group to be enabled for the current AFI/SAFI.

Syntax **neighbor** [*ipv6-address* | *peer-group-name*] **activate**

To disable, use the **no neighbor** [*ipv6-address* | *peer-group-name*] **activate** command.

Parameters

ipv6-address	(OPTIONAL) Enter the IPv6 address in the **x:x:x:x::x** format. The **::** notation specifies successive hexadecimal fields of zeros.
peer-group-name	(OPTIONAL) Enter the name of the peer group
activate	Enter the keyword **activate** to enable the neighbor/peer group in the new AFI/SAFI.

Defaults Disabled

Command Modes ROUTER BGP Address Family (conf-router_bgpv6-af)

Command History

Version 7.4.1.0	Introduced

Usage Information By default, when a neighbor/peer group configuration is created in the Router BGP context, it is enabled for the IPv6/Unicast AFI/SAFI. By using **activate** in the new context, the neighbor/peer group is enabled for AFI/SAFI.

Related Commands

address family	Changes the context to SAFI

neighbor advertisement-interval

C-Series	**No**
E-Series	✓

Set the advertisement interval between BGP neighbors or within a BGP peer group.

Syntax **neighbor** {*ipv6-address* | *peer-group-name*} **advertisement-interval** *seconds*

To return to the default value, use the **no neighbor** {*ipv6-address* | *peer-group-name*} **advertisement-interval** command.

Parameters

ipv6-address	(OPTIONAL) Enter the IPv6 address in the **x:x:x:x::x** format. The **::** notation specifies successive hexadecimal fields of zeros.
peer-group-name	Enter the name of the peer group to set the advertisement interval for all routers in the peer group.
seconds	Enter a number as the time interval, in seconds, between BGP advertisements. Range: 0 to 600 seconds. Default: 5 seconds for internal BGP peers; 30 seconds for external BGP peers.

Defaults *seconds* = 5 seconds (internal peers); *seconds* = 30 seconds (external peers)

Command Modes ROUTER BGP Address Family (conf-router_bgpv6-af)

Command History

Version 7.4.1.0	Introduced

neighbor default-originate

C-Series	No
E-Series	✓

Inject the default route to a BGP peer or neighbor.

Syntax **neighbor** {*ipv6-address* | *peer-group-name*} **default-originate** [**route-map** *map-name*]

To remove a default route, use the **no neighbor** {*ipv6-address* | *peer-group-name*} **default-originate** command.

Parameters

ipv6-address	(OPTIONAL) Enter the IPv6 address in the **x:x:x:x::x** format. The **::** notation specifies successive hexadecimal fields of zeros.
peer-group-name	Enter the name of the peer group to set the default route of all routers in that peer group.
route-map *map-name*	(OPTIONAL) Enter the keyword **route-map** followed by the name of a configured route map.

Defaults Not configured.

Command Modes ROUTER BGP Address Family (conf-router_bgpv6-af)

Command History

Version 7.4.1.0	Introduced

neighbor distribute-list

C-Series	No
E-Series	✓

Distribute BGP information via an established prefix list.

Syntax **neighbor** [*ipv6-address* | *peer-group-name*] **distribute-list** *prefix-list-name* [**in** | **out**]

To delete a neighbor distribution list, use the **no neighbor** [*ipv6-address* | *peer-group-name*] **distribute-list** *prefix-list-name* [**in** | **out**] command.

Parameters

ipv6-address	(OPTIONAL) Enter the IPv6 address in the **x:x:x:x::x** format. The **::** notation specifies successive hexadecimal fields of zeros.
peer-group-name	Enter the name of the peer group to apply the distribute list filter to all routers in the peer group.

prefix-list-name	Enter the name of an established prefix list. If the prefix list is not configured, the default is permit (to allow all routes).
in	Enter the keyword **in** to distribute only inbound traffic.
out	Enter the keyword **out** to distribute only outbound traffic.

Defaults Not configured.

Command Modes ROUTER BGP Address Family (conf-router_bgpv6-af)

Command History

Version 7.4.1.0	Introduced

Usage Information Other BGP filtering commands include: neighbor filter-list and neighbor route-map.

Related Commands

neighbor filter-list	Assign a AS-PATH list to a neighbor or peer group.
neighbor route-map	Assign a route map to a neighbor or peer group.

neighbor filter-list

C-Series	**No**
E-Series	✓

Configure a BGP filter based on the AS-PATH attribute.

Syntax **neighbor** [*ipv6-address* | *peer-group-name*] **filter-list aspath** *access-list-name* [**in** | **out**]

To delete a BGP filter, use the **no neighbor** [*ipv6-address* | *peer-group-name*] **filter-list aspath** *access-list-name* [**in** | **out**] command.

Parameters

ipv6-address	(OPTIONAL) Enter the IPv6 address in the **x:x:x:x::x** format. The **::** notation specifies successive hexadecimal fields of zeros.
peer-group-name	Enter the name of the peer group to apply the filter to all routers in the peer group.
access-list-name	Enter the name of an established AS-PATH access list. If the AS-PATH access list is not configured, the default is permit (to allow routes).
in	Enter the keyword **in** to filter inbound BGP routes.
out	Enter the keyword **out** to filter outbound BGP routes.

Defaults Not configured.

Command Modes ROUTER BGP Address Family (conf-router_bgpv6-af)

Command History

Version 7.4.1.0	Introduced

neighbor maximum-prefix

C-Series	**No**
E-Series	✔

Control the number of network prefixes received.

Syntax **neighbor** *ipv6-address* | *peer-group-name* **maximum-prefix** *maximum* [*threshold*] [**warning-only**]

To return to the default values, use the **no neighbor** *ipv6-address* | *peer-group-name* **maximum-prefix** *maximum* command.

Parameters

ipv6-address	(OPTIONAL) Enter the IPv6 address in the **x:x:x:x::x** format. The **::** notation specifies successive hexadecimal fields of zeros.
peer-group-name	(OPTIONAL) Enter the name of the peer group.
maximum	Enter a number as the maximum number of prefixes allowed for this BGP router. Range: 1 to 4294967295.
threshold	(OPTIONAL) Enter a number to be used as a percentage of the *maximum* value. When the number of prefixes reaches this percentage of the *maximum* value, the E-Series software sends a message. Range: 1 to 100 percent. Default: 75
warning-only	(OPTIONAL) Enter the keyword **warning-only** to set the router to send a log message when the maximum value is reached. If this parameter is not set, the router stops peering when the maximum number of prefixes is reached.

Defaults *threshold* = 75

Command Modes ROUTER BGP Address Family (conf-router_bgpv6-af)

Command History

Version 7.4.1.0	Introduced

neighbor next-hop-self

C-Series	No
E-Series	✓

Allows you to configure the router as the next hop for a BGP neighbor.

Syntax **neighbor** *ipv6-address* | *peer-group-name* **next-hop-self**

To return to the default setting, use the **no neighbor** *ipv6-address* | *peer-group-name* **next-hop-self** command.

Parameters

ipv6-address	(OPTIONAL) Enter the IPv6 address in the **x:x:x:x::x** format. The **::** notation specifies successive hexadecimal fields of zeros.
peer-group-name	(OPTIONAL) Enter the name of the peer group.

Defaults Disabled.

Command Modes ROUTER BGP Address Family (conf-router_bgpv6-af)

Command History

Version 7.4.1.0	Introduced

Usage Information If the set ipv6 next-hop command in the ROUTE-MAP mode is configured, its configuration takes precedence over the neighbor next-hop-self command.

neighbor remove-private-AS

C-Series	No
E-Series	✓

Remove private AS numbers from the AS-PATH of outgoing updates.

Syntax **neighbor** *ipv6-address* | *peer-group-name* **remove-private-as**

To return to the default, use the **no neighbor** *ipv6-address* | *peer-group-name* **remove-private-as** command.

Parameters

ipv6-address	(OPTIONAL) Enter the IPv6 address in the **x:x:x:x::x** format. The **::** notation specifies successive hexadecimal fields of zeros.
peer-group-name	(OPTIONAL) Enter the name of the peer group to remove the private AS numbers

Defaults Disabled (that is, private AS number are not removed).

Command Modes ROUTER BGP Address Family (conf-router_bgpv6-af)

Command History

Version 7.4.1.0	Introduced

neighbor route-map

C-Series	No
E-Series	✓

Apply an established route map to either incoming or outbound routes of a BGP neighbor or peer group.

Syntax **neighbor** *ipv6-address* | *peer-group-name* **route-map** *map-name* [**in** | **out**]

To remove the route map, use the **no neighbor** [*ipv6-address* | *peer-group-name*] **route-map** *map-name* [**in** | **out**] command.

Parameters

ipv6-address	(OPTIONAL) Enter the IPv6 address in the **x:x:x:x::x** format. The **::** notation specifies successive hexadecimal fields of zeros.
peer-group-name	(OPTIONAL) Enter the name of the peer group.
map-name	Enter the name of an established route map. If the Route map is not configured, the default is deny (to drop all routes).
in	Enter the keyword **in** to filter inbound routes.
out	Enter the keyword **out** to filter outbound routes.

Defaults Not configured.

Command Modes ROUTER BGP Address Family (conf-router_bgpv6-af)

Command History

Version 7.4.1.0	Introduced

Usage Information When you apply a route map to outbound routes, only routes that match at least one section of the route map are permitted.

If you identify a peer group by name, the peers in that peer group inherit the characteristics in the Route map used in this command. If you identify a peer by IP address, the Route map overwrites either the inbound or outbound policies on that peer.

neighbor route-reflector-client

C-Series	No
E-Series	✓

Configure a neighbor as a member of a route reflector cluster.

Syntax

neighbor *ipv6-address*| *peer-group-name* **route-reflector-client**

To indicate that the neighbor is not a route reflector client or to delete a route reflector configuration, use the **no neighbor** *ipv6-address* | *peer-group-name* **route-reflector-client** command.

Parameters

ipv6-address	(OPTIONAL) Enter the IPv6 address in the **x:x:x:x::x** format. The **::** notation specifies successive hexadecimal fields of zeros.
peer-group-name	(OPTIONAL) Enter the name of the peer group. All routers in the peer group receive routes from a route reflector.

Defaults

Not configured.

Command Modes

ROUTER BGP Address Family (conf-router_bgpv6-af)

Command History

Version 7.4.1.0	Introduced

Usage Information

The first time you enter this command it configures the neighbor as a route reflector and members of the route-reflector cluster. Internal BGP (IBGP) speakers do not need to be fully meshed if you configure a route reflector.

When all clients of a route reflector are disabled, the neighbor is no longer a route reflector.

network

C-Series	No
E-Series	✓

Specify the networks for the BGP process and enter them in the BGP routing table.

Syntax

network *ipv6-address* [**route-map** *map-name*]

To remove a network, use the **no network** *ipv6-address* [**route-map** *map-name*] command.

Parameters

ipv6-address	Enter the IPv6 address in the **x:x:x:x::x** format. The **::** notation specifies successive hexadecimal fields of zeros.
route-map *map-name*	(OPTIONAL) Enter the keyword **route-map** followed by the name of an established route map. Only the following ROUTE-MAP mode commands are supported: • match ipv6 address • match ipv6 next-hop • match ipv6 route-source • set ipv6 next-hop If the route map is not configured, the default is deny (to drop all routes).

Defaults

Not configured.

Command Modes

ROUTER BGP Address Family (conf-router_bgpv6-af)

Command History

Version 7.4.1.0	Introduced

Usage Information

The E-Series software resolves the network address configured by the network command with the routes in the main routing table to ensure that the networks are reachable via non-BGP routes and non-default routes.

Related Commands

redistribute	Redistribute routes into BGP.

redistribute

C-Series	**No**
E-Series	✓

Redistribute routes into BGP.

Syntax

redistribute [**connected** | **static**] [**route-map** *map-name*]

To disable redistribution, use the **no redistribution** [**connected** | **static**] [**route-map** *map-name*] command.

Parameters

connected	Enter the keyword **connected** to redistribute routes from physically connected interfaces.

static	Enter the keyword **static** to redistribute manually configured routes. These routes are treated as incomplete routes.
route-map *map-name*	(OPTIONAL) Enter the keyword **route-map** followed by the name of an established route map. Only the following ROUTE-MAP mode commands are supported: • match ipv6 address • match ipv6 next-hop • match ipv6 route-source • set ipv6 next-hop If the route map is not configured, the default is deny (to drop all routes).

Defaults Not configured.

Command Modes ROUTER BGP Address Family (conf-router_bgpv6-af)

Command History

Version 7.4.1.0	Introduced

Usage Information If you do not configure default-metric command, in addition to the redistribute command, or there is no route map to set the metric, the metric for redistributed static and connected is "0".

To redistribute the default route (0::0/0) configure the neighbor default-originate command.

Related Commands

neighbor default-originate	Inject the default route.

show ip bgp ipv6 unicast

C-Series	No
E-Series	✓

View the current MBGP routing table for the E-Series.

Syntax **show ip bgp ipv6 unicast** [*network* [*network-mask*] [**length**]]

Parameters

network	(OPTIONAL) Enter the network address (in dotted decimal format) of the BGP network to view information only on that network.
network-mask	(OPTIONAL) Enter the network mask (in slash prefix format) of the BGP network address.
longer-prefixes	(OPTIONAL) Enter the keyword **longer-prefixes** to view all routes with a common prefix.

Command Modes EXEC

EXEC privilege

Command History

Version 7.4.1.0	Introduced

Example

```
Force10#show ip bgp ipv6 unicast
BGP table version is 8, local router ID is 5.5.10.4
Status codes: s suppressed, S stale, d damped, h history, * valid, > best Path source: I - internal, a
- aggregate, c - confed-external, r - redistributed, n - network Origin codes: i - IGP, e - EGP, ? -
incomplete

     Network            Next Hop            Metric     LocPrf Weight Path
h    dead:1::/100       5ffe:10::3               0                  0 1 i
h                       5ffe:11::3               0                  0 1 i
*>   dead:2::/100       5ffe:10::3               0                  0 1 i
*                       5ffe:11::3               0                  0 1 i
*>   dead:3::/100       5ffe:10::3               0                  0 1 i
*                       5ffe:11::3               0                  0 1 i
h    dead:4::/100       5ffe:10::3               0                  0 1 i
h                       5ffe:11::3               0                  0 1 i
Force10#show ip bgp ipv6 unicast dead:3::/100

BGP routing table entry for dead:3::/100, version 3
Paths: (2 available, table Default-MBGP-Routing-Table.)
Not advertised to any peer

Received from :
  5ffe:10::3  (5.5.5.3)    Best
    AS_PATH :  1

    Next-Hop : 5ffe:10::3, Cost : 0
    Origin IGP, Metric  0, LocalPref  100, Weight  0, external

  5ffe:11::3  (5.5.5.3)
    AS_PATH :  1

    Next-Hop : 5ffe:11::3, Cost : 0
    Origin IGP, Metric  0, LocalPref  100, Weight  0, external
    Inactive reason: Peer IP address
Force10#
```

Figure 364 show ip bgp ipv6 unicast Example

Table 107 defines the information displayed in Figure 364.

Table 107 show ip bgp Command Example Fields

Field	Description
Network	Displays the destination network prefix of each BGP route.
Next Hop	Displays the next hop address of the BGP router. If 0::0/0 is listed in this column, then local routes exist in the routing table.
Metric	Displays the BGP route's metric, if assigned.
LocPrf	Displays the BGP LOCAL_PREF attribute for the route.
Weight	Displays the route's weight
Path	Lists all the ASs the route passed through to reach the destination network.

Related Commands		
	show ip bgp ipv6 unicast community	View BGP communities.

show ip bgp ipv6 unicast cluster-list

C-Series	No
E-Series	✓

View BGP neighbors in a specific cluster.

Syntax **show ip bgp ipv6 unicast cluster-list** [*cluster-id*]

Parameters

cluster-id	(OPTIONAL) Enter the cluster id in dotted decimal format.

Command Modes EXEC

EXEC privilege

Command History

Version 7.4.1.0	Introduced

show ip bgp ipv6 unicast community

C-Series	No
E-Series	✓

View information on all routes with Community attributes or view specific BGP community groups.

Syntax **show ip bgp ipv6 unicast community** [*community-number*] [**local-as**] [**no-export**] [**no-advertise**]

Parameters

community-number	Enter the community number in AA:NN format where AA is the AS number (2 bytes) and NN is a value specific to that autonomous system. You can specify up to eight community numbers to view information on those community groups.
local-AS	Enter the keywords **local-AS** to view all routes with the COMMUNITY attribute of NO_EXPORT_SUBCONFED. All routes with the NO_EXPORT_SUBCONFED (0xFFFFFF03) community attribute must not be advertised to external BGP peers.

no-advertise	Enter the keywords **no-advertise** to view all routes containing the well-known community attribute of NO_ADVERTISE. All routes with the NO_ADVERTISE (0xFFFFFF02) community attribute must not be advertised to other BGP peers.
no-export	Enter the keywords **no-export** to view all routes containing the well-known community attribute of NO_EXPORT. All routes with the NO_EXPORT (0xFFFFFF01) community attribute must not be advertised outside a BGP confederation boundary.

Command Modes

EXEC

EXEC privilege

Command History

Version 7.4.1.0	Introduced

Usage Information

To view the total number of COMMUNITY attributes found, use the show ip bgp ipv6 summary command. The text line above the route table states the number of COMMUNITY attributes found.

The show ip bgp community command without any parameters lists BGP routes with at least one BGP community attribute and the output is the same as for the show ip bgp ipv6 command output.

show ip bgp ipv6 unicast community-list

C-Series	No
E-Series	✓

View routes that are affected by a specific community list.

Syntax **show ip bgp ipv6 unicast community-list** *community-list-name*

Parameters

community-list-name	Enter the name of a configured IP community list.

Command Modes

EXEC

EXEC privilege

Command History

Version 7.4.1.0	Introduced

show ip bgp ipv6 unicast dampened-paths

C-Series	No
E-Series	✓

View BGP routes that are dampened (non-active).

Syntax **show ip bgp ipv6 unicast dampened-paths**

Command Modes EXEC

EXEC privilege

Command History

Version 7.4.1.0	Introduced

show ip bgp ipv6 unicast detail

C-Series	No
E-Series	✓

Display detailed BGP information.

Syntax **show ip bgp ipv6 unicast detail**

Command Modes EXEC

EXEC privilege

Command History

Version 7.5.1.0	Introduced

Example

```
R2_Training#show ip bgp ipv6 unicast detail

Detail information for BGP Node
bgpNdP 0x41a17000 : NdTmrP 0x41a17000 : NdKATmrP 0x41a17014 : NdTics 327741 :
NhLocAS 1 : NdState 2 : NdRPMPrim 1 : NdListSoc 13
NdAuto 1 : NdEqCost 1 : NdSync 0 : NdDefOrg 0
NdV6ListSoc 14 NdDefDid 0 : NdConfedId 0 : NdMedConfed 0 : NdMedMissVal -1 :
NdIgnrIllId 0 : NdRRC2C 1 : NdClstId 33686273 : NdPaTblP 0x41a19088
NdASPTblP 0x41a19090 : NdCommTblP 0x41a19098 : NhOptTransTblP 0x41a190a0 :
NdRRClsTblP 0x41a190a8
NdPktPA 0 : NdLocCBP 0x41a6f000 : NdTmpPAP 0x419efc80 : NdTmpASPAP 0x41a25000 :
NdTmpCommP 0x41a25800
NdTmpRRClP 0x41a4b000 : NdTmpOptP 0x41a4b800 : NdTmpNHP  : NdOrigPAP 0
NdOrgNHP 0 : NdModPathP 0x419efcc0 : NdModASPAP 0x41a4c000 : NdModCommP 0x41a4c800
NdModOptP 0x41a4d000 : NdModNHP  : NdComSortBufP 0x41a19110 : NdComSortHdP
0x41a19d04 : NdUpdAFMsk 0 : AFRstSe
t 0x41a1a298 : NHopDfrdHdP 0x41a1a3e0 : NumNhDfrd 0 : CfgHdrAFMsk 1
```

Figure 365 show ip bgp ipv6 unicast detail Command Example (Partial)

show ip bgp ipv6 unicast filter-list

C-Series	**No**
E-Series	✔

View the routes that match the filter lists.

Syntax **show ip bgp ipv6 unicast filter-list** *as-path-name*

Parameters

as-path-name	Enter the name of an AS-PATH.

Command Modes

EXEC

EXEC privilege

Command History

Version 7.4.1.0	Introduced

show ip bgp ipv6 unicast flap-statistics

C-Series	No
E-Series	✓

View flap statistics on BGP routes.

Syntax **show ip bgp ipv6 unicast flap-statistics** [*ipv6-address prefix-length*] [**filter-list** *as-path-name*] [**regexp** *regular-expression*]

Parameters

ipv6-address prefix-length	(OPTIONAL) Enter the IPv6 address in the **x:x:x:x::x** format followed by the prefix length in the **/x** format. Range: /0 to /128 The **::** notation specifies successive hexadecimal fields of zeros..
filter-list *as-path-name*	(OPTIONAL) Enter the keyword **filter-list** followed by the name of a configured AS-PATH ACL.
regexp *regular-expression*	Enter a regular expression then use one or a combination of the following characters to match: • **.** = (period) any single character (including a white space) • ***** = (asterisk) the sequences in a pattern (0 or more sequences) • **+** = (plus) the sequences in a pattern (1 or more sequences) • **?** = (question mark) sequences in a pattern (either 0 or 1 sequences). **You must enter an escape sequence (CTRL+v) prior to entering the ? regular expression.** • **[ ]** = (brackets) a range of single-character patterns. • **^** = (caret) the beginning of the input string. If the caret is used at the beginning of a sequence or range, it matches on everything BUT the characters specified. • **$** = (dollar sign) the end of the output string.

Command Modes EXEC

EXEC privilege

Command History

Version 7.4.1.0	Introduced

Example

```
Force10#show ip bgp ipv6 unicast flap-statistics
BGP table version is 8, local router ID is 5.5.10.4
Status codes: s suppressed, S stale, d damped, h history, * valid, > best Path
source: I - internal, a - aggregate, c - confed-external, r - redistributed, n -
network Origin codes: i - IGP, e - EGP, ? - incomplete

     Network             From             Flaps Duration Reuse     Path
h    dead:1::/100        5ffe:10::3       1     00:03:20           1 i
h    dead:1::/100        5ffe:11::3       1     00:03:20           1 i
h    dead:4::/100        5ffe:10::3       1     00:04:39           1 i
h    dead:4::/100        5ffe:11::3       1     00:04:39           1 i

Force10#
```

Figure 366 show ip bgp ipv6 unicast flap-statistics command Example

show ip bgp ipv6 unicast inconsistent-as

C-Series	No
E-Series	✓

View routes with inconsistent originating Autonomous System (AS) numbers, that is, prefixes that are announced from the same neighbor AS but with a different AS-Path.

Syntax **show ip bgp ipv6 unicast inconsistent-as**

Command Modes EXEC

EXEC privilege

Command History

Version 7.4.1.0	Introduced

show ip bgp ipv6 unicast neighbors

C-Series	No
E-Series	✓

Allows you to view the information exchanged by BGP neighbors.

Syntax **show ip bgp ipv6 unicast neighbors** [*ipv6-address prefix-length* [**advertised-routes** | **dampened-routes** | **detail** | **flap-statistics** | **routes**]]

Parameters

ipv6-address prefix-length	(OPTIONAL) Enter the IPv6 address in the **x:x:x:x::x** format followed by the prefix length in the **/x** format. Range: /0 to /128 The **::** notation specifies successive hexadecimal fields of zeros.
advertised-routes	(OPTIONAL) Enter the keywords **advertised-routes** to view only the routes the neighbor sent.
dampened-routes	(OPTIONAL) Enter the keyword **dampened-routes** to view information on dampened routes from the BGP neighbor.
flap-statistics	(OPTIONAL) Enter the keyword **flap-statistics** to view flap statistics on the neighbor's routes.
detail	(OPTIONAL) Display detailed neighbor information.
routes	(OPTIONAL) Enter the keywords **routes** to view only the neighbor's feasible routes.

Command Modes EXEC
EXEC privilege

Command History

Version 7.5.1.0	Modified: Added **detail** option; added information to output.
Version 7.4.1.0	Introduced

Example

```
Force10#show ip bgp ipv6 unicast neighbors

BGP neighbor is 5ffe:10::3, remote AS 1, external link
  BGP version 4, remote router ID 5.5.5.3
  BGP state ESTABLISHED, in this state for 00:00:32
  Last read 00:00:32, last write 00:00:32
  Hold time is 180, keepalive interval is 60 seconds
Received 1404 messages, 0 in queue
    3 opens, 1 notifications, 1394 updates
    6 keepalives, 0 route refresh requests
  Sent 48 messages, 0 in queue
    3 opens, 2 notifications, 0 updates
    43 keepalives, 0 route refresh requests
Minimum time between advertisement runs is 30 seconds
  Minimum time before advertisements start is 0 seconds

  Capabilities received from neighbor for IPv6 Unicast :
    MULTIPROTO_EXT(1)
    ROUTE_REFRESH(2)
    CISCO_ROUTE_REFRESH(128)

  Capabilities advertised to neighbor for IPv6 Unicast :
    MULTIPROTO_EXT(1)
    ROUTE_REFRESH(2)
    CISCO_ROUTE_REFRESH(128)

  For address family: IPv6 Unicast
  BGP table version 12, neighbor version 12
  2 accepted prefixes consume 32 bytes
Prefixes accepted 1 (consume 4 bytes), withdrawn 0 by peer
  Prefixes advertised 0, rejected 0, withdrawn 0 from peer

  Connections established 3; dropped 2
  Last reset 00:00:39, due to Closed by neighbor

  Notification History
   'OPEN error/Bad AS' Sent : 0  Recv: 1

Local host: 5ffe:10::4, Local port: 179
Foreign host: 5ffe:10::3, Foreign port: 35470

BGP neighbor is 5ffe:11::3, remote AS 1, external link
  BGP version 4, remote router ID 5.5.5.3
  BGP state ESTABLISHED, in this state for 00:00:28
  Last read 00:00:28, last write 00:00:28
  Hold time is 180, keepalive interval is 60 seconds
  Received 27 messages, 3 notifications, 0 in queue
  Sent 0 messages, 0 notifications, 0 in queue
  Received 8 updates, Sent 0 updates
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
  Minimum time before advertisements start is 0 seconds

  Capabilities received from neighbor for IPv6 Unicast :
    MULTIPROTO_EXT(1)
    ROUTE_REFRESH(2)
    CISCO_ROUTE_REFRESH(128)

  Capabilities advertised to neighbor for IPv6 Unicast :
    MULTIPROTO_EXT(1)
    ROUTE_REFRESH(2)
    CISCO_ROUTE_REFRESH(128)

  For address family: IPv6 Unicast
  BGP table version 12, neighbor version 12
  2 accepted prefixes consume 32 bytes
  Prefix advertised 0, rejected 0, withdrawn 0

  Connections established 3; dropped 2
  Last reset 00:00:41, due to Closed by neighbor

  Notification History
   'OPEN error/Bad AS' Sent : 0  Recv: 1

Local host: 5ffe:11::4, Local port: 179
```

Figure 367 show ip bgp ipv6 unicast neighbors Command Example (Partial)

Figure 108 defines the information displayed in Figure 367.

Table 108 show ip bgp neighbors Command Fields

Lines beginning with	Description
BGP neighbor	Displays the BGP neighbor address and its AS number. The last phrase in the line indicates whether the link between the BGP router and its neighbor is an external or internal one. If they are located in the same AS, then the link is internal; otherwise the link is external.
BGP version	Displays the BGP version (always version 4) and the remote router ID.
BGP state	Displays the neighbor's BGP state and the amount of time in hours:minutes:seconds it has been in that state.
Last read	This line displays the following information: • last read is the time (hours:minutes:seconds) the router read a message from its neighbor • hold time is the number of seconds configured between messages from its neighbor • keepalive interval is the number of seconds between keepalive messages to help ensure that the TCP session is still alive.
Received messages	This line displays the number of BGP messages received, the number of notifications (error messages) and the number of messages waiting in a queue for processing.
Sent messages	The line displays the number of BGP messages sent, the number of notifications (error messages) and the number of messages waiting in a queue for processing.
Received updates	This line displays the number of BGP updates received and sent.
Minimum time	Displays the minimum time, in seconds, between advertisements.
(list of inbound and outbound policies)	Displays the policy commands configured and the names of the Route map, AS-PATH ACL or Prefix list configured for the policy.
For address family:	Displays IPv6 Unicast as the address family.
BGP table version	Displays the which version of the primary BGP routing table the router and the neighbor are using.
accepted prefixes	Displays the number of network prefixes accepted by the router and the amount of memory used to process those prefixes.
Prefix advertised	Displays the number of network prefixes advertised, the number rejected and the number withdrawn from the BGP routing table.
Connections established	Displays the number of TCP connections established and dropped between the two peers to exchange BGP information.
Last reset	Displays the amount of time since the peering session was last reset. Also states if the peer resets the peering session. If the peering session was never reset, the word never is displayed.

Table 108 show ip bgp neighbors Command Fields (continued)

Lines beginning with	Description
Local host:	Displays the peering address of the local router and the TCP port number.
Foreign host:	Displays the peering address of the neighbor and the TCP port number.

Related Commands

show ip bgp ipv6	View the current BGP routing table.

show ip bgp ipv6 unicast peer-group

C-Series	No
E-Series	✓

Allows you to view information on the BGP peers in a peer group.

Syntax **show ip bgp ipv6 unicast peer-group** [*peer-group-name* [**summary**]]

Parameters

peer-group-name	(OPTIONAL) Enter the name of a peer group to view information about that peer group only.
summary	(OPTIONAL) Enter the keyword **summary** to view status information of the peers in that peer group. The output is the same as that found in show ip bgp ipv6 unicast summary command

Command Modes EXEC

EXEC privilege

Command History

Version 7.4.1.0	Introduced

Related Commands

neighbor peer-group (assigning peers)	Assign peer to a peer-group.
neighbor peer-group (creating group)	Create a peer group.

show ip bgp ipv6 unicast summary

C-Series	No
E-Series	✓

Allows you to view the status of all BGP connections.

Syntax **show ip bgp ipv6 unicast summary**

Command Modes EXEC

EXEC privilege

Command History

Version 7.4.1.0	Introduced

Example

```
Force10#show ip bgp ipv6 unicast summary
BGP router identifier 5.5.10.4, local AS number 100
BGP table version is 12, main routing table version 12
2 network entrie(s) and 4 paths using 536 bytes of memory
1 BGP path attribute entrie(s) using 112 bytes of memory
1 BGP AS-PATH entrie(s) using 39 bytes of memory
Dampening enabled. 0 history paths, 0 dampened paths, 0 penalized paths

Neighbor        AS     MsgRcvd  MsgSent     TblVer  InQ  OutQ Up/Down  State/Pfx

5ffe:10::3      1           28        0         12    0     0 00:01:01         2
5ffe:11::3      1           27        0         12    0     0 00:00:55         2
Force10#
```

Figure 368 show ip bgp summary Command Example

Table 109 defines the information displayed in Figure 368.

Table 109 show ip bgp summary Command Fields

Field	Description
BGP router identifier	Displays the local router ID and the AS number.
BGP table version	Displays the BGP table version and the main routing table version.
network entries	Displays the number of network entries and route paths and the amount of memory used to process those entries.
BGP path attribute entries	Displays the number of BGP path attributes and the amount of memory used to process them.
BGP AS-PATH entries	Displays the number of BGP AS_PATH attributes processed and the amount of memory used to process them.
BGP community entries	Displays the number of BGP COMMUNITY attributes processed and the amount of memory used to process them. The show ip bgp community command provides more details on the COMMUNITY attributes.
Dampening enabled	Displayed only when dampening is enabled. Displays the number of paths designated as history, dampened, or penalized.

Table 109 show ip bgp summary Command Fields

Field	Description
Neighbor	Displays the BGP neighbor address.
AS	Displays the AS number of the neighbor.
MsgRcvd	Displays the number of BGP messages that neighbor received.
MsgSent	Displays the number of BGP messages that neighbor sent.
TblVer	Displays the version of the BGP table that was sent to that neighbor.
InQ	Displays the number of messages from that neighbor waiting to be processed.
OutQ	Displays the number of messages waiting to be sent to that neighbor. If a number appears in parentheses, the number represents the number of messages waiting to be sent to the peer group.
Up/Down	Displays the amount of time (in hours:minutes:seconds) that the neighbor is in the Established stage. If the neighbor has never moved into the Established stage, the word never is displayed.
State/Pfx	If the neighbor is in Established stage, the number of network prefixes received. If a maximum limit was configured with the neighbor maximum-prefix command, (prfxd) appears in this column. If the neighbor is not in Established stage, the current stage is displayed (Idle, Connect, Active, OpenSent, OpenConfirm) When the peer is transitioning between states and clearing the routes received, the phrase (Purging) may appear in this column. If the neighbor is disabled, the phrase (Admin shut) appears in this column.

Chapter 44 Quality of Service

FTOS commands for Quality of Service (QoS) includes traffic conditioning and congestion control.

- Per-Port QoS on page 1219
- Policy-Based QoS on page 1227
- Queue Level Debugging on page 1264 (**E-Series Only**)

Per-Port QoS

Per-Port QoS allows users to defined QoS configuration on a per-physical-port basis. The commands include:

- dot1p-priority on page 1219
- rate limit on page 1220
- rate police on page 1221
- rate shape on page 1223
- service-class dynamic dot1p on page 1223
- show interfaces rate on page 1224
- strict-priority queue on page 1226

dot1p-priority

Assign a value to the IEEE 802.1p bits on the traffic received by this interface.

Syntax **dot1p-priority** *priority-value*

To delete the IEEE 802.1p configuration on the interface, enter **no dot1p-priority**.

Parameters

priority-value For the **E-Series**, enter a value from 0 to 7.

dot1p	Queue Number
0	2
1	0
2	1
3	3
4	4
5	5
6	6
7	7

For the **C-Series**, enter a value 0, 2, 4, or 6

dot1p	Queue Number
0	1
2	0
4	2
6	3

Defaults No default behavior or values

Command Modes INTERFACE

Usage Information The dot1p-priority command changes the priority of incoming traffic on the interface. The system places traffic marked with a priority in the correct queue and processes that traffic according to its queue.

When you set the priority for a Port Channel, the physical interfaces assigned to the Port Channel are configured with the same value. You cannot assign dot1p-priority command to individual interfaces in a Port Channel.

rate limit

C-Series	No
E-Series	✓

Limit the outgoing traffic rate.

Syntax **rate limit** *committed-rate* [*burst-KB*] [**peak** *peak-rate* [*burst-KB*]] [**vlan** *vlan-id*]

To remove rate limiting, enter **no rate limit** *committed-rate* [*burst-KB*] [**peak** *peak-rate* [*burst-KB*]] [**vlan** *vlan-id*] command.

Parameters

committed-rate	Enter the bandwidth in Mbps Range: 0 to 10000
burst-KB	(OPTIONAL) Enter the burst size in KB. Range: 16 to 200000 Default: 50
peak *peak-rate*	(OPTIONAL) Enter the keyword **peak** followed by a number to specify the peak rate in Mbps. Range: 0 to 10000
vlan *vlan-id*	(OPTIONAL) Enter the keyword **vlan** followed by a VLAN ID to limit traffic to those specific VLANs. Range: 1 to 4094

Defaults No default behavior or values

Command Modes INTERFACE

Usage Information

Note: Per Port rate limit and rate police is supported for Layer 2 tagged and untagged switched traffic and for Layer 3 traffic. Per VLAN rate limit and rate police is supported on only tagged ports with Layer 2 switched traffic.

On one interface, you can configure the rate limit or rate police command for a VLAN or you can configure the rate limit or the rate police command for the interface. For each physical interface, you can configure six rate limit commands specifying different VLANS.

If you receive the error message:

```
%Error: Specified VLANs overlap with existing config.
```

after configuring VLANs in the rate police command, check to see if the same VLANs are used in rate limit command on other interfaces. To clear the problem, remove the rate limit configuration(s), and re-configure the rate police command. After the rate police command is configured, return to the other interfaces and re-apply the rate limit configuration.

rate police

Police the incoming traffic rate.

Syntax **rate police** *committed-rate* [*burst-KB*] [**peak** *peak-rate* [*burst-KB*]] [**vlan** *vlan-id*]

To remove rate policing, use the **no rate police** *committed-rate* [*burst-KB*] [**peak** *peak-rate* [*burst-KB*]] [**vlan** *vlan-id*] command.

Parameters

committed-rate	Enter a number as the bandwidth in Mbps. Range: 0 to 10000
burst-KB	(OPTIONAL) Enter a number as the burst size in KB. Range: 16 to 200000 Default: 50
peak *peak-rate*	(OPTIONAL) Enter the keyword **peak** followed by a number to specify the peak rate in Mbps. Range: 0 to 10000
vlan *vlan-id*	(OPTIONAL) Enter the keyword vlan followed by a VLAN ID to police traffic to those specific VLANs. Range: 1 to 4094

Defaults

No default behavior or values

Command Mode

INTERFACE

Usage Information

Note: Per Port rate limit and rate police is supported for Layer 2 tagged and untagged switched traffic and for Layer 3 traffic. Per VLAN rate limit and rate police is supported on only tagged ports with Layer 2 switched traffic.

C-Series

On *one* C-Series interface, you can configure the rate police command for a VLAN or you can configure the rate police command for an interface. For each physical interface, you can configure three rate police commands specifying different VLANS.

E-Series

On *one* E-Series interface, you can configure the rate limit or rate police command for a VLAN or you can configure the rate limit or the rate police command for the interface.

For each physical interface, you can configure six rate police commands specifying different VLANS.

If you receive the error message:

```
%Error: Specified VLANs overlap with existing config.
```

after configuring VLANs in the rate police command, check to see if the same VLANs are used in rate limit command on other interfaces. To clear the problem, remove the rate limit configuration(s), and re-configure the rate police command. After the rate police command is configured, return to the other interfaces and re-apply the rate limit configuration.

rate shape

C-Series	No
E-Series	✓

Shape the interface's traffic output.

Syntax **rate shape** *rate* [*burst-KB*]

To delete the command, use the **no rate shape** *rate* command.

Parameters

rate	Enter the outgoing rate in multiples of 10 Mbps. Range: 0 to 10000
burst-KB	(OPTIONAL) Enter a number as the burst size in KB. Range: 0 to 10000 Default: 10

Defaults No default behavior or values

Command Modes INTERFACE

service-class dynamic dot1p

Set the software to honor all incoming 802.1p markings on incoming switched traffic on this interface.

Syntax **service-class dynamic dot1p**

To return to the default setting, enter **no service-class dynamic dot1p**.

Defaults Not enabled (that is, the 802.1p markings on incoming traffic are not honored).

Command Modes INTERFACE

Command History

Version 6.5.1.0	Expanded command to permit configuration on port channels

Usage Information Enter this command to honor all incoming 802.1p markings, on incoming switched traffic, on the interface. By default, this facility is not enabled (that is, the 802.1p markings on incoming traffic are not honored).

This command can now be applied on both physical interfaces and port channels. When you set the service-class dynamic for a port channel, the physical interfaces assigned to the port channel are configured with this configuration. You cannot assign the service-class dynamic command to individual interfaces in a port channel.

show interfaces rate

C-Series	No
E-Series	✓

View information of either rate limiting or rate policing on the interface.

Syntax **show interfaces** [*interface*] **rate** [**limit** | **police**]

Parameters

interface	(OPTIONAL) Enter the following keywords and slot/port or number information: • For a 100/1000 Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For a SONET interface, enter the keyword **sonet** followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information.
limit	(OPTIONAL) Enter the keyword **limit** to view the outgoing traffic rate.
police	(OPTIONAL) Enter the keyword **police** to view the incoming traffic rate.

Command Mode EXEC

EXEC privilege

Example

```
Force10#show interfaces gigabitEthernet 1/1 rate limit
  Rate limit 300 (50) peak 800 (50)
    Traffic Monitor 0: normal 300 (50) peak 800 (50)
      Out of profile yellow 23386960 red 320605113
    Traffic Monitor 1: normal NA peak NA
      Out of profile yellow 0 red 0
    Traffic Monitor 2: normal NA peak NA
      Out of profile yellow 0 red 0
    Traffic Monitor 3: normal NA peak NA
      Out of profile yellow 0 red 0
    Traffic Monitor 4: normal NA peak NA
      Out of profile yellow 0 red 0
    Traffic Monitor 5: normal NA peak NA
      Out of profile yellow 0 red 0
    Traffic Monitor 6: normal NA peak NA
      Out of profile yellow 0 red 0
    Traffic Monitor 7: normal NA peak NA
      Out of profile yellow 0 red 0
    Total: yellow 23386960 red 320605113
```

Figure 369 show interfaces rate limit Command Example

Table 110 describes the information found in Figure 369.

Table 110 show interfaces Command Example Fields

Field	Description
Rate limit	Committed rate (Mbs) and burst size (KB) of the committed rate
peak	Peak rate (Mbs) and burst size (KB) of the peak rate
Traffic monitor 0	Traffic coming to class 0
Normal	Committed rate (Mbs) and burst size (KB) of the committed rate
peak	Peak rate (Mbs) and burst size (KB) of the peak rate
Out of profile Yellow	Number of packets that have exceeded the configured committed rate
Out of profile Red	Number of packets that have exceeded the configured peak rate
Traffic monitor 1	Traffic coming to class 1
Traffic monitor 2	Traffic coming to class 2
Traffic monitor 3	Traffic coming to class 3
Traffic monitor 4	Traffic coming to class 4
Traffic monitor 5	Traffic coming to class 5
Traffic monitor 6	Traffic coming to class 6
Traffic monitor 7	Traffic coming to class 7
Total: yellow	Total number of packets that have exceeded the configured committed rate
Total: red	Total number of packets that have exceeded the configured peak rate

```
Force10#show interfaces gigabitEthernet 1/2 rate police
  Rate police 300 (50) peak 800 (50)
    Traffic Monitor 0: normal 300 (50) peak 800 (50)
      Out of profile yellow 23386960 red 320605113
    Traffic Monitor 1: normal NA peak NA
      Out of profile yellow 0 red 0
    Traffic Monitor 2: normal NA peak NA
      Out of profile yellow 0 red 0
    Traffic Monitor 3: normal NA peak NA
      Out of profile yellow 0 red 0
    Traffic Monitor 4: normal NA peak NA
      Out of profile yellow 0 red 0
    Traffic Monitor 5: normal NA peak NA
      Out of profile yellow 0 red 0
    Traffic Monitor 6: normal NA peak NA
      Out of profile yellow 0 red 0
    Traffic Monitor 7: normal NA peak NA
      Out of profile yellow 0 red 0
    Total: yellow 23386960 red 320605113
```

Figure 370 show interfaces rate police Command Example

Table 111 describes the information found in Figure 370.

Table 111 show interfaces police Command Example Fields

Field	Description
Rate police	Committed rate (Mbs) and burst size (KB) of the committed rate
peak	Peak rate (Mbs) and burst size (KB) of the peak rate
Traffic monitor 0	Traffic coming to class 0

Table 111 show interfaces police Command Example Fields (continued)

Field	Description
Normal	Committed rate (Mbs) and burst size (KB) of the committed rate
peak	Peak rate (Mbs) and burst size (KB) of the peak rate
Out of profile Yellow	Number of packets that have exceeded the configured committed rate
Out of profile Red	Number of packets that have exceeded the configured peak rate
Traffic monitor 1	Traffic coming to class 1
Traffic monitor 2	Traffic coming to class 2
Traffic monitor 3	Traffic coming to class 3
Traffic monitor 4	Traffic coming to class 4
Traffic monitor 5	Traffic coming to class 5
Traffic monitor 6	Traffic coming to class 6
Traffic monitor 7	Traffic coming to class 7
Total: yellow	Total number of packets that have exceeded the configured committed rate
Total: red	Total number of packets that have exceeded the configured peak rate

strict-priority queue

Configure a unicast queues as a strict-priority (SP) queue.

Syntax **strict-priority queue unicast queue** *number*

Parameters

unicast queue *number*	Enter the keyword **unicast** followed by the queue number. **C-Series** Range: 1 to 3 **E-Series** Range: 1 to 7

Defaults No default behavior or value

Command Modes CONFIGURATION

Usage Information Once a unicast queue is configured as strict-priority, that particular queue, on the entire chassis, is treated as strict-priority queue. Traffic for a strict priority is scheduled before any other queues are serviced. For example, if you send 100% line rate traffic over the SP queue, it will *starve* all other queues on the ports on which this traffic is flowing.

Policy-Based QoS

Policy-based traffic classification is handled by using class maps. These maps classify unicast traffic to one of eight classes in E-Series and one of four classes in C-Series. FTOS enables you to match multiple class maps and specify multiple match criteria. Policy-based QoS is not supported on logical interfaces, such as port-channels, VLANS, or loopbacks. The commands are:

- bandwidth-percentage on page 1228
- class-map on page 1228
- clear qos statistics on page 1229
- match ip access-group on page 1230
- match ip dscp on page 1231
- match ip precedence on page 1232
- match mac access-group on page 1233
- match mac dot1p on page 1233
- policy-aggregate on page 1234
- policy-map-input on page 1235
- policy-map-output on page 1236
- qos-policy-input on page 1236
- qos-policy-name on page 1237
- qos-policy-output on page 1237
- queue egress on page 1238
- queue ingress on page 1240
- rate-limit on page 1241
- rate-police on page 1241
- rate-shape on page 1242
- service-policy input on page 1243
- service-policy output on page 1243
- service-queue on page 1244
- set on page 1245
- show cam layer2-qos on page 1245
- show cam layer3-qos on page 1247
- show qos class-map on page 1248
- show qos policy-map on page 1249
- show qos policy-map-input on page 1251
- show qos policy-map-output on page 1252
- show qos qos-policy-input on page 1253
- show qos qos-policy-output on page 1253
- show qos statistics on page 1254
- show qos wred-profile on page 1257
- test cam-usage on page 1258

- threshold on page 1260
- trust on page 1261
- wred on page 1262
- wred-profile on page 1263

bandwidth-percentage

C-Series	No
E-Series	✓

Assign a percentage of weight to class/queue.

Syntax **bandwidth-percentage** *percentage*

To remove the bandwidth percentage, use the **no bandwidth-percentage** command.

Parameters

percentage	Enter the percentage assignment of weight to class/queue. Range: 0 to 100% (granularity 1%)

Defaults No default behavior or values

Command Modes CONFIGURATION (conf-qos-policy-out)

Usage Information The unit of bandwidth percentage is 1%. A bandwidth percentage of 0 is allowed and will disable the scheduling of that class. If the sum of the bandwidth percentages given to all eight classes exceeds 100%, the bandwidth percentage will automatically scale down to 100%.

class-map

Create a class map to match packets to a specified class.

Syntax **class-map** {**match-all** | **match-any**} *class-map-name* [**layer2**]

To delete an existing class map, use the **no class-map** {**match-all** | **match-any**} *class-map-name* [**layer2**] command.

Parameters

match-all	Determines how packets are evaluated when multiple match criteria exist. Enter the keyword **match-all** to determine that the packets must meet all the match criteria in order to be considered a member of the class.
match-any	Determines how packets are evaluated when multiple match criteria exist. Enter the keyword **match-any** to determine that the packets must meet at least one of the match criteria in order to be considered a member of the class.
class-map-name	Enter a name of the class for the class map in a character format (16 character maximum).
layer2	**E-Series Only**—(OPTIONAL) Enter the keyword **layer2** to specify a Layer 2 Class Map. Default: Layer 3

Defaults Layer 3

Command Modes CONFIGURATION

Command History

Version 7.4.1.0	E-Series Only: Expanded to add support for Layer 2

Usage Information Packets arriving at the input interface are checked against the match criteria, configured using this command, to determine if the packet belongs to that class. This command enables the class-map configuration mode—(config-class-map).

Related Commands

match ip access-group	Configure the match criteria based on the access control list (ACL)
match ip precedence	Identify IP precedence values as match criteria
match ip dscp	Configure the match criteria based on the DSCP value

clear qos statistics

Clears Matched Packets, Matched Bytes, and Dropped Packets. For TeraScale, clears Matched Packets, Matched Bytes, Queued Packets, Queued Bytes, and Dropped Packets.

Syntax **clear qos statistics** *interface-name*.

Parameters

interface-name	Enter one of the following keywords: • For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information.

Defaults No default behavior or values

Command Modes EXEC

EXEC privilege

Usage Information

E-Series Only Behavior

If a Policy QoS is applied on an interface when **clear qos statistics** is issued, it will clear the egress counters in show queue statistics and vice-versa. This behavior is due to the values being read from the same hardware registers.

The **clear qos statistics** command clears both the queued and matched byte and packet counters if the queued counters incremented based on classification of packets to the queues because of policy-based QoS. If the queued counters were incremented because of some other reason and do not reflect a matching QoS entry in CAM, then this command clears the matched byte and packet counters only.

Related Commands

show qos statistics	Display qos statistics.

match ip access-group

Configure match criteria, for a class map, based on the contents of the ACL (access control list).

Syntax **match ip access-group** *access-group-name* [**set-ip-dscp** *value*]

To remove ACL match criteria from a class map, enter **no match ip access-group** *access-group-name* [**set-ip-dscp** *value*] command.

Parameters

access-group-name	Enter the ACL name whose contents are used as the match criteria in determining if packets belong to the class specified by **class-map**.
set-ip-dscp *value*	(OPTIONAL) Enter the keyword **set-ip-dscp** followed by the IP DSCP value. The matched traffic will be marked with the DSCP value. Range: 0 to 63

Defaults No default behavior or values

Command Modes CONFIGURATION (config-class-map)

Command History

Version 7.5.1.0	Added support for DSCP Marking option

Usage Information

You must enter the **class-map** command before using this command. Once the class map is identified, you can configure the match criteria. For **class-map match-any**, a maximum of five ACL match criteria is allowed. For **class-map match-all**, only one ACL match criteria is allowed.

Related Commands

class-map	Identify the class map.

match ip dscp

Use a DSCP (Differentiated Service Code Point) value as a match criteria.

Syntax

match ip dscp *dscp-list* [**set-ip-dscp** *value*]

To remove a DSCP value as a match criteria, enter **no match ip dscp** *dscp-list* [**set-ip-dscp** *value*] command.

Parameters

dscp-list	Enter the IP DSCP value(s) that is to be the match criteria. Separate values by commas—no spaces (1,2,3) or indicate a list of values separated by a hyphen (1-3). Range: 0 to 63
set-ip-dscp *value*	(OPTIONAL) Enter the keyword **set-ip-dscp** followed by the IP DSCP value. The matched traffic will be marked with the DSCP value. Range: 0 to 63

Defaults

No default behavior or values

Command Modes

CONFIGURATION (config-class-map)

Command History

Version 7.5.1.0	Added support for DSCP Marking option

Usage Information

The **match ip dscp** command and the **match ip precedence** command are mutually exclusive.

Up to 64 IP DSCP values can be matched in one match statement. For example, to indicate IP DCSP values 0 1 2 3 4 5 6 7 enter either the command **match ip dscp 0,1,2,3,4,5,6,7** or **match ip dscp 0-7.**

Note: Only one of the IP DSCP values must be a successful match criterion, not all of the specified IP DSCP values need to match.

Related Commands		
	class-map	Identify the class map.

match ip precedence

Use IP precedence values as a match criteria.

Syntax **match ip precedence** *ip-precedence-list* [**set-ip-dscp** *value*]

To remove IP precedence as a match criteria, enter **no match ip precedence** *ip-precedence-list* [**set-ip-dscp** *value*] command.

Parameters

ip-precedence-list	Enter the IP precedence value(s) that is to be the match criteria. Separate values by commas—no spaces (1,2,3) or indicated a list of values separated by a hyphen (1-3). Range: 0 to 7
set-ip-dscp *value*	(OPTIONAL) Enter the keyword **set-ip-dscp** followed by the IP DSCP value. The matched traffic will be marked with the DSCP value. Range: 0 to 63

Defaults No default behavior or values

Command Modes CONFIGURATION (conf-class-map)

Command History

Version 7.5.1.0	Added support for DSCP Marking option

Usage Information The **match ip precedence** command and the **match ip dscp** command are mutually exclusive.

Up to 8 precedence values can be matched in one match statement. For example, to indicate the IP precedence values 0 1 2 3 enter either the command **match ip precedence 0-3** or **match ip precedence 0,1,2,3**.

Note: Only one of the IP precedence values must be a successful match criterion, not all of the specified IP precedence values need to match.

Related Commands		
	class-map	Identify the class map.

match mac access-group

C-Series	No
E-Series	✓

Configure a match criterion for a class map, based on the contents of the MAC ACL.

Syntax **match mac access-group** {*mac-acl-name* }

To remove the match criterion, use the **no match mac access-group** {*mac-acl-name* } command.

Parameters

mac-acl-name	Enter the MAC ACL name whose contents are used as the match criteria in the class-map.

Defaults No default values or behavior

Command Modes CONFIGURATION (config-class-map)

Command History

Version 7.4.1.0	Introduced

match mac dot1p

C-Series	No
E-Series	✓

Configure a match criterion for a class map, based on the dot1p values.

Syntax **match mac dot1p** {*dot1p-list*}

To remove the match criterion, use the **no match mac dot1p** {*dot1p-list*} command.

Parameters

dot1p-list	Enter the dot1p values.

Defaults No default values or behavior

Command Modes CONFIGURATION (config-class-map)

Command History

Version 7.4.1.0	Introduced

policy-aggregate

This command allows an aggregate method of configuring per port QoS via the QoS policy maps. An aggregate QoS policy is part of the policy map (input/output) applied on an interface.

Syntax **policy-aggregate** *qos-policy-name*

To remove a policy aggregate configuration, use **no policy-aggregate** *qos-policy-name* command.

Parameters

qos-policy-name	Enter the name of the policy map in character format (16 characters maximum)

Defaults No default behavior or values

Command Modes CONFIGURATION (policy-map-input and policy-map-output)

Usage Information

C-Series

Aggregate input/output QoS policy applies to all the port ingoing/outgoing traffic. Aggregate input/output QoS policy can co-exist with per queue input/output QoS policies.

1. If only aggregate input QoS policy exists, input traffic conditioning configurations (rate-police) will apply. Any marking configurations in aggregate input QoS policy will be ignored.
2. If aggregate input QoS policy and per class input QoS policy co-exist, then aggregate input QoS policy will preempt per class input QoS policy on input traffic conditioning (rate-police). In other words, if rate police configuration exists in aggregate QoS policy, the rate police configurations in per class QoS are ignored. Marking configurations in per class input QoS policy still apply to each queue.

E-Series

Aggregate input/output QoS policy applies to all the port ingoing/outgoing traffic. Aggregate input/output QoS policy can co-exist with per queue input/output QoS policies.

1. If only aggregate input QoS policy exists, input traffic conditioning configurations (rate-police) will apply. Any marking configurations in aggregate input QoS policy will be ignored.
2. If aggregate input QoS policy and per class input QoS policy co-exist, then aggregate input QoS policy will preempt per class input QoS policy on input traffic conditioning (rate-police). In other words, if rate police configuration exists in aggregate QoS policy, the rate police configurations in per class QoS are ignored. Marking configurations in per class input QoS policy still apply to each queue.
3. If only aggregate output QoS policy exists, egress traffic conditioning configurations (rate-limit and rate-shape) configurations in aggregate output QoS policy

will apply. Scheduling and queuing configurations in aggregate output QoS policy (if exist) are ignored. Each queue will use default scheduling and queuing configuration (WRED and Bandwidth).

4. If aggregate output QoS policy and per queue output QoS policy co-exist, the aggregate output QoS policy will preempt per queue output QoS policy on egress traffic conditioning (rate-limit). In other words, if rate limit configuration exists in aggregate output QoS policy, the rate limit configurations in per queue output QoS policies are ignored. Scheduling and queuing configurations (WRED and Bandwidth) in per queue output QoS policy still apply to each queue.

Related Commands

policy-map-input	Create an inputy policy map
policy-map-output	Create an output policy map (E-Series Only)

policy-map-input

Create an input policy map.

Syntax **policy-map-input** *policy-map-name* [**layer2**]

To remove an input policy map, use the **no policy-map-input** *policy-map-name* [**layer2**] command.

Parameters

policy-map-name	Enter the name for the policy map in character format (16 characters maximum).
layer2	**E-Series Only**—(OPTIONAL) Enter the keyword **layer2** to specify a Layer 2 Class Map. Default: Layer 3

Defaults Layer 3

Command Modes CONFIGURATION

Command History

Version 7.4.1.0	E-Series Only: Expanded to add support for Layer 2

Usage Information Input policy map is used to classify incoming traffic to different flows using class-map, QoS policy, or simply using incoming packets DSCP. This command enables policy-map-input configuration mode (conf-policy-map-in).

policy-map-output

C-Series	No
E-Series	✓

Create an output policy map.

Syntax **policy-map-output** *policy-map-name*

To remove a policy map, use the **no policy-map-output** *policy-map-name* command.

Parameters

policy-map-name	Enter the name for the policy map in character format (16 characters maximum).

Defaults No default behavior or values

Command Modes CONFIGURATION

Usage Information Output policy map is used to assign traffic to different flows using QoS policy. This command enables the policy-map-output configuration mode (conf-policy-map-out).

qos-policy-input

Create a QoS input policy on the router.

Syntax **qos-policy-input** *qos-policy-name* [**layer2**]

To remove an existing input QoS policy from the router, use **no qos-policy-input** *qos-policy-name* [**layer2**] command.

Parameters

qos-policy-name	Enter your input QoS policy name in character format (16 character maximum).
layer2	**E-Series Only**—(OPTIONAL) Enter the keyword **layer2** to specify a Layer 2 Class Map. Default: Layer 3

Defaults Layer 3

Command Modes CONFIGURATION

Command History

Version 7.4.1.0	E-Series Only: Expanded to add support for Layer 2

Usage Information Use this command to specify the name of the input QoS policy. Once input policy is specified, rate-police can be defined. This command enables the qos-policy-input configuration mode—(conf-qos-policy-in).

Related Commands

rate-police	Incoming traffic policing function

qos-policy-name

C-Series	**No**
E-Series	✓

This specifies the input QoS policy assigned in the policy-map-input context.

Syntax **qos-policy-name** *qos-policy-name*

To remove an existing input QoS policy from the router, use **no qos-policy-input** *qos-policy-name* command.

Parameters

qos-policy-name	Enter your input QoS policy name in character format (16 character maximum).

Defaults No default behavior or values

Command Modes CONFIGURATION

Usage Information Use this command to specify the name of the input QoS policy. Once input policy is specified, rate-police can be defined. This command enables the qos-policy-input configuration mode—(conf-qos-policy-in).

qos-policy-output

C-Series	**No**
E-Series	✓

Create a QoS output policy on the router.

Syntax **qos-policy-output** *qos-policy-name*

To remove an existing output QoS policy from the router, use **no qos-policy-output** *qos-policy-name* command.

Parameters

qos-policy-name	Enter your output QoS policy name in character format (16 character maximum).

Defaults No default behavior or values

Command Modes CONFIGURATION

Usage Information Use this command to specify the name of the output QoS policy. Once output policy is specified, rate-limit, bandwidth-percentage, and WRED can be defined. This command enables the qos-policy-output configuration mode—(conf-qos-policy-out).

Related Commands

rate-limit	Outgoing traffic rate-limit functionality
bandwidth-percentage	Assign weight to class/queue percentage
wred	Assign yellow or green drop precedence

queue egress

C-Series	**No**
E-Series	✓

Assign a WRED Curve to all eight egress Multicast queues or designate the percentage for the Multicast bandwidth queue.

Syntax **queue egress multicast linecard** {*slot number* **port-set** *number* | **all**} [**wred-profile** *name* | **multicast-bandwidth** *percentage*]

To return to the default, use the **no queue egress multicast linecard** {*slot number* **port-set** *number* | **all**} [**wred-profile** *name* | **multicast-bandwidth** *percentage*] command.

Parameters

linecard *number*	Enter the keyword **linecard** followed by the line card slot number. E-Series Range: 0 to 13 on a E1200, 0 to 6 on a E600/E600i, and 0 to 5 on a E300.
port-set *number*	Enter the keyword **port-set** followed by the line card's port pipe. Range: 0 or 1
all	Enter the keyword **all** to apply to all line cards.

wred-profile *name*	(OPTIONAL) Enter the keyword **wred-profile** followed by your WRED profile name in character format (16 character maximum). Or use one of the pre-defined WRED profile names. Pre-defined Profiles: wred_drop, wred-ge_y, wred_ge_g, wred_teng_y, wred_teng_g
multicast-bandwidth *percentage*	(OPTIONAL) Enter the keyword **multicast-bandwidth** followed by the bandwidth percentage. Range: 0 to 100%

Defaults

No default behavior or values

Command Modes

CONFIGURATION

Command History

Version 7.5.1.0	Added support for multicast-bandwidth
Version 7.4.1.0 and 6.5.3.0	Introduced

Usage Information

This command does not uniquely identify a queue, but rather identifies only a set of queues. The WRED curve is applied to all eight egress Multicast queues.

Important Points to Remember—multicast-bandwidth option

- A unique Multicast WFQ setting can be applied only on a per port-pipe basis. The minumum percentage of the multicast bandwidth assigned to any of the ports in the port-pipe will take effect for the entire port-pipe.
- If the percentage of multicast bandwidth is 0, control traffic going through mutilcast queues are dropped.
- The no form of the command without **multicast-bandwidth** and **wred-profile**, will remove both the wred-profile and multicast-bandwidth configuration.
- On 10 Gigabit ports only, the multicast bandwidth option will work only if the total unicast bandwidth is more than the multicast bandwidth.
- If strict priority is applied along with multicast-bandwidth, the effect of strict priority is on all ports where unicast and multicast bandwidth are applied.
- When multicast bandwidth is assigned along with unicast bandwidth, first multicast bandwidth will be reserved for that port, then the remaining unicast bandwidth configured is adjusted according to the bandwidth available after reserving for multicast bandwidth.

Related Commands

show queue statistics egress	Display the egress queue statistics

queue ingress

C-Series	No
E-Series	✓

Assign a WRED Curve to all eight ingress Multicast queues or designate the percentage for the Multicast bandwidth queue..

Syntax

queue ingress multicast {**linecard** *slot number* **port-set** *number* | **all**} [**wred-profile** *name*]

To return to the default, use the **no queue ingress multicast** {**linecard** *slot number* **port-set** *number* | **all**} [**wred-profile** *name*] command.

Parameters

linecard *number*	Enter the keyword **linecard** followed by the line card slot number. E-Series Range: 0 to 13 on a E1200, 0 to 6 on a E600/E600i, and 0 to 5 on a E300.
port-set *number*	Enter the keyword **port-set** followed by the line card's port pipe. Range: 0 or 1
all	Enter the keyword **all** to apply to all line cards.
wred-profile *name*	(OPTIONAL) Enter the keyword **wred-profile** followed by your WRED profile name in character format (16 character maximum). Or use one of the pre-defined WRED profile names. Pre-defined Profiles: wred_drop, wred-ge_y, wred_ge_g, wred_teng_y, wred_teng_g

Defaults

No default behavior or values

Command Modes

CONFIGURATION

Command History

Version 7.4.1.0 and 6.5.3.0	Introduced

Usage Information

This command does not uniquely identify a queue, but rather identifies only a set of queues. The WRED Curve is applied to all eight ingress Multicast queues.

Note: The multicast-bandwidth option is not supported on queue ingress. If you attempt to use the multicast-bandwidth option, the following reject error message is generated:

```
% Error:Bandwidth-percent is not allowed for ingress multicast
```

Related Commands

show queue statistics ingress	Display the ingress queue statistics

rate-limit

C-Series	No
E-Series	✓

Specify the rate-limit functionality on outgoing traffic.

Syntax **rate-limit** *committed-rate* [*burst-KB*] [**peak** *peak-rate* [*burst-KB*]]

To remove the rate limiting functionality, use **no rate-limit** *committed-rate* [*burst-KB*] [**peak** *peak-rate* [*burst-KB*]] command.

Parameters

committed-rate	Enter the committed rate in Mbps. Range: 0 to 10000 Mbps
burst-KB	(OPTIONAL) Enter the burst size in KB. Range: 16 to 200000 KB Default: 50 KB
peak *peak-rate*	(OPTIONAL) Enter the keyword **peak** followed by the peak rate in Mbps. Range: 0 to 10000 Mbps Default: Same as designated for *committed-rate*

Defaults Burst size = 50 KB

Command Modes CONFIGURATION (conf-qos-policy-out)

Usage Information Traffic parameters are commit rate/burst and peak rate/burst.

rate-police

Specify the policing functionality on incoming traffic.

Syntax **rate-police** *committed-rate* [*burst-KB*] [**peak** *peak-rate* [*burst-KB*]]

To remove the rate policing functionality, use the **no rate-police** *committed-rate* [*burst-KB*] [**peak** *peak-rate* [*burst-KB*]] command.

Parameters

committed-rate	Enter the committed rate in Mbps. Range: 0 to 10000 Mbps

burst-KB	(OPTIONAL) Enter the burst size in KB. Range: 16 to 200000 KB Default: 50 KB
peak *peak-rate*	(OPTIONAL) Enter the keyword **peak** followed by the peak rate in Mbps. Range: 0 to 10000 Mbps Default: Same as designated for *committed-rate*

Defaults Burst size = 50 KB

Command Modes CONFIGURATION (conf-qos-policy-in)

Usage Information Traffic parameters are commit rate/burst and peak rate/burst.

rate-shape

C-Series	No
E-Series	✓

Shape the interface's traffic output.

Syntax **rate-shape** *rate* [*burst-KB*]

To delete the command, use the **no rate-shape** *rate* command.

Parameters

rate	Enter the outgoing rate in multiples of 10 Mbps. Range: 0 to 10000
burst-KB	(OPTIONAL) Enter a number as the burst size in KB. Range: 0 to 10000 Default: 10

Defaults No default behavior or values

Command Modes CONFIGURATION (conf-qos-policy-out)

Usage Information **rate-shape** can be applied only as an aggregate policy. If it is applied as class-based policy, then rate-shape will not take effect.

service-policy input

Apply input policy map to the interface.

Syntax **service-policy input** *policy-map-name* [**layer2**]

To remove the input policy map from the interface, use the **no service-policy input** *policy-map-name* [**layer2**] command.

Parameters

policy-map-name	Enter the name for the policy map in character format (16 characters maximum).
layer2	(**E-Series Only**—(OPTIONAL) Enter the keyword **layer2** to specify a Layer 2 Class Map. Default: Layer 3

Defaults Layer 3

Command Modes INTERFACE

Command History

Version 7.4.1.0	E-Series Only: Expanded to add support for Layer 2

Usage Information A single policy-map can be attached to one or more interfaces to specify the service-policy for those interfaces. A policy map attached to an interface can be modified.

Note: The **service-policy** commands are not allowed on a port channel. The **service-policy input** *policy-map-name* command and the **service-class dynamic dot1p** command are not allowed simultaneously on an interface. However, the **service-policy input** command (without the *policy-map-name* option) and the **service-class dynamic dot1p** command are allowed on an interface.

service-policy output

C-Series	No
E-Series	✓

Apply output policy map to the interface.

Syntax **service-policy output** *policy-map-name*

To remove the output policy map from the interface, use the **no service-policy output** *policy-map-name* command.

Parameters	*policy-map-name*	Enter the name for the policy map in character format (16 characters maximum).

Defaults No default behavior or values

Command Modes INTERFACE

Usage Information A single policy-map can be attached to one or more interfaces to specify the service-policy for those interfaces. A policy map attached to an interface can be modified.

service-queue

Assign class map and QoS policy to different queues.

Syntax **service-queue** *queue-id* [**class-map** *class-map-name*] [**qos-policy** *qos-policy-name*]

To remove the queue assignment, use the **no service-queue** *queue-id* [**class-map** *class-map-name*] [**qos-policy** *qos-policy-name*] command.

Parameters	*queue-id*	Enter the value used to identify a queue. There are eight (8) queues per interface. Range: 0 to 7
	class-map *class-map-name*	(OPTIONAL) Enter the keyword **class-map** followed by the class map name assigned to the queue in character format (16 character maximum). **Note**: This option is available under policy-map-input only.
	qos-policy *qos-policy-name*	(OPTIONAL) Enter the keyword **qos-policy** followed by the QoS policy name assigned to the queue in character format (16 character maximum). This specifies the input QoS policy assigned to the queue under policy-map-input and output QoS policy under policy-map-output context.

Defaults No default behavior or values

Command Modes CONFIGURATION (conf-policy-map-in and conf-policy-map-out)

Usage Information There are eight (8) queues per interface on the E-Series and four (4) queues per interface on the C-Series. This command assigns class-map or qos-policy to different queues.

set

This command marks the outgoing traffic withe differentiated service code point (DSCP) or dot1p values.

Syntax **set** {**ip-dscp** *value* | **mac-dot1p** *value* }

To remove a previously set value, use the **no set** {**ip-dscp** *value* | **mac-dot1p** *value* } command.

Parameters

ip-dscp *value*	(OPTIONAL) Enter the the keyword **ip-dscp** followed by the IP DSCP value. Range: 0 to 63
mac-dot1p *value*	**E-Series Only**—(OPTIONAL) Enter the the keyword **mac-dot1p** followed by the dot1p value. Range: 0 to 7

Defaults No default behavior or values

Command Modes CONFIGURATION (conf-qos-policy-in)

Command History

Version 7.4.1.0	E-Series Only: Expanded to add support for mac-dot1p

Usage Information

C-Series

Once the IP DSCP bit is set, other QoS services can then operate on the bit settings.

E-Series

Once the IP DSCP bit is set, other QoS services can then operate on the bit settings. WRED (Weighten Random Early Detection) ensures that high-precedence traffic has lower loss rates than other traffic during times of congestion.

show cam layer2-qos

C-Series	No
E-Series	✓

Display the Layer 2 QoS CAM entries.

Syntax **show cam layer2-qos** {[**linecard** *number* **port-set** *number*] | [**interface** *interface*]} [**summary**]

Parameters

linecard *number*	Enter the keyword **linecard** followed by the line card slot number. E-Series Range: 0 to 13 on a E1200, 0 to 6 on a E600/E600i, and 0 to 5 on a E300.
port-set *number*	Enter the keyword **port-set** followed by the line card's port pipe. Range: 0 or 1
interface *interface*	Enter the keyword **interface** followed by one of the keywords below and slot/port or number information: • For a Fast Ethernet interface, enter the keyword **FastEthernet** followed by the slot/port information. • For a Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For a SONET interface, enter the keyword **sonet** followed by the slot/port information. • For a Ten Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information.
summary	(OPTIONAL) Enter the keyword **summary** to display only the total number of CAM entries.

Defaults No default behavior or values

Command Modes EXEC

Command History

Version 7.4.1.0	Introduced

Example

```
Force10#show cam layer2-qos interface gigabitethernet 2/0

Cam   Port Dot1p Proto       SrcMac            SrcMask           DstMac            DstMask            Dot1p      DSCP     Queue
Index                                                                                                   Marking    Marking
-------------------------------------------------------------------------------------------------------------------------------
-------
01817 0    -     0           00:00:00:00:cc:cc 00:00:00:00:ff:ff 00:00:00:00:dd:dd 00:00:00:00:ff:ff  -          -        7
01818 0    -     0           00:00:00:00:00:c0 00:00:00:00:00:f0 00:00:00:00:00:d0 00:00:00:00:00:f0  -          45       5
01819 0    4     0           00:00:00:a0:00:00 00:00:00:ff:00:00 00:00:00:b0:00:00 00:00:00:ff:00:00  4          -        4
01820 0    -     0x2000      00:00:00:00:00:00 00:00:00:00:00:00 00:00:00:00:00:b0 ff:ff:ff:ff:ff:ff  -          -        1
02047 0    -     0           00:00:00:00:00:00 00:00:00:00:00:00 00:00:00:00:00:00 00:00:00:00:00:00  -          -        0
Force10#
```

Figure 371 show cam layer2-qos interface

Example

```
Force10#show cam layer2-qos linecard 2 port-set 0
Cam   Port Dot1p Proto       SrcMac            SrcMask           DstMac            DstMask            Dot1p      DSCP     Queue
Index                                                                                                   Marking    Marking
-------------------------------------------------------------------------------------------------------------------------------=--
01817 0    -     0           00:00:00:00:cc:cc 00:00:00:00:ff:ff 00:00:00:00:dd:dd 00:00:00:00:ff:ff  -          -        7
01818 0    -     0           00:00:00:00:00:c0 00:00:00:00:00:f0 00:00:00:00:00:d0 00:00:00:00:00:f0  -          45       5
01819 0    4     0           00:00:00:a0:00:00 00:00:00:ff:00:00 00:00:00:b0:00:00 00:00:00:ff:00:00  4          -        4
01820 0    -     0x2000      00:00:00:00:00:00 00:00:00:00:00:00 00:00:00:00:00:b0 ff:ff:ff:ff:ff:ff  -          -        1
02047 0    -     0           00:00:00:00:00:00 00:00:00:00:00:00 00:00:00:00:00:00 00:00:00:00:00:00  -          -        0
Force10#
```

Figure 372 show cam layer2-qos linecard

show cam layer3-qos

C-Series	No
E-Series	✓

Display the Layer 3 QoS CAM entries.

Syntax **show cam layer3-qos** {[**linecard** *number* **port-set** *number*] | [**interface** *interface*]} [**summary**]

Parameters

linecard *number*	Enter the keyword **linecard** followed by the line card slot number. E-Series Range: 0 to 13 on a E1200, 0 to 6 on a E600/E600i, and 0 to 5 on a E300.
port-set *number*	Enter the keyword **port-set** followed by the line card's port pipe. Range: 0 or 1
interface *interface*	Enter the keyword **interface** followed by one of the keywords below and slot/port or number information: • For a Fast Ethernet interface, enter the keyword **FastEthernet** followed by the slot/port information. • For a Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For a SONET interface, enter the keyword **sonet** followed by the slot/port information. • For a Ten Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information.
summary	(OPTIONAL) Enter the keyword **summary** to display only the total number of CAM entries.

Defaults No default behavior or values

Command Modes EXEC

Command History

Version 6.5.1.0	Introduced

Example

```
Force10#sh cam layer3-qos interface gigabitethernet 2/1

Cam   Port Dscp Proto Tcp   Src   Dst   SrcIp              DstIp              DSCP    Queue
Index                 Flag  Port  Port                                        Marking
-------------------------------------------------------------------------------------------
----
23488 1     0   0     0x0   0     0     0.0.0.0/0          0.0.0.0/0          -       TRUST-DSCP
Force10#
```

Figure 373 show cam layer3-qos linecard interface Command

In Figure 373, Figure 374, Figure 375 outputs, note that:

- The entry TRUST-DSCP in the Queue column (Figure 373) indicates that the trust diffserv is configured on the policy-map. Figure 375 is an example of the trust diffserv not configured on the plicy-map.
- A hypen (-) entry in the DSCP Marking column indicates that there is no DSCP marking.
- In the Proto column (Protocol), IP, ICMP, UDP, and TCP strings are displayed. For other protocols, the corresponding protocol number is displayed.

Example

```
Force10#show cam layer3-qos linecard 13 port-set 0

Cam    Port    Dscp Proto Tcp  Src   Dst   SrcIp        DstIp        DSCP     Queue
Index                     Flag Port  Port                            Marking
-------------------------------------------------------------------------------
24511  1       0    TCP   0x5  2     5     1.0.0.1/24   2.0.0.2/24   -        TRUST-DSCP
24512  1       0    UDP   0x2  2     5     8.0.0.8/24   8.0.0.8/24   23       3

Force10#
```

Figure 374 show cam layer3-qos linecard port-set Command

Example

```
Force10#sh cam layer3-qos interface gigabitethernet 2/1

Cam   Port Dscp Proto Tcp   Src   Dst   SrcIp             DstIp             DSCP    Queue
Index                Flag  Port  Port                                      Marking
-------------------------------------------------------------------------------------
---
23488 1    56   0     0x0   0     0     0.0.0.0/0         0.0.0.0/0         -       7
23489 1    48   0     0x0   0     0     0.0.0.0/0         0.0.0.0/0         -       6
23490 1    40   0     0x0   0     0     0.0.0.0/0         0.0.0.0/0         -       5
23491 1     0   IP    0x0   0     0     10.1.1.1/32       20.1.1.1/32       -       0
23492 1     0   IP    0x0   0     0     10.1.1.1/32       20.1.1.2/32       -       0
24511 1     0   0     0x0   0     0     0.0.0.0/0         0.0.0.0/0         -       0
Force10#
```

Figure 375 show cam layer3-qos linecard interface Command without Trust

Example

```
Force10#show cam layer3-qos linecard 13 port-set 0 summary

Total number of CAM entries for Port-Set 0 is 100
Force10#
```

Figure 376 show cam layer3-qos summary Command

show qos class-map

View the current class map information.

Syntax **show qos class-map** [*class-name*]

Parameters		
	class-name	(Optional) Enter the name of a configured class map.

Defaults No default behavior or values

Command Modes EXEC

EXEC privilege

Example

```
Force10#show qos class-map

Class-map match-any CM
  Match ip access-group ACL
```

Figure 377 show qos class-map Command

Related Commands		
	class-map	Identify the class map

show qos policy-map

View the QoS policy map information.

Syntax **show qos policy-map** {**summary** [*interface*] | **detail** [*interface*]}

Parameters

summary *interface*	To view a policy map interface summary, enter the keyword **summary** and optionally one of the following keywords and slot/port or number information: • For a Fast Ethernet interface, enter the keyword **FastEthernet** followed by the slot/port information. • For a Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For a SONET interface, enter the keyword **sonet** followed by the slot/port information. • For a Ten Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information.
detail *interface*	To view a policy map interface in detail, enter the keyword **detail** and optionally one of the following keywords and slot/port or number information: • For a Fast Ethernet interface, enter the keyword **FastEthernet** followed by the slot/port information. • For a Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For a SONET interface, enter the keyword **sonet** followed by the slot/port information. • For a Ten Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information.

Defaults

No default behavior or values

Command Modes

EXEC

EXEC privilege

Command History

Version 7.4.1.0	E-Series Only: Added Trust IPv6 diffserv

Example 1

```
Force10#show qos policy-map detail gigabitethernet 0/0

Interface GigabitEthernet 4/1

Policy-map-input policy
Trust diffserv
Queue#   Class-map-name          Qos-policy-name
  0           -                  q0
  1          CM1                 q1
  2          CM2                 q2
  3          CM3                 q3
  4          CM4                 q4
  5          CM5                 q5
  6          CM6                 q6
  7          CM7                 q7
Force10#
```

Figure 378 show qos policy-map detail (IPv4) Command

Example 2

```
Force10# show qos policy-map detail gigabitethernet 0/0

Interface GigabitEthernet 8/29

Policy-map-input pmap1
Trust ipv6-diffserv
Queue#   Class-map-name          Qos-policy-name
  0           c0                                q0
  1           c1                                q1
  2           c2                                q2
  3           c3                                q3
  4           c4                                q4
  5           c5                                 -
  6           c6                                q6
  7           c7                                q7
Force10#
```

Figure 379 show qos policy-map detail (IPv6) Command

Example 3

```
Force10#sho qos policy-map summary

Interface        policy-map-input        policy-map-output
Gi 4/1             PM1                      -
Gi 4/2             PM2                    PMOut
Force10#
```

Figure 380 show qos policy-map summary (IPv4) Command

show qos policy-map-input

View the input QoS policy map details.

Syntax **show qos policy-map-input** [*policy-map-name*] [**class** *class-map-name*] [**qos-policy-input** *qos-policy-name*]

Parameters

policy-map-name	Enter the policy map name.
class *class-map-name*	Enter the keyword class followed by the class map name.
qos-policy-input *qos-policy-name*	Enter the keyword **qos-policy-input** followed by the QoS policy name.

Defaults No default behavior or values

Command Modes EXEC

EXEC privilege

Command History

Version 7.4.1.0	E-Series Only: Added Trust IPv6 diffserv

Example 1

```
Force10#show qos policy-map-input

Policy-map-input PolicyMapInput
Aggregate Qos-policy-name AggPolicyIn
Queue#   Class-map-name          Qos-policy-name
  0      ClassMap1               qosPolicyInput
Force10#
```

Figure 381 show qos policy-map-input (IPv4) Command

Example 2

```
Force10# show qos policy-map-input

Policy-map-input pmap1
Trust ipv6-diffserv
Queue#   Class-map-name          Qos-policy-name
  0           c0                                q0
  1           c1                                q1
  2           c2                                q2
  3           c3                                q3
  4           c4                                q4
  5           c5                                 -
  6           c6                                q6
  7           c7                                q7
Force10#
```

Figure 382 show qos policy-map-input (IPv6) Command

show qos policy-map-output

C-Series	No
E-Series	✓

View the output QoS policy map details.

Syntax **show qos policy-map-output** [*policy-map-name*] [**qos-policy-output** *qos-policy-name*]

Parameters

policy-map-name	Enter the policy map name.
qos-policy-output *qos-policy-name*	Enter the keyword **qos-policy-output** followed by the QoS policy name.

Defaults No default behavior or values

Command Modes EXEC

EXEC privilege

Example

```
Force10#show qos policy-map-output

Policy-map-output PolicyMapOutput
Aggregate Qos-policy-name AggPolicyOut
Queue#            Qos-policy-name
  0               qosPolicyOutput
Force10#
```

Figure 383 show qos policy-map-output

show qos qos-policy-input

View the input QoS policy details.

Syntax **show qos qos-policy-input** [*qos-policy-name*]

Parameters

qos-policy-name	Enter the QoS policy name.

Defaults No default behavior or values.

Command Modes EXEC

EXEC privilege

Example

```
Force10#show qos qos-policy-input

Qos-policy-input QosInput
        Rate-police 100 50 peak 100 50
        Dscp 32
Force10#
```

Figure 384 show qos qos-policy-input Command

show qos qos-policy-output

C-Series	**No**
E-Series	✓

View the output QoS policy details.

Syntax **show qos qos-policy-output** [*qos-policy-name*]

Parameters		
	qos-policy-name	Enter the QoS policy name.

Defaults No default behavior or values

Command Modes EXEC

EXEC privilege

Example

```
Force10#show qos qos-policy-output

Qos-policy-output qosOut
        Rate-limit 50 50 peak 50 50
        Wred yellow 1
        Wred green 1
```

Figure 385 show qos qos-policy-output Command

show qos statistics

View QoS statistics.

Syntax **show qos statistics** {**wred-profile** [*interface*]} | [*interface*]

Parameters		
	wred-profile *interface*	**Platform—E-Series Only**: Enter the keyword **wred-profile** and optionally one of the following keywords and slot/port or number information: • For a Fast Ethernet interface, enter the keyword **FastEthernet** followed by the slot/port information. • For a Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For a SONET interface, enter the keyword **sonet** followed by the slot/port information. • For a Ten Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information.
	interface	Enter one of the following keywords and slot/port or number information: • For a Fast Ethernet interface, enter the keyword **FastEthernet** followed by the slot/port information. • For a Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For a SONET interface, enter the keyword **sonet** followed by the slot/port information. • For a Ten Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information.

Defaults No default behavior or values

Command Modes

EXEC

EXEC privilege

Usage Information

E-Series

The show qos statistics output differs from the ED and EE series line cards and the EF series line cards. The qos statistics for the EF series generates two extra columns, Queued Pkts and Dropped Pkts, see Example 2.

Note: The **show qos statistics** command displays Matched Packets and Matched Bytes. The show queue statistics egress command displays Queued Packets and Queued Bytes. The following example explains how these two displays relate to each other.

- 9000 byte size packets are sent from Interface A to Interface B.
- The Matched Packets on Interface A are equal to the Queued Packets on Interface B.
- Matched bytes on Interface A = matched packets *9000
- Queued bytes on Interface B = queued packets *(9020)—Each packet has an additional header of 20 bytes.

Example 1

```
Force10#show qos statistics

Interface Gi 0/0
Queue#   Queued Bytes            Matched Pkts            Matched Bytes
  0       0                       0                       0
  1       0                       0                       0
  2       0                       0                       0
  3       0                       0                       0
  4       0                       0                       0
  5       0                       0                       0
  6       0                       0                       0
  7       0                       0                       0

Interface Gi 0/1
Queue#   Queued Bytes            Matched Pkts            Matched Bytes
  0       0                       0                       0
  1       0                       0                       0
  2       0                       0                       0
  3       0                       0                       0
  4       0                       0                       0
  5       0                       0                       0
  6       0                       0                       0
  7       0                       0                       0
```

Figure 386 show qos statistics Command (ED and EE Series)

Table 112 show qos statistics Command Example Fields (ED and EE Series)

Field	Description
Queue #	Queue Number
Queued Bytes	Snapshot of the byte count in that queuet.

Table 112 show qos statistics Command Example Fields (ED and EE Series) (continued)

Field	Description
Matched Pkts	The number of packets that matched the class-map criteria. **Note:** When trust is configured, matched packet counters are not incremented in this field.
Matched Bytes	The number of bytes that matched the class-map criteria. **Note:** When trust is configured, matched byte counters are not incremented in this field.

Example 2

```
Force10#show qos statistics gig 0/1

Queue#  Queued           Queued          Matched         Matched         Dropped
        Bytes            Pkts            Pkts            Bytes           Pkts
        (Cumulative)     (Cumulative)
  0      0                0               1883725         1883725000      0
  1      0                0               1883725         1883725000      0
  2      0                0               1883725         1883725000      0
  3      0                0               1883725         1883725000      0
  4      0                0               1883725         1883725000      0
  5      0                0               1883724         1883724000      0
  6      0                0               1883720         1883720000      0
  7      0                0               1883720         1883720000      0

Force10#
```

Figure 387 show qos statistics Command (EFSeries)

Table 113 show qos statistics Command Example Fields (EF Series)

Field	Description
Queue #	Queue Number
Queued Bytes	Cumulative byte count in that queue
Queued Pkts	Cumulative packet count in that queue.
Matched Pkts	The number of packets that matched the class-map criteria. **Note:** When trust is configured, matched packet counters are not incremented in this field.
Matched Bytes	The number of bytes that matched the class-map criteria. **Note:** When trust is configured, matched byte counters are not incremented in this field.
Dropped Pkts	The total of the number of packets dropped for green, yellow and out-of-profile.

Example 3

```
Force10#show qos statistics wred-profile
Interface Gi 5/11
Queue#  Drop-statistic  WRED-name        Dropped Pkts

  0     Green           WRED1            51623
        Yellow          WRED2            51300
        Out of Profile                   0
  1     Green           WRED1            52082
        Yellow          WRED2            51004
        Out of Profile                   0
  2     Green           WRED1            50567
        Yellow          WRED2            49965
        Out of Profile                   0
  3     Green           WRED1            50477
        Yellow          WRED2            49815
        Out of Profile                   0
  4     Green           WRED1            50695
        Yellow          WRED2            49476
        Out of Profile                   0
  5     Green           WRED1            50245
        Yellow          WRED2            49535
        Out of Profile                   0
  6     Green           WRED1            50033
        Yellow          WRED2            49595
        Out of Profile                   0
  7     Green           WRED1            50474
        Yellow          WRED2            49522
        Out of Profile                   0
Force10#
```

Figure 388 show qos statistics wred-profile Command (ED, EE, and EF Series)

Table 114 show qos statistics wred-profile Command Example Fields (ED, EE, and EF Series)

Field	Description
Queue #	Queue Number
Drop-statistic	Drop statistics for green, yellow and out-of-profile packets
WRED-name	WRED profile name
Dropped Pkts	The number of packets dropped for green, yellow and out-of-profile

Related Commands

clear qos statistics	Clears counters as shown in show qos statistics

show qos wred-profile

C-Series	No
E-Series	✓

View the WRED profile details.

Syntax **show qos wred-profile** *wred-profile-name*

Parameters		
	wred-profile-name	Enter the WRED profile name to view the profile details.

Defaults No default behavior or values

Command Modes EXEC

EXEC privilege

Example

```
Force10#show qos wred-profile

Wred-profile-name       min-threshold   max-threshold
wred_drop               0               0
wred_ge_y               1024            2048
wred_ge_g               2048            4096
wred_teng_y             4096            8192
wred_teng_g             8192            16384
WRED1                   2000            7000
```

Figure 389 show qos wred-profile Command

test cam-usage

C-Series	**No**
E-Series	✓

Check the Input Policy Map configuration for the CAM usage.

Syntax **test cam-usage service-policy input** *policy-map* **linecard** { [*number* **port-set** *portpipe number*] | [**all**] }

Parameters		
	policy-map	Enter the policy map name.
	linecard *number*	(OPTIONAL) Enter the keyword **linecard** followed by the line card slot number. E-Series Range: 0 to 13 on a E1200, 0 to 6 on a E600/E600i, and 0 to 5 on a E300.
	port-set *portpipe number*	Enter the keyword **port-set** followed by the line card's port pipe number. Range: 0 or 1
	linecard all	(OPTIONAL) Enter the keyword **linecard all** to indicate all line cards.

Defaults No default values or behavior

Command Modes EXEC

Command History

Version 7.4.1.0	Introduced

Example

```
Force10# test cam-usage service-policy input pmap_l2 linecard all

For a L2 Input Policy Map pmap_l2, the output must be as follows,

Linecard  |  Portpipe | CAM Partition  | Available CAM  | Estimated CAM  | Status
          |           |                |                | per Port       | (Allowed ports)

   0           0          L2ACL              500          200              Allowed (2)
   0           1          L2ACL              100          200               Exception
   1           0          L2ACL             1000          200              Allowed (5)
   1           1          L2ACL              0            200               Exception
                          …
                          …
                          …
   13          1          L2ACL              400          200              Allowed (2)
Force10#
```

Figure 390 test cam-usage service-policy input policy-map linecard all Example Command

Note: In a Layer 2 Policy Map, IPv4/IPv6 rules are not allowed and hence the output contains only L2ACL CAM partition entries.

Table 115 defines the fields in Figure 390.

Table 115 test cam-usage Command Example Fields

Field	Description
Linecard	Indicates the line card slot number.
Portpipe	Indicates the portpipe number.
CAM Partition	The CAM space where the rules are added.
Available CAM	Indicates the free CAM space, in the partition, for the classification rules. **Note:** The CAM entries reserved for the default rules are not included in the Available CAM column; free entries, from the default rules space, can not be used as a policy map for the classification rules.
Estimated CAM per Port	Indicates the number of free CAM entries required (for the classification rules) to apply the input policy map on a single interface. **Note:** The CAM entries for the default rule are not included in this column; a CAM entry for the default rule is always dedicated to a port and is always available for that interface.
Status (Allowed ports)	Indicates if the input policy map configuration on an interface belonging to a linecard/port-pipe is successful—Allowed (*n*)—or not successful—Exception. The allowed number (*n*) indicates the number of ports in that port-pipe on which the Policy Map can be applied successfully.

Usage Information

This features allows you to determine if the CAM has enough space available before applying the configuration on an interface.

An input policy map with both Trust and Class-map configuration, the Class-map rules are ignored and only the Trust rule is programmed in the CAM. In such an instance, the Estimated CAM output column will contain the size of the CAM space required for the Trust rule and *not* the Class-map rule.

threshold

C-Series	No
E-Series	✔

Specify the minimum and maximum threshold values for the configured WRED profiles.

Syntax

threshold min *number* **max** *number*

To remove the threshold values, use the **no threshold min** *number* **max** *number* command.

Parameters

min *number*	Enter the keyword **min** followed by the minimum threshold number for the WRED profile. Range: 1024 to 77824 KB
max *number*	Enter the keyword **max** followed by the maximum threshold number for the WRED profile. Range: 1024 to 77824 KB

Defaults

No default behavior or values

Command Modes

CONFIGURATION (config-wred)

Usage Information

Use this command to configure minimum and maximum threshold values for user defined profiles. Additionally, use this command to modify the minimum and maximum threshold values for the pre-defined WRED profiles. If you delete threshold values of the pre-defined WRED profiles, the profiles will revert to their original default values (Table 116).

Table 116 Pre-defined WRED Profile Threshold Values

Pre-defined WRED Profile Name	Minimum Threshold	Maximum Threshold
wred_drop	0	0
wred_ge_y	1024	2048
wred_ge_g	2048	4096
wred_teng_y	4096	8192
wred_teng_g	8192	16384

Related Commands		
	wred-profile	Create a WRED profile.

trust

Specify dynamic classification (DSCP) or dot1p to trust.

Syntax **trust** {**diffserv** | **dot1p** | **ipv6-diffserv**}

To remove the definition, use the **no trust** {**diffserv** | **dot1p** | **ipv6-diffserv**} command.

Parameters

diffserv	(OPTIONAL) Enter the keyword **diffserv** to specify trust configuration of DSCP.
dot1p	(OPTIONAL) Enter the keyword **dot1p** to specify trust dot1p configuration.
ipv6-diffserv	(OPTIONAL) Enter the keyword **ipv6-diffserv** to specify trust configuration of IPv6 DSCP.

Defaults No default behavior or values

Command Modes CONFIGURATION (conf-policy-map-in)

Command History

Version 7.4.1.0	Expanded to add support for dot1p and IPv6 DSCP

Usage Information

E-Series

When trust is configured, matched bytes/packets counters are not incremented in the show qos statistics command.

Dynamic mapping honors packets marked according to the standard definitions of DSCP. The default mapping table is detailed in Table 117.

Table 117 Standard Default DSCP Mapping Table

DSCP/CP	DSCP Definition	Traditional IP Precedence	Internal Queue ID
111XXX		Network Control	7
110XXX		Internetwork Control	6
101XXX	EF (Expedited forwarding) 101110	CRITIC/ECP	5
100XXX	AF4 (Assured Forwarding)	Flash Override	4
011XXX	AF3	Flash	3
010XXX	AF2	Immediate	2
001XXX	AF1	Priority	1
000XXX	BE: Best Effort	BE: Best Effort	0

wred

C-Series	**No**
E-Series	✔

Designate the WRED profile to yellow or green traffic.

Syntax **wred** {**yellow** | **green**} *profile-name*

To remove the WRED drop precedence, use the **no wred** {**yellow** | **green**} [*profile-name]* command.

Parameters

yellow | **green**	Enter the keyword **yellow** for yellow traffic. DSCP value of xxx110 and xxx100 maps to yellow. Enter the keyword **green** for green traffic. DSCP value of xxx010 maps to green.
profile-name	Enter your WRED profile name in character format (16 character maximum). Or use one of the 5 pre-defined WRED profile names. Pre-defined Profiles: wred_drop, wred-ge_y, wred_ge_g, wred_teng_y, wred_teng_

Defaults No default behavior or values

Command Modes CONFIGURATION (conf-qos-policy-out)

Usage Information Use this command to assign drop precedence to green or yellow traffic. If there is no honoring enabled on the input, all the traffic defaults to green drop precedence.

Related Commands		
	wred-profile	Create a WRED profile and name that profile
	trust	Define the dynamic classification to trust DSCP

wred-profile

C-Series	No
E-Series	✓

Create a WRED profile and name that profile.

Syntax **wred-profile** *wred-profile-name*

To remove an existing WRED profile, use the **no wred-profile** command.

Parameters		
	wred-profile-name	Enter your WRED profile name in character format (16 character maximum). Or use one of the pre-defined WRED profile names. You can configure up to 26 WRED profiles plus the 5 pre-defined profiles, for a total of 31 WRED profiles. Pre-defined Profiles: wred_drop, wred-ge_y, wred_ge_g, wred_teng_y, wred_teng_g

Defaults The five pre-defined WRED profiles. When a new profile is configured, the minimum and maximum threshold defaults to predefined wred_ge_g values

Command Modes CONFIGURATION

Usage Information Use the default pre-defined profiles or configure your own profile. You can not delete the pre-defined profiles or their default values. This command enables the WRED configuration mode—(conf-wred).

Related Commands		
	threshold	Specify the minimum and maximum threshold values of the WRED profile

Queue Level Debugging

Platform Specific Feature: Queue Level Debugging is an E-Series only feature.

The following queuing statistics are available in EtherScale and TeraScale systems.

- clear queue statistics egress on page 1264
- clear queue statistics ingress on page 1265
- show queue statistics egress on page 1266
- show queue statistics ingress on page 1270

clear queue statistics egress

C-Series	No
E-Series	✓

Clear egress queue statistics.

Syntax **clear queue statistics egress** [**unicast** | **multicast**] [*Interface*]

Parameters

unicast | multicast	(OPTIONAL) Enter the keyword **multicast** to clear only Multicast queue statistics. Enter the keyword **unicast** to clear only Unicast queue statistics. Default: Both Unicast and Multicast queue statistics are cleared.
Interface	(OPTIONAL) Enter one of the following interfaces to display the interface specific queue statistics. • For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information. • For a SONET interface, enter the keyword **sonet** followed by the slot/port information. • Fast Ethernet is not supported

Defaults No default behavior or values

Command Modes EXEC

EXEC privilege

Command History

Version 6.2.1.1	Introduced

Usage Information

If a Policy QoS is applied on an interface when **clear queue statistics egress** is issued, it will clear the egress counters in show queue statistics and vice-versa. This behavior is due to the values being read from the same hardware registers.

Related Commands

clear queue statistics ingress	Clear ingress queue statistics
show queue statistics egress	Display egress queue statistics
show queue statistics ingress	Display ingress queue statistics

clear queue statistics ingress

C-Series	**No**
E-Series	✓

Clear ingress queue statistics.

Syntax **clear queue statistics ingress** [**unicast** [**src-card** *ID* [**dst-card** *ID*]] | [**multicast**] [**src-card** *ID*]]

Parameters

unicast [**src-card** *ID* [**dst-card** *ID*]]	(OPTIONAL) Enter the keyword **unicast** to clear Unicast queue statistics. Optionally, enter the source card identification (**src-card** *ID*) and the destination card identification (**dst-card** *ID*) to clear the unicast statistics from the source card to the destination card.
multicast [**src-card** *ID*]	(OPTIONAL) Enter the keyword **multicast** to clear only Multicast queue statistics. Optionally, enter the source card identification (**src-card** *ID*) to clear the multicast statistics from the source card. Default: Both Unicast and Multicast queue statistics are cleared.

Defaults No default behavior or values

Command Modes EXEC

EXEC privilege

Command History

Version 6.2.1.1	Introduced

Related Commands

clear queue statistics egress	Clear egress queue statistics
show queue statistics egress	Display egress queue statistics
show queue statistics ingress	Display ingress queue statistics

show queue statistics egress

C-Series	No
E-Series	✓

Display the egress queue statistics.

Syntax

show queue statistics egress [**unicast** | **multicast**] [*Interface*] [**brief**]

Parameters

unicast | multicast	(OPTIONAL) Enter the keyword **multicast** to display only Multicast queue statistics. Enter the keyword **unicast** to display only Unicast queue statistics. Default: Both Unicast and Multicast queue statistics are displayed.
Interface	(OPTIONAL) Enter one of the following interfaces to display the interface specific queue statistics. • For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information. • For a SONET interface, enter the keyword **sonet** followed by the slot/port information. • Fast Ethernet is not supported.
brief	(OPTIONAL) Enter the keyword **brief** to display only ingress per link buffering and egress per port buffering statistics.

Defaults

No default behavior or values

Command Modes

EXEC

EXEC privilege

Command History

Version 6.2.1.1	Introduced

Usage Information

EtherScale systems display cumulative dropped packets, while TeraScale systems display cumulative queued bytes (in KB), cumulative queued packets (in KB), and cumulative dropped packets (in KB).

The display area is limited to 80 spaces to accommodate the screen and for optimal readability. Numbers, that is values, are limited to 12 characters. The numbering conventions are detailed in Table 118.

Table 118 Numbering Conventions for show queue egress statistics Output

Value	Divide the number by	Quotient Display	Examples
(10^11) - (10^14)	1024	K	12345678901**K**
(10^14) - (10^17)	1024*1024	M	12345678901**M**
> (10^17)	1024*1024*1024	T	12345678901**T**

Note: The **show queue statistics** command displays Queued Packets and Queued Bytes. The show qos statistics command displays Matched Packets and Matched Bytes. The following example explains how these two outputs relate to each other.

- 9000 byte size packets are sent from Interface A to Interface B.
- The Matched Packets on Interface A are equal to the Queued Packets on Interface B.
- Matched bytes on Interface A = matched packets *9000
- Queued bytes on Interface B = queued packets *(9020)—Each packet has an additional header of 20 bytes.

Example 1

```
Force10#show queue statistics egress unicast gigabitethernet 9/1

Interface Gi 9/1

Egress Queued       Queued       Packet Type    Min      Max      Dropped
Port   bytes        packets                     KB       KB       packets
Queue#
0      281513847K   31959000     Green          2048     4096     0
                                 Yellow         1024     2048     0
                                 Out of Profile                   30385770
1      99281660K    11271000     Green          2048     4096     0
                                 Yellow         1024     2048     0
                                 Out of Profile                   9886100
2      99281660K    11271000     Green          2048     4096     0
                                 Yellow         1024     2048     0
                                 Out of Profile                   9784600
3      38984440000  4322000      Green          2048     4096     0
                                 Yellow         1024     2048     0
                                 Out of Profile                   3053753
4      99281660K    11271000     Green          2048     4096     0
                                 Yellow         1024     2048     0
                                 Out of Profile                   9581600
5      39760160000  4408000      Green          2048     4096     0
                                 Yellow         1024     2048     0
                                 Out of Profile                   3070671
6      39642900000  4395000      Green          2048     4096     0
                                 Yellow         1024     2048     0
                                 Out of Profile                   3026100
7      99274410K    11270177     Green          2048     4096     0
                                 Yellow         1024     2048     0
                                 Out of Profile                   9273402
Force10#
```

Figure 391 show queue statistics egress Command (TeraScale)

Table 119 defines the columns displayed in Figure 391.

Table 119 show queue statistics egress Command Fields

Field	Description
Egress Port Queue#	Egress Port Queue Number
Queued bytes	Cumulative byte count in that queue

Table 119 show queue statistics egress Command Fields

Field	Description
Queued packets	Cumulative packet count in that queue.
Packet type	Green, yellow, and out-of-profile packets
Min KB	Minimum threshold for WRED queue
Max KB	Maximum threshold for WRED queue
Dropped Pkts	The number of packets dropped for green, yellow and out-of-profile

Example 2

```
Force10#sho queue statistics egress multicast

Linecard 3 port pipe 0, multicast

Packet Type         Min       Max       Dropped
                    KB        KB        packets
Green               8192      16384     0
Yellow              4096      8192      0
Out of Profile                          0

Linecard 3 port pipe 1, multicast

Packet Type         Min       Max       Dropped
                    KB        KB        packets
Green               8192      16384     0
Yellow              4096      8192      0
Out of Profile                          0

Linecard 7 port pipe 0, multicast

Packet Type         Min       Max       Dropped
                    KB        KB        packets
Green               2048      4096      0
Yellow              1024      2048      0
Out of Profile                          0

Linecard 7 port pipe 1, multicast

Packet Type         Min       Max       Dropped
                    KB        KB        packets
Green               2048      4096      0
Yellow              1024      2048      0
Out of Profile                          0
Force10#
```

Figure 392 show queue statistics egress multicast Command (EtherScale)

Table 120 defines the columns displayed in Figure 392.

Table 120 show queue statistics egress multicast Command Fields

Field	Description
Packet type	Green, yellow, and out-of-profile packets
Min KB	Minimum threshold for WRED queue
Max KB	Maximum threshold for WRED queue
Dropped Pkts	The number of packets dropped for green, yellow and out-of-profile

Example 3

```
Force10#show queue statistics egress brief

LC      Portpipe        Port       Dropped
        PortPipe                   packets
0       0               0          0
0       0               1          0
0       0               2          0
0       0               3          0
0       0               4          0
0       0               5          0
0       0               6          0
0       0               7          0
0       0               8          0
0       0               9          0
0       0               10         0
0       0               11         0
0       0               M          0
0       1               0          0
0       1               1          0
0       1               2          0
0       1               3          0
0       1               4          0
0       1               5          0
0       1               6          0
0       1               7          0
0       1               8          0
0       1               9          0
0       1               10         0
0       1               11         0
0       1               M          0
1       0               0          0
Force10#
```

Figure 393 show queue statistics egress brief Command

Table 121 defines the columns displayed in Figure 393.

Table 121 show queue statistics egress brief Command Fields

Field	Description
LC	Line Card
Portpipe	Portpipe number
Port	Port Queue. Where **M** is Multicast queue
Dropped Pkts	The number of packets dropped for green, yellow and out-of-profile

Related Commands

clear queue statistics egress	Clear egress queue statistics.
clear queue statistics ingress	Clear ingress queue statistics.
show queue statistics ingress	Display ingress queue statistics

show queue statistics ingress

C-Series	No
E-Series	✓

Display the ingress queue statistics.

Syntax

show queue statistics ingress [**unicast** [**src-card** *ID* [**dst-card** *ID*]] | [**multicast**] [**src-card** *ID*]] [**brief**]

Parameters

unicast [**src-card** *ID* [**dst-card** *ID*]]	(OPTIONAL) Enter the keyword **unicast** to display Unicast queue statistics. Optionally, enter the source card identification (**src-card** *ID*) and the destination card identification (**dst-card** *ID*) to display the unicast statistics from the source card to the destination card. Destination card Identification: Range 0 to 13 or RPM
multicast [**src-card** *ID*]	(OPTIONAL) Enter the keyword **multicast** to display only Multicast queue statistics. Optionally, enter the source card identification (**src-card** *ID*) to display the multicast statistics from the source card. Default: Both Unicast and Multicast queue statistics are displayed.
brief	(OPTIONAL) Enter the keyword **brief** to display only ingress per link buffering and egress per port buffering statistics.

Defaults

No default behavior or values

Command Modes

EXEC

EXEC privilege

Command History

Version 6.2.1.1	Introduced

Usage Information

EtherScale systems display cumulative dropped packets, while TeraScale systems display cumulative queued bytes (in KB), cumulative queued packets (in KB), and cumulative dropped packets (in KB).

The display area is limited to 80 spaces to accommodate the screen and for optimal readability. Numbers, that is values, are limited to 12 characters. The conventions are detailed in Table 122.

Table 122 Numbering Conventions for show queue statistics ingress Output

Value	Divide the number by	Quotient Display	Examples
(10^11) - (10^14)	1024	K	12345678901**K**
(10^14) - (10^17)	1024*1024	M	12345678901**M**
> (10^17)	1024*1024*1024	T	12345678901**T**

Note: The **show queue statistics** command displays Queued Packets and Queued Bytes. The show qos statistics command displays Matched Packets and Matched Bytes. The following example explains how these two displays relate to each other.

- 9000 byte size packets are sent from Interface A to Interface B.
- The Matched Packets on Interface A are equal to the Queued Packets on Interface B.
- Matched bytes on Interface A = matched packets *9000
- Queued bytes on Interface B = queued packets *(9020)—Each packet has an additional header of 20 bytes.

```
Force10#show queue statistics ingress unicast src-card 7 dst-card 3

Linecard 7 port pipe 0, to linecard 3 port pipe 0, unicast

SF          Packet Type         Min       Max       Dropped
Ingress                         KB        KB        packets
Queue#
0           Green               4096      4096      0
            Yellow              3276      3276      0
            Out of Profile                          0
1           Green               4096      4096      0
            Yellow              3276      3276      0
            Out of Profile                          0
2           Green               4096      4096      0
            Yellow              3276      3276      0
            Out of Profile                          0
3           Green               4096      4096      0
            Yellow              3276      3276      0
            Out of Profile                          0
4           Green               4096      4096      0
            Yellow              3276      3276      0
            Out of Profile                          0
5           Green               4096      4096      0
            Yellow              3276      3276      0
            Out of Profile                          0
6           Green               4096      4096      0
            Yellow              3276      3276      0
            Out of Profile                          0
7           Green               4096      4096      0
            Yellow              3276      3276      0
            Out of Profile                          0
Linecard 7 port pipe 0, to linecard 3 port pipe 1, unicast
SF          Packet Type         Min       Max       Dropped
Ingress                         KB        KB        packets
Queue#
0           Green               4096      4096      0
            Yellow              3276      3276      0
            Out of Profile                          0
1           Green               4096      4096      0
            Yellow              3276      3276      0
            Out of Profile                          0
2           Green               4096      4096      0
            Yellow              3276      3276      0
            Out of Profile                          0
3           Green               4096      4096      0
            Yellow              3276      3276      0
            Out of Profile                          0
4           Green               4096      4096      0
            Yellow              3276      3276      0
            Out of Profile                          0
5           Green               4096      4096      0
            Yellow              3276      3276      0
            Out of Profile                          0
6           Green               4096      4096      0
            Yellow              3276      3276      0
            Out of Profile                          0
7           Green               4096      4096      0
            Yellow              3276      3276      0
            Out of Profile                          0
4           Green               4096      4096      0
            Yellow              3276      3276      0
            Out of Profile                          0
5           Green               4096      4096      0
            Yellow              3276      3276      0
            Out of Profile                          0
6           Green               4096      4096      0
            Yellow              3276      3276      0
            Out of Profile                          0
7           Green               4096      4096      0
            Yellow              3276      3276      0
            Out of Profile 0
```

Figure 394 show queue statistics ingress Command (EtherScale) Partial

Table 123 defines the columns displayed in Figure 394.

Table 123 show queue statistics Command Fields

Field	Description
SF Ingress Queue #	Switch Fabric Queue Number
Packet type	Green, yellow, and out-of-profile packets
Min KB	Minimum threshold for WRED queue
Max KB	Maximum threshold for WRED queue
Dropped Pkts	The number of packets dropped for green, yellow and out-of-profile

Example 2

```
Force10#show queue statistics ingress multicast src-card 7

Linecard 7 port pipe 0, multicast

SF          Packet Type         Min       Max       Dropped
Ingress                         KB        KB        packets
Queue#
0           Green               4096      4096      0
            Yellow              3276      3276      0
            Out of Profile                          0
1           Green               4096      4096      0
            Yellow              3276      3276      0
            Out of Profile                          0
2           Green               4096      4096      0
            Yellow              3276      3276      0
            Out of Profile                          0
3           Green               4096      4096      0
            Yellow              3276      3276      0
            Out of Profile                          0
4           Green               4096      4096      0
            Yellow              3276      3276      0
            Out of Profile                          0
5           Green               4096      4096      0
            Yellow              3276      3276      0
            Out of Profile                          0
6           Green               4096      4096      0
            Yellow              3276      3276      0
            Out of Profile                          0
7           Green               4096      4096      0
            Yellow              3276      3276      0
            Out of Profile                          0

Linecard 7 port pipe 1, multicast

SF          Packet Type         Min       Max       Dropped
Ingress                         KB        KB        packets
Queue#
0           Green               4096      4096      0
            Yellow              3276      3276      0
            Out of Profile                          0
1           Green               4096      4096      0
            Yellow              3276      3276      0
            Out of Profile                          0
2           Green               4096      4096      0
            Yellow              3276      3276      0
            Out of Profile                          0
3           Green               4096      4096      0
            Yellow              3276      3276      0
            Out of Profile                          0
4           Green               4096      4096      0
            Yellow              3276      3276      0
            Out of Profile                          0
5           Green               4096      4096      0
            Yellow              3276      3276      0
            Out of Profile                          0
6           Green               4096      4096      0
            Yellow              3276      3276      0
            Out of Profile                          0
7           Green               4096      4096      0
            Yellow              3276      3276      0
            Out of Profile                          0
Force10#
```

Figure 395 show queue statistics ingress Multicast Command (EtherScale)

Table 124 defines the columns displayed in Figure 395.

Table 124 show queue statistics ingress Multicast Command Fields

Field	Description
SF Ingress Queue #	Switch Fabric Queue Number
Packet type	Green, yellow, and out-of-profile packets

Table 124 show queue statistics ingress Multicast Command Fields

Field	Description
Min KB	Minimum threshold for WRED queue
Max KB	Maximum threshold for WRED queue
Dropped Pkts	The number of packets dropped for green, yellow and out-of-profile

Example 3

```
Force10#show queue statistics ingress src-card 0 brief
Source Linecard 0

Dest LC         Src             Dest            Dropped
                Port set        Port set        packets
0               0               0               0
0               0               1               100
0               1               0               0
0               1               1               100
1               0               0               0
1               0               1               100
1               1               0               0
1               1               1               100
2               0               0               0
2               0               1               100
2               1               0               0
2               1               1               100
3               0               0               0
3               0               1               100
3               1               0               0
3               1               1               100
4               0               0               0
4               0               1               100
4               1               0               0
4               1               1               100
5               0               0               0
5               0               1               100
5               1               0               0
5               1               1               100
6               0               0               0
6               0               1               100
6               1               0               0
6               1               1               100
RPM             0                               0
RPM             1                               100
Multicast       0                               0
Multicast       1                               0

Force10#
```

Figure 396 show queue statistics ingress brief Command

Table 125 defines the columns displayed in Figure 396.

Table 125 show queue statistics ingress brief Command Fields

Field	Description
Dest LC	Destination Line Card
Src Port Set	Source PortPipe Number
Dest Port Set	Destination PortPipe Number
Dropped Pkts	The number of packets dropped

Related Commands

clear queue statistics egress	Clear egress queue statistics.
clear queue statistics ingress	Clear ingress queue statistics.
show queue statistics egress	Display egress queue statistics

Chapter 45 Multicast

FTOS supports IGMPv1/v2/v3 and IGMP Snooping in addition to general multicast commands.

- Multicast Commands on page 1277 (**E-Series Only**)
- IGMP Commands on page 1284 (**E-Series Only**)
- IGMP Snooping Commands on page 1292 (**E-Series and C-Series**)

Note: Multicast is not supported on secondary IP addresses.

Multicast Commands

C-Series	NO
E-Series	✓

Platform Specific Feature: The general Multicast commands are supported on E-Series Only.

General Multicast commands are:

- clear ip mroute on page 1278
- ip mroute on page 1278
- ip multicast-lag-hashing on page 1279
- mtrace on page 1281
- show ip mroute on page 1281
- show ip rpf on page 1283

clear ip mroute

C-Series	No
E-Series	✓

Clear learned multicast routes on the multicast forwarding table. To clear PIM routes, use clear ip pim tib command.

Syntax **clear ip mroute** {*group-address* [*source-address*] | *}

Parameters

group-address [*source-address*]	Enter multicast group address and source address (if desired), in dotted decimal format, to clear information on a specific group.
*	Enter * to clear all multicast routes.

Command Modes EXEC privilege

Related Commands

show ip pim tib	Clear the PIM Tree Information Base.

ip mroute

C-Series	No
E-Series	✓

Assign a static mroute to the E-Series.

Syntax **ip mroute** *destination mask* **[null 0] | [protocol [process-id | tag] ip-address] |Static** *ip-address \ Ip-address* [*distance*]

To delete a specific static mroute, use the **no ip mroute** *destination mask* **[null 0] | [protocol [process-id | tag] ip-address] |Static** *ip-address \ Ip-address* [*distance*] command.

To delete all mroutes matching a certain mroute, use the **no ip mroute** *destination mask* command.

Parameters

destination	Enter the IP address in dotted decimal format of the destination device.
mask	Enter the mask in slash prefix formation (/x) of the destination device's IP address.
null 0	(OPTIONAL) Enter the null followed by zero (0).

protocol [process-id | tag] ip-address	(OPTIONAL) Enter one of the routing protocols: • Enter the BGP as-number followed by the IP address in dotted decimal format of the reverse path forwarding (RPF) neighbor. Range:1-65535 • Enter the OSPF process identification number followed by the IP address in dotted decimal format of the reverse path forwarding (RPF) neighbor. Range: 1-65535 • Enter the IS-IS alphanumeric tag string followed by the IP address in dotted decimal format of the reverse path forwarding (RPF) neighbor. • Enter the RIP IP address in dotted decimal format of the reverse path forwarding (RPF) neighbor.
Static *ip-address*	(OPTIONAL) Enter the Static IP address in dotted decimal format of the reverse path forwarding (RPF) neighbor.
ip-address	(OPTIONAL) Enter the IP address in dotted decimal format of the reverse path forwarding (RPF) neighbor.
distance	(OPTIONAL) Enter a number as the distance metric assigned to the mroute. Range: 1 to 255

Defaults Not configured.

Command Modes CONFIGURATION

Related Commands

show ip mroute	View the E-Series routing table.

ip multicast-lag-hashing

C-Series	No
E-Series	✓

Distribute multicast traffic among Port Channel members in a round-robin fashion.

Syntax **ip multicast-lag-hashing**

To revert to the default, enter **no ip multicast-lag-hashing**.

Defaults Disabled

Command Modes CONFIGURATION

Command History

Version 6.3.1.0	Introduced

Usage Information

By default, one Port Channel member is chosen to forward multicast traffic. With this feature turned on, multicast traffic will be distributed among the Port Channel members in a round-robin fashion. This feature applies to the routed multicast traffic. If IGMP Snooping is turned on, this feature also applies to switched multicast traffic.

Related Commands

ip multicast-routing	Enable IP multicast forwarding.

ip multicast-routing

C-Series	**No**
E-Series	✓

Enable IP multicast forwarding.

Syntax **ip multicast-routing**

To disable multicast forwarding, enter **no ip multicast-routing**.

Defaults Disabled

Command Modes CONFIGURATION

Usage Information

You must enter this command to enable multicast on the E-Series.

After you enable multicast, you can enable IGMP and PIM on an interface. In the INTERFACE mode, enter the ip pim sparse-mode command to enable IGMP and PIM on the interface.

Related Commands

ip pim sparse-mode	Enable IGMP and PIM on an interface.

mtrace

C-Series	No
E-Series	✓

Trace a multicast route from the source to the receiver.

Syntax **mtrace** {*source/host address*} {*destination/host*} {*group-address*}

Parameters

source/host address	Enter the source IP address in dotted decimal format (A.B.C.D).
destination/host	Enter the destination (receiver) IP address in dotted decimal format (A.B.C.D).
group-address	Enter the multicast group address in dotted decimal format (A.B.C.D).

Command Modes EXEC privilege

Command History

Version 7.5.1.0	Expanded to support originator
Version 7.4.1.0	Expanded to support intermediate (transit) router

Usage Information Mtrace is an IGMP protocol based on the Multicast traceroute facility and implemented according to the IETF draft "A *traceroute* facility for IP Multicast" (draft-fenner-traceroute-ipm-01.txt). FTOS supports the Mtrace client and transmit functionality.

As an Mtrace client, FTOS transmits Mtrace queries, receives, parses and prints out the details in the response packet received.

As an Mtrace transit or intermediate router, FTOS returns the response to Mtrace queries. Upon receiving the Mtrace request, FTOS computes the RPF neighbor for the source, fills in the request and the forwards the request to the RPF neighbor. While computing the RPF neighbor, the static mroute and mBGP route is preferred over the unicast route.

show ip mroute

C-Series	No
E-Series	✓

View multicast routes.

Syntax **show ip mroute** [**static** | *group-address* [*source-address*] | **active** [*rate*] | **count** | **summary**]

Parameters

static	(OPTIONAL) Enter the keyword **static** to view static multicast routes.
group-address [*source-address*]	(OPTIONAL) Enter the multicast group-address to view only routes associated with that group. Enter the source-address to view routes with that group-address and source-address.
active [*rate*]	(OPTIONAL) Enter the keyword **active** to view only active multicast routes. Enter a rate to view active routes over the specified rate. Range: 0 to 10000000
count	(OPTIONAL) Enter the keyword **count** to view the number of multicast routes and packets on the E-Series.
summary	(OPTIONAL) Enter the keyword **summary** to view routes in a tabular format.

Command Modes

EXEC

EXEC privilege

Example 1

```
Force10#show ip mroute static

Mroute: 23.23.23.0/24, interface: Lo 2
Protocol: static, distance: 0, route-map: none, last change: 00:00:23

Force10#
```

Figure 397 show ip mroute static Command Example

Example 2

```
Force10#show ip mroute

IP Multicast Routing Table

(*, 224.10.10.1), uptime 00:05:12
  Incoming interface: GigabitEthernet 3/12
  Outgoing interface list:
    GigabitEthernet 3/13

(1.13.1.100, 224.10.10.1), uptime 00:04:03
  Incoming interface: GigabitEthernet 3/4
  Outgoing interface list:
    GigabitEthernet 3/12
    GigabitEthernet 3/13

(*, 224.20.20.1), uptime 00:05:12
  Incoming interface: GigabitEthernet 3/12
  Outgoing interface list:
    GigabitEthernet 3/4

Force10#
```

Figure 398 show ip mroute Command Example

Table 126 explains the fields in Figure 398.

Table 126 show ip mroute Command Example Fields

Field	Description
(S,G)	Displays the forwarding entry in the multicast route table.
uptime	Displays the amount of time the entry has been in the multicast forwarding table.
Incoming interface	Displays the reverse path forwarding (RPF) information towards the the source for (S,G) entries and the RP for (*,G) entries.
Outgoing interface list:	Lists the interfaces that meet one of the following: • a directly connected member of the Group • statically configured member of the Group • received a (*,G) or (S,G) Join message

show ip rpf

C-Series	No
E-Series	✓

View reverse path forwarding.

Syntax **show ip rpf**

Command Modes EXEC

EXEC privilege

Usage Information Static mroutes are used by network administrators to control the reachability of the multicast sources. If a PIM registered multicast source is reachable via static mroute as well as unicast route, the distance of each route is examined and the route with shorter distance is the one the PIM selects for reachability.

Note: The default distance of mroutes is zero (0) and is CLI configurable on a per route basis.

Example

```
force10#show ip rpf
RPF information for 10.10.10.9
   RPF interface: Gi 3/4
   RPF neighbor: 165.87.31.4
   RPF route/mask: 10.10.10.9/255.255.255.255
   RPF type: unicast
```

Figure 399 show ip rpf Command Example

IGMP Commands

Platform Specific Feature: The IGMPv1/v2/v3 commands are supported on E-Series Only.

FTOS supports IGMPv1/v2/v3 and is compliant with RFC-3376.

Important Points to Remember

- FTOS supports PIM-SM and PIM-SSM include and exclude modes
- IGMPv2 is the default version of IGMP on interfaces. IGMPv3 can be configured on interfaces and is backward compatible with IGMPv2.
- Maximum number of interfaces supported is 512
- Maximum number of groups supported – no hard limit
- IGMPv3 router interoperability with IGMPv2 and IGMPv1 routers on the same subnet is *not* supported
- An administrative command (**ip igmp version**) is added to manually set the IGMP version.
- All commands, previously used for IGMPv2, are compatible with IGMPv3.

The commands include:

- clear ip igmp groups on page 1285
- debug ip igmp on page 1285
- ip igmp immediate-leave on page 1286
- ip igmp last-member-query-interval on page 1286
- ip igmp querier-timeout on page 1287
- ip igmp query-interval on page 1287
- ip igmp query-max-resp-time on page 1288
- ip igmp static-group on page 1288
- ip igmp version on page 1289
- show ip igmp groups on page 1290
- show ip igmp interface on page 1291

clear ip igmp groups

C-Series	No
E-Series	✓

Clear entries from the group cache table.

Syntax **clear ip igmp groups** [*group-address* | *interface*]

Parameters

group-address	(OPTIONAL) Enter the IP multicast group address in dotted decimal format.
interface	(OPTIONAL) Enter the following keywords and slot/port or number information: • For an 100/1000 Base-T Ethernet interface, enter the keyword **gigabitethernet** followed by the slot/port information. • For a 1-Gigabit Ethernet interface, enter the keyword **gigabitethernet** followed by the slot/port information. • For a SONET interface, enter the keyword **sonet** followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **tengigabitethernet** followed by the slot/port information.

Command Modes EXEC privilege

Usage Information IGMP commands accept *only* non-VLAN interfaces—specifying VLAN will not yield a results.

debug ip igmp

C-Series	No
E-Series	✓

Enable debugging of IGMP packets.

Syntax **debug ip igmp** [*group address* | *interface*]

To disable IGMP debugging, enter **no ip igmp**. To disable all debugging, enter **undebug all**.

Parameters

group-address	(OPTIONAL) Enter the IP multicast group address in dotted decimal format.
interface	(OPTIONAL) Enter the following keywords and slot/port or number information: • For an 100/1000 Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For a SONET interface, enter the keyword **sonet** followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information.

Defaults Disabled

Command Modes EXEC privilege

Usage Information IGMP commands accept *only* non-VLAN interfaces—specifying VLAN will not yield a results.

ip igmp immediate-leave

C-Series	No
E-Series	✓

Enable IGMP immediate leave.

Syntax **ip igmp immediate-leave** [**group-list** *prefix-list-name*]

To disable ip igmp immediate leave, use the **no ip igmp immediate-leave** command.

Parameters

group-list *prefix-list-name*	Enter the keyword **group-list** followed by a string up to 16 characters long of the *prefix-list-name*.

Defaults Not configured

Command Modes INTERFACE

Usage Information Querier normally send a certain number of group specific queries when a leave message is received, for a group, prior to deleting a group from the membership database. There may be situations in which immediate deletion of a group from the membership database is required. This command provides a way to achieve the immediate deletion. In addition, this command provides a way to enable immediate-leave processing for specified groups.

ip igmp last-member-query-interval

C-Series	No
E-Series	✓

Change the last member query interval, which is the Max Response Time inserted into Group-Specific Queries sent in response to Leave Group messages. This interval is also the interval between Group-Specific Query messages.

Syntax **ip igmp last-member-query-interval** *milliseconds*

To return to the default value, enter **no ip igmp last-member-query-interval**.

Parameters		
	milliseconds	Enter the number of milliseconds as the interval. Default: 1000 milliseconds Range: 100 to 65535

Defaults 1000 milliseconds

Command Modes INTERFACE

ip igmp querier-timeout

C-Series	No
E-Series	✓

Change the interval that must pass before a multicast router decides that there is no longer another multicast router that should be the querier.

Syntax **ip igmp querier-timeout** *seconds*

To return to the default value, enter **no ip igmp querier-timeout**.

Parameters		
	seconds	Enter the number of seconds the router must wait to become the new querier. Default: 120 seconds Range: 60 to 300

Defaults 120 seconds

Command Modes INTERFACE

ip igmp query-interval

C-Series	No
E-Series	✓

Change the transmission frequency of IGMP general queries sent by the Querier.

Syntax **ip igmp query-interval** *seconds*

To return to the default values, enter **no ip igmp query-interval**.

Parameters		
	seconds	Enter the number of seconds between queries sent out. Default: 60 seconds Range: 1 to 18000

Defaults 60 seconds

Command Modes INTERFACE

ip igmp query-max-resp-time

C-Series	No
E-Series	✓

Set the maximum query response time advertised in the General Queries.

Syntax **ip igmp query-max-resp-time** *seconds*

To return to the default values, enter **no ip igmp query-max-resp-time**.

Parameters		
	seconds	Enter the number of seconds. Default: 10 seconds Range: 1 to 25

Defaults 10 seconds

Command Modes INTERFACE

ip igmp static-group

C-Series	No
E-Series	✓

Configure an IGMP static group.

Syntax **ip igmp static-group** {*group address* [**exclude** [*source address*]] | [**include** {*source address*}]}

To delete a static address, use the **no ip igmp static-group** {*group address* [**exclude** [*source address*]] | [**include** {*source address*}]} command.

Parameters

group address	Enter the group address in dotted decimal format (A.B.C.D)
exclude *source address*	(OPTIONAL) Enter the keyword **exclude** followed by the source address, in dotted decimal format (A.B.C.D), for which a static entry needs to be added.
include *source address*	(OPTIONAL) Enter the keyword **include** followed by the source address, in dotted decimal format (A.B.C.D), for which a static entry needs to be added. **Note:** A group in **include** mode must have at least one source address defined.

Defaults

No default values or behavior

Command Modes

INTERFACE

Command History

Version 7.5.1.0	Expanded to support the **exclude** and **include** options

Usage Information

A group in the **include** mode should have at least one source address defined. In **exclude** mode if no source address is specified, FTOS implicitly assumes all sources are excluded. If neither **include** or **exclude** is specified, FTOS implicitly assumes a IGMPv2 static join.

Command Limitations

- Only one mode (**include** or **exclude**) is permitted per multicast group per interface. To configure another mode, all sources belonging to the original mode must be unconfigured.
- If a static configuration is present and a packet for the same group arrives on an interface, the dynamic entry will completely overwrite all the static configuration for the group.

Related Commands

show ip igmp groups	Display IGMP group information

ip igmp version

C-Series	**No**
E-Series	✓

Manually set the version of the router to IGMPv2 or IGMPv3.

Syntax

ip igmp version {**2** | **3**}

Parameters

2	Enter the number **2** to set the IGMP version number to IGMPv2.
3	Enter the number **3** to set the IGMP version number to IGMPv3.

Defaults

2 that is IGMPv2

Command Modes INTERFACE

Command History

Version 7.5.1.0	Introduced

show ip igmp groups

C-Series	**No**
E-Series	✓

View the IGMP groups.

Syntax **show ip igmp groups** [*group-address* [**detail**] | **detail** | *interface* [*group-address* [**detail**]]]

Parameters

group-address	(OPTIONAL) Enter the group address in dotted decimal format to view information on that group only.
interface	(OPTIONAL) Enter the interface type and slot/port information: • For a 100/1000 Ethernet interface, enter the keyword **gigabitethernet** followed by the slot/port information. • For a 1-Gigabit Ethernet interface, enter the keyword **gigabitethernet** followed by the slot/port information. • For a Loopback interface, enter the keyword **loopback** followed by a number from 0 to 16383. • For a SONET interface, enter the keyword **sonet** followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **tengigabitethernet** followed by the slot/port information. • For a VLAN interface enter the keywork **vlan** followed by a number from 1 to 4094.
detail	(OPTIONAL) Enter the keyword **detail** to display the IGMPv3 source information.

Command Modes EXEC

EXEC privilege

Command History

Version 7.5.1.0	Expanded to support the **detail** option.

Usage Information This command displays the IGMP database including configured entries for either all groups on all interfaces, or all groups on specific interfaces, or specific groups on specific interfaces.

Example

```
Force10#show ip igmp groups
IGMP Connected Group Membership
Group Address    Interface                Uptime    Expires   Last Reporter
224.0.1.40       GigabitEthernet 13/6     09:45:23  00:02:08  10.87.7.5
Force10#
```

Figure 400 show ip igmp groups Command Example

Table 127 defines the fields displayed in Figure 400

Table 127 show ip igmp groups Command Example Fields

Field	Description
Group Address	Lists the multicast address for the IGMP group.
Interface	Lists the interface type, slot and port number.
Uptime	Displays the amount of time the group has been operational.
Expires	Displays the amount of time until the entry expires.
Last Reporter	Displays the IP address of the last host to be a member of the IGMP group.

show ip igmp interface

C-Series	No
E-Series	✓

View information on the interfaces participating in IGMP.

Syntax **show ip igmp interface** [*interface*]

Parameters

interface (OPTIONAL) Enter the interface type and slot/port information:

- For a 100/1000 Ethernet interface, enter the keyword **gigabitethernet** followed by the slot/port information.
- For a 1-Gigabit Ethernet interface, enter the keyword **gigabitethernet** followed by the slot/port information.
- For a Loopback interface, enter the keyword **loopback** followed by a number from 0 to 16383.
- For a SONET interface, enter the keyword **sonet** followed by the slot/port information.
- For a 10-Gigabit Ethernet interface, enter the keyword **tengigabitethernet** followed by the slot/port information.

Command Modes

EXEC
EXEC privilege

Usage Information

IGMP commands accept *only* non-VLAN interfaces—specifying VLAN will not yield a results.

Example

```
Force10#show ip igmp interface
GigabitEthernet 0/0 is down, line protocol is down
  Internet protocol processing disabled
GigabitEthernet 0/5 is down, line protocol is down
  Internet protocol processing disabled
GigabitEthernet 0/6 is down, line protocol is down
  Internet protocol processing disabled
GigabitEthernet 0/7 is up, line protocol is down
  Internet protocol processing disabled
GigabitEthernet 7/9 is up, line protocol is up
  Internet address is 10.87.5.250/24
  IGMP is enabled on interface
  IGMP query interval is 60 seconds
  IGMP querier timeout is 120 seconds
  IGMP max query response time is 10 seconds
  IGMP last member query response interval is 1000 ms
  IGMP activity: 0 joins, 0 leaves
  IGMP querying router is 10.87.5.250 (this system)
  IGMP version is 2
```

Figure 401 show ip igmp interface Command Example

IGMP Snooping Commands

FTOS supports IGMP Snooping version 2 on both the E-Series and C-Series chassis. The IGMP Snooping commands are:

- debug ip igmp on page 1293
- ip igmp snooping enable on page 1294
- ip igmp snooping fast-leave on page 1295
- ip igmp snooping flood on page 1295
- ip igmp snooping last-member-query-interval on page 1296
- ip igmp snooping mrouter on page 1296
- ip igmp snooping querier on page 1297
- show ip igmp snooping mrouter on page 1297

Important Points to Remember for IGMP Snooping

- FTOS supports version 1 and version 2 hosts.
- FTOS IGMP snooping implementation is based on IP multicast address (not based on Layer 2 multicast mac-address) and the IGMP snooping entries are in Layer 3 flow table not in Layer 2 FIB.
- FTOS IGMP snooping implementation is based on draft-ietf-magma-snoop-10.
- FTOS supports IGMP snooping on JUMBO enabled cards.
- IGMP snooping is not enabled by default on the switch.
- A maximum of 1800 groups and 600 VLAN are supported.
- IGMP snooping is not supported on default VLAN interface.
- IGMP snooping is not supported over VLAN-Stack-enabled VLAN interfaces (you must disable IGMP snooping on a VLAN interface before configuring VLAN-Stack-related commands).

- IGMP snooping does not react to Layer 2 topology changes triggered by STP.
- IGMP snooping reacts to Layer 2 topology changes triggered by MSTP by sending a general query on the interface that comes in FWD state.

Important Points to Remember for IGMP Querier

- The IGMP snooping Querier supports version 2.
- You must configure an IP address to the VLAN interface for IGMP snooping Querier to begin. The IGMP snooping Querier disables itself when a VLAN IP address is cleared, and then it restarts itself when an IP address is re-assigned to the VLAN interface.
- When enabled, IGMP snooping Querier will not start if there is a statically configured multicast router interface in the VLAN.
- When enabled, IGMP snooping Querier starts after one query interval in case no IGMP general query (with IP SA lower than its VLAN IP address) is received on any of its VLAN members.
- When enabled, IGMP snooping Querier periodically sends general queries with an IP source address of the VLAN interface. If it receives a general query on any of its VLAN member, it will check the IP source address of the incoming frame.

  If the IP SA in the incoming IGMP general query frame is lower than the IP address of the VLAN interface, then the switch disables its IGMP snooping Querier functionality.

  If the IP SA of the incoming IGMP general query is higher than the VLAN IP address, the switch will continue to work as an IGMP snooping Querier.

debug ip igmp

Enable debugging of IGMP packets.

Syntax **debug ip igmp** [*group address* | *interface*]

To disable IGMP debugging, enter **no debug ip igmp**. To disable all debugging, enter **undebug all**.

Parameters

group-address	(OPTIONAL) Enter the IP multicast group address in dotted decimal format.
interface	(OPTIONAL) Enter the following keywords and slot/port or number information: • For an 100/1000 Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information. • For VLAN, enter the keywork **vlan** followed by a number from 1 to 4094. • For a Port Channel interface, enter the keyword **port-channel** followed by a number: C-Series Range: 1-128 E-Series Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale

Defaults Disabled

Command Modes EXEC privilege

ip igmp snooping enable

Enable IGMP snooping globally. This is the master on/off switch to enable IGMP snooping.

Syntax **ip igmp snooping enable**

To disable IGMP snooping, enter **no ip igmp snooping enable** command.

Defaults Disabled

Command Modes CONFIGURATION

Usage Information You must enter this command to enable IGMP snooping. When enabled globally, IGMP Snooping is enabled on all VLAN interfaces (except default VLAN).

Note: You must execute the **no shutdown** command on the VLAN interface for IGMP Snooping to function.

Related Commands

no shutdown	Activate an interface

ip igmp snooping fast-leave

Enable IGMP snooping fast leave for this VLAN.

Syntax **ip igmp snooping fast-leave**

To disable IGMP snooping fast leave, use the **no igmp snooping fast-leave** command.

Defaults Not configured

Command Modes INTERFACE VLAN—(conf-if-vl-*n*)

Usage Information Queriers normally send a certain number of queries when a leave message is received prior to deleting a group from the membership database. There may be situations in which *fast* deletion of a group is required. When IGMP fast leave processing is enabled, the switch will remove an interface from the multicast group as soon as it detects an IGMP version 2 leave message on the interface.

ip igmp snooping flood

This command controls the flooding behavior of unregistered multicast data packets. When flooding is enabled (the default), unregistered multicast data traffic is flooded to all ports in a VLAN. When flooding is disabled, unregistered multicast data traffic is forwarded to *only* multicast router ports, both static and dynamic, in a VLAN. If there is no multicast router port in a VLAN, then unregistered multicast data traffic is dropped.

Syntax **ip igmp snooping flood**

To disable flooding, enter **no ip igmp snooping flood**.

Defaults Enabled

Command Modes CONFIGURATION

Usage Information When flooding is disabled default entries are installed for each and every VLAN, where IGMP snooping is enabled, to forward the unregistered multicast data traffic to multicast router ports.

When flooding is enabled, all the default entries are removed to enable flooding of unregistered multicast data traffic to all ports in a VLAN.

ip igmp snooping last-member-query-interval

The last member query interval is the "maximum response time" inserted into Group-Specific queries sent in response to Group-Leave messages. This interval is also the interval between successive Group-Specific Query messages. Use this command to change the last member query interval.

Syntax **ip igmp snooping last-member-query-interval** *milliseconds*

To return to the default value, enter **no ip igmp snooping last-member-query-interval**.

Parameters

milliseconds	Enter the interval in milliseconds. Default: 1000 milliseconds Range: 100 to 65535

Defaults 1000 milliseconds

Command Modes INTERFACE VLAN—(conf-if-vl-*n*)

ip igmp snooping mrouter

Statically configure a VLAN member port as a multicast router interface.

Syntax **ip igmp snooping mrouter interface**

To delete a specific multicast router interface, use the **no igmp snooping mrouter interface** command.

Parameters

interface	Enter the following keywords and slot/port or number information: • For an 100/1000 Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information. • For a Port Channel interface, enter the keyword **port-channel** followed by a number: C-Series Range: 1-128 E-Series Range: 1 to 32 for EtherScale, 1 to 255 for TeraScale

Defaults Not configured

Command Modes INTERFACE VLAN—(conf-if-vl-*n*)

Usage Information FTOS provides the capability of statically configuring interface to which a multicast router is attached. To configure a static connection to the multicast router, enter the **ip igmp snooping mrouter interface** command in the VLAN context. The interface to the router must be a part of the VLAN where you are entering the command.

ip igmp snooping querier

Enable IGMP querier processing for the VLAN interface.

Syntax **ip igmp snooping querier**

To disable IGMP querier processing for the VLAN interface, enter **no igmp snooping querier** command.

Defaults Not configured

Command Modes INTERFACE VLAN—(conf-if-vl-*n*)

Usage Information This command enables the IGMP switch to send General Queries periodically. This is useful when there is no multicast router present in the VLAN because the multicast traffic does not need to be routed. An IP address must be assigned to the VLAN interface for the switch to act as a querier for this VLAN.

show ip igmp snooping mrouter

Display multicast router interfaces.

Syntax **show ip igmp snooping mrouter**

Command Modes EXEC

EXEC privilege

Example

```
Force10#show ip igmp snooping mrouter
Interface Router Ports
Vlan 2    Gi 13/3, Po 1
Force10#
```

Related Commands		
	show ip igmp groups	Use this IGMP command to view groups

Chapter 46 IPv6 Multicast

C-Series	NO
E-Series	✓

Platform Specific Feature: IPv6 Multicast is supported on the E-Series only.

FTOS supports Multicast Listener Discovery Protocol (MLD) version 2 and is backward compatible with MLD version 1. FTOS supports MLD Snooping version 1 only.

- IPv6 Multicast Commands on page 1299
- MLD Commands on page 1304
- MLD Snooping Commands on page 1311

Note: Multicast is not supported on secondary IP addresses.

IPv6 Multicast Commands

General IPv6 Multicast commands are:

- clear ipv6 mroute on page 1300
- show ipv6 mroute on page 1300
- show ipv6 mroute mld on page 1303
- show ipv6 mroute summary on page 1304

clear ipv6 mroute

C-Series	No
E-Series	✓

Clear learned multicast routes on the multicast forwarding table. To clear PIM routes, use clear ipv6 pim tib command.

Syntax **clear ipv6 mroute** {*group-address* [*source-address*] | *}

Parameters

group-address [*source-address*]	Enter multicast group address and source address (if desired) to clear information on a specific group. Enter the addresses in the **x:x:x:x::x** format. The **::** notation specifies successive hexadecimal fields of zero.
*	Enter * to clear all multicast routes.

Defaults No default behavior or values

Command Modes EXEC privilege

Command History

Version 7.4.1.0	Introduced

Related Commands

show ipv6 pim tib	Clear the IPv6 PIM Tree Information Base.

show ipv6 mroute

C-Series	No
E-Series	✓

View IPv6 multicast routes.

Syntax **show ipv6 mroute** [*group-address* [*source-address*]] [**active** *rate*] [**count** *group-address* [**source** *source-address*]]

Parameters

group-address [*source-address*]	(OPTIONAL) Enter the IPv6 multicast group-address to view only routes associated with that group. Optionally, enter the IPv6 source-address to view routes with that group-address and source-address.

active *rate*]	(OPTIONAL) Enter the keyword **active** to view active multicast sources. Enter a rate to view active routes over the specified rate. Range: 0 to 10000000
count *group-address* [**source** *source-address*]}	(OPTIONAL) Enter the keyword **count** to view the number of IPv6 multicast routes and packets on the E-Series. Optionally, enter the IPv6 source-address count information.

Command Modes

EXEC

EXEC privilege

Command History

Version 7.4.1.0	Introduced

Example

```
YForce10#show ipv6 mroute
IP Multicast Routing Table
(165:87:32::30, ff05:100::1), uptime 00:01:11
  Incoming interface: Vlan 200
  Outgoing interface list:
    GigabitEthernet 2/14

(165:87:37::30, ff05:200::1), uptime 00:01:04
  Incoming interface: Port-channel 200
  Outgoing interface list:
    Vlan 200

(165:87:31::30, ff05:300::1), uptime 00:01:19
  Incoming interface: GigabitEthernet 2/14
  Outgoing interface list:
    Port-channel 200

(165:87:32::30, ff05:1100::1), uptime 00:01:08
  Incoming interface: Vlan 200
  Outgoing interface list:
    GigabitEthernet 2/14

(165:87:37::30, ff05:2200::1), uptime 00:01:01
  Incoming interface: Port-channel 200
  Outgoing interface list:
    Vlan 200

Force10#
```

Figure 402 show ipv6 mroute command Example

Example

```
Force10#show ipv6 mroute active 10

Active Multicast Sources - sending >= 10 pps

Group: ff05:300::1
   Source: 165:87:31::30
     Rate: 100 pps

Group: ff05:3300::1
   Source: 165:87:31::30
     Rate: 100 pps

Group: ff3e:300::4000:1
   Source: 165:87:31::20
     Rate: 100 pps

Group: ff3e:3300::4000:1
   Source: 165:87:31::20
     Rate: 100 pps

Force10#
```

Figure 403 show ipv6 mroute active command Example

Example

```
Force10#show ipv6 mroute count group ff05:3300::1

IP Multicast Statistics
1 routes using 648 bytes of memory
1 groups, 1.00 average sources per group
Forwarding Counts: Pkt Count/Pkts per second

Group: ff05:3300::1, Source count: 1
  Source: 165:87:31::30, Forwarding: 3997/0
Force10#
```

Figure 404 show ipv6 mroute count group command Examples

Example

```
Force10#show ipv6 mroute count source 165:87:31::30

IP Multicast Statistics
2 routes using 1296 bytes of memory
2 groups, 1.00 average sources per group
Forwarding Counts: Pkt Count/Pkts per second

Group: ff05:300::1, Source count: 1
 Source: 165:87:31::30, Forwarding: 3993/0

Group: ff05:3300::1, Source count: 1
 Source: 165:87:31::30, Forwarding: 3997/0

Force10#
```

Figure 405 show ipv6 mroute count source command Examples

show ipv6 mroute mld

C-Series	No
E-Series	✓

Display the Multicast MLD information.

Syntax **show ipv6 mroute** [**mld** [*group-address* | **all** | **vlan** *vlan-id*]]

Parameters

mld	(OPTIONAL) Enter the keyword **mld** to display Multicast MLD information.
group-address	(OPTIONAL) Enter the multicast group address in the **x:x:x:x::x** format. The **::** notation specifies successive hexadecimal fields of zero.
all	(OPTIONAL) Enter the keyword **all** to view all the MLD information.
vlan *vlan-id*	(OPTIONAL) Enter the keyword **vlan** followed by the VLAN ID to view MLD VLAN information.

Defaults No default values or behavior

Command Modes EXEC

EXEC privilege

Command History

Version 7.4.1.0	Introduced

Example

```
Force10#show ipv6 mroute mld all

MLD SNOOPING MRTM Table

(*, ff05:100::1), uptime 00:04:21
  Incoming vlan: Vlan 200
  Outgoing interface list:
    GigabitEthernet 2/15
    GigabitEthernet 2/16

(*, ff05:200::1), uptime 00:04:15
  Incoming vlan: Vlan 200
  Outgoing interface list:
    GigabitEthernet 2/15
    GigabitEthernet 2/16

(*, ff05:1100::1), uptime 00:04:18
  Incoming vlan: Vlan 200
  Outgoing interface list:
    GigabitEthernet 2/15
    GigabitEthernet 2/16
Force10#
```

Figure 406 show ipv6 mroute mld all command Example

show ipv6 mroute summary

C-Series	No
E-Series	✓

Display a summary of the Multicast routing table.

Syntax **show ipv6 mroute summary**.

Defaults No default values or behavior

Command Modes EXEC

EXEC privilege

Command History

Version 7.4.1.0	Introduced

Example

```
Force10#show ipv6 mroute summary

IP Multicast Routing Table
12 groups, 12 routes

(165:87:32::30, ff05:100::1), 00:00:24
(165:87:37::30, ff05:200::1), 00:00:24
(165:87:31::30, ff05:300::1), 00:00:24
(165:87:32::30, ff05:1100::1), 00:00:21
(165:87:37::30, ff05:2200::1), 00:00:21
(165:87:31::30, ff05:3300::1), 00:00:21
(165:87:32::20, ff3e:100::4000:1), 00:00:41
Force10#
```

MLD Commands

FTOS supports MLD version 2 and is backward compatible with version 1. The MLD commands are:

- clear ipv6 mld groups on page 1305
- debug ipv6 mld on page 1306
- ipv6 mld explicit-tracking on page 1306
- ipv6 mld last-member-query-interval on page 1307
- ipv6 mld querier-timeout on page 1307
- ipv6 mld query-interval on page 1308
- ipv6 mld query-max-resp-time on page 1308
- ipv6 mld static-group on page 1309
- ipv6 mld version on page 1310

- show ipv6 mld interface on page 1310

clear ipv6 mld groups

C-Series	No
E-Series	✓

Clear entries from the group cache table.

Syntax **clear ipv6 mld groups** [*interface* | *group-address*]

Parameters

interface	(OPTIONAL) Enter the following keywords and slot/port or number information: • For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For a Port Channel interface, enter the keyword **port-channel** followed by a number from 1 to 255. • For a SONET interface, enter the keyword **sonet** followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information. • For a VLAN, enter the keyword **vlan** followed by a number from 1 to 4094.
group-address	(OPTIONAL) Enter the group address in the **x:x:x:x::x** format. The **::** notation specifies successive hexadecimal fields of zero.

Defaults No default values or behavior

Command Modes EXEC privilege

Command History

Version 7.4.1.0	Introduced

Related Commands

show ipv6 mld interface	Display the IPv6 MLD interface

debug ipv6 mld

C-Series	No
E-Series	✓

Enable debugging on IPv6 MLD packets.

Syntax **degug ipv6 mld** {*group-address* | *interface*}

To turn off debugging, use the **no debug ipv6 mld** {*group-address* | *interface*} command.

Parameters

group-address	(OPTIONAL) Enter the multicast group address in the **x:x:x:x::x** format. The **::** notation specifies successive hexadecimal fields of zero.
interface	(OPTIONAL) Enter the following keywords and slot/port or number information: • For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For a Port Channel interface, enter the keyword **port-channel** followed by a number from 1 to 255. • For a SONET interface, enter the keyword **sonet** followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information. • For a VLAN, enter the keyword **vlan** followed by a number from 1 to 4094.

Defaults Disabled

Command Modes EXEC privilege

Command History

Version 7.4.1.0	Introduced

ipv6 mld explicit-tracking

C-Series	No
E-Series	✓

Enable MLD explicit tracking of receivers.

Syntax **ipv6 mld explicit-tracking**

To disable explicit tracking, use the **no ipv6 mld explicit-tracking** command.

Defaults Disabled

Command Modes INTERFACE (conf-if)

Command History

Version 7.4.1.0	Introduced

ipv6 mld last-member-query-interval

C-Series	No
E-Series	✓

Change the MAX Response Time inserted into the Group-Specific Queries sent in response to a Leave Group messages. This interval is also the interval between Group-Specific Query messages.

Syntax **ipv6 mld last-member-query-interval** {*milliseconds*}

To return to the default, use the **no ipv6 mld last-member-query-interval** {*milliseconds*} command.

Parameters

milliseconds	Enter the last member query interval in milliseconds. Range: 200 - 60000 Default: 1000

Defaults 1000 milliseconds

Command Modes INTERFACE (conf-if)

Command History

Version 7.4.1.0	Introduced

ipv6 mld querier-timeout

C-Series	No
E-Series	✓

Change the interval that must pass before a multicast router decides that there is no longer another multicast router that should be the querier.

Syntax **ipv6 mld querier-timeout** {*seconds*}

To return to the default, use the **no ipv6 mld querier-timeout** command.

Parameters

seconds	Enter the querier timeout in seconds. Range: 60 - 300 Default: 255

Defaults 255 seconds

Command Modes INTERFACE (conf-if)

Command History

Version 7.4.1.0	Introduced

ipv6 mld query-interval

C-Series	**No**
E-Series	✓

Change the transmission frequency of the MLD host.

Syntax **ipv6 mld query-interval** {*seconds*}

To return to the default interval, use the **no ipv6 mld query-interval** command.

Parameters

seconds	Enter the interval in seconds. Range: 1 - 18000 Default: 125

Defaults 125 seconds

Command Modes INTERFACE (conf-if)

Command History

Version 7.4.1.0	Introduced

ipv6 mld query-max-resp-time

Set the maximum query response time advertised in the general queries.

C-Series	No
E-Series	✓

Syntax **ipv6 mld query-max-resp-time** {*seconds*}

To return to the default, use the **no ipv6 mld query-max-resp-time** command.

Parameters

seconds	Enter the interval in seconds. Range: 1 - 25 Default: 10

Defaults 10 seconds

Command Modes INTERFACE (conf-if)

Command History

Version 7.4.1.0	Introduced

ipv6 mld static-group

C-Series	No
E-Series	✓

Configure an MLD static group to exclude or include mode.

Syntax **ipv6 mld static-group** *group-address* {**exclude** [*source-address*] | **include** *source-address*}

To return to default, use the **no ipv6 mld static-group** *group-address* {**exclude** [*source-address*] | **include** *source-address*} command.

Parameters

group-address	(OPTIONAL) Enter the multicast group address in the **x:x:x:x::x** format. The **::** notation specifies successive hexadecimal fields of zero.
exclude *source-address*	Enter the keyword **exclude** and optionally enter the source ip address in the **x:x:x:x::x** format. The **::** notation specifies successive hexadecimal fields of zero.
include *source-address*	Enter the keyword **include** followed by source ip address in the **x:x:x:x::x** format. The **::** notation specifies successive hexadecimal fields of zero.

Defaults No default behavior or values

Command Modes INTERFACE (conf-if)

Command History	
Version 7.4.1.0	Introduced

ipv6 mld version

C-Series	No
E-Series	✓

Set the MLD version number on this interface.

Syntax **ipv6 mld version 1**

Defaults Version 2

Command Modes INTERFACE (conf-if)

Command History	
Version 7.4.1.0	Introduced

Usage Information FTOS supports MLD version 2 and is backward compatible with MLD version 1.

Command History	
Version 7.4.1.0	Introduced

show ipv6 mld interface

C-Series	No
E-Series	✓

View the configured MDL interfaces.

Syntax **show ipv6 mld interface** [*interface*]

Parameters

interface [*interface*]	Enter the keyword **interface** to display the configured MDL interfaces. Optionally, enter the keyword **interface** followed by one of the keywords below, with slot/port or number information, to display information for that specific interface: • For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For a Port Channel interface, enter the keyword **port-channel** followed by a number from 1 to 255. • For a SONET interface, enter the keyword **sonet** followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information. • For a VLAN, enter the keyword **vlan** followed by a number from 1 to 4094.

Command Modes

EXEC

EXEC privilege

Command History

Version 7.4.1.0	Introduced

Example

```
Force10#show ipv6 mld interface

GigabitEthernet 2/14 is up, line protocol is up
  Interface address is fe80::201:e8ff:fe08:9a09/64
  Current MLD version is 2
  MLD query interval is 125 seconds
  MLD querier expiry time is 255 seconds
  MLD max query response time is 10 seconds
  Last member response interval is 1000 ms
  MLD explicit tracking is disabled
  MLD querying router is fe80::201:e8ff:fe08:9a09 (this router)

Port-channel 200 is up, line protocol is up
  Interface address is fe80::201:e8ff:fe08:9abd/64
  Current MLD version is 2
  MLD query interval is 125 seconds
  MLD querier expiry time is 255 seconds
  MLD max query response time is 10 seconds
  Last member response interval is 1000 ms
  MLD explicit tracking is disabled
  MLD querying router is fe80::201:e8ff:fe08:9abd (this router)

Vlan 200 is up, line protocol is up
  Interface address is fe80::201:e8ff:fe08:9abc/64
  Current MLD version is 2
  MLD query interval is 125 seconds
  MLD querier expiry time is 255 seconds
  MLD max query response time is 10 seconds
  Last member response interval is 1000 ms
  MLD explicit tracking is disabled
  MLD querying router is fe80::201:e8ff:fe08:9abc (this router)
Force10#
```

MLD Snooping Commands

FTOS supports MLD Snooping version 1 only:

- ipv6 mld snooping enable on page 1312

- ipv6 mld snooping flood on page 1312
- ipv6 mld snooping on page 1313
- ipv6 mld snooping explicit-tracking on page 1313
- ipv6 mld snooping mrouter on page 1314
- ipv6 mld snooping querier on page 1315
- show ipv6 mld snooping groups on page 1315
- show ipv6 mld snooping mrouter on page 1316

ipv6 mld snooping enable

C-Series	No
E-Series	✓

Enable MLD Snooping globally.

Syntax **ipv6 mld snooping enable**

To disable MLD Snooping, use the **no ipv6 mld snooping** {**enable | flood**} command.

Defaults Disabled

Command Modes CONFIGURATION (conf)

Command History

Version 7.4.1.0	Introduced

ipv6 mld snooping flood

C-Series	No
E-Series	✓

Enable MLD Snooping Flood globally.

Syntax **ipv6 mld snooping flood**

To disable, use the **no ipv6 mld snooping flood** command.

Defaults Enabled

Command Modes CONFIGURATION (conf)

Usage Information When flooding is enabled, unregistered multicast data is flooded on the VLAN.

When flooding is disabled, unregistered multicast data is forwarded only to mrouter ports on the VLAN.

Command History

Version 7.4.1.0	Introduced

ipv6 mld snooping

C-Series	No
E-Series	✓

Enable MLD Snooping on this interface.

Syntax **ipv6 mld snooping**

To disable MLD Snooping, use the **no ipv6 mld snooping** command.

Defaults Enabled on all VLAN interfaces

Command Modes INTERFACE VLAN (conf-if-vl-*n*)

Command History

Version 7.4.1.0	Introduced

ipv6 mld snooping explicit-tracking

C-Series	No
E-Series	✓

Enable explicit MLD Snooping tracking on an interface.

Syntax **ipv6 mld snooping explicit-tracking**

To disable, use the **no ipv6 mld snooping explicit-tracking** command.

Defaults Disabled

Command Modes INTERFACE VLAN (conf-if-vl-*n*)

Command History

Version 7.4.1.0	Introduced

ipv6 mld snooping mrouter

C-Series	**No**
E-Series	✓

Configure a Layer 2 port as a multicast router port.

Syntax **ipv6 mld snooping mrouter interface** {*interface*}

To return to default, use the **no ipv6 mld snooping mrouter** {*interface*}command.

Parameters

interface	Enter the keyword **interface** to indicate the next-hop interface to the multicast router.
interface	Enter the following keywords and slot/port or number information: • For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For a Port Channel interface, enter the keyword **port-channel** followed by a number from 1 to 255. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information.

Defaults No default values or behavior

Command Modes INTERFACE VLAN (conf-if-vl-*n*)

Command History

Version 7.4.1.0	Introduced

ipv6 mld snooping querier

C-Series	No
E-Series	✓

Enable the MLD querier processing for the VLAN interface.

Syntax **ipv6 mld snooping querier**

To disable the querier feature, use the **no ipv6 mld snooping querier** command.

Defaults Disabled

Command Modes INTERFACE VLAN (conf-if-vl-*n*)

Command History

Version 7.4.1.0	Introduced

Usage Information This command enables the VLAN to send out periodic queries as a proxy querier.

show ipv6 mld snooping groups

C-Series	No
E-Series	✓

Display the IPv6 MLD Snooping group information.

Syntax **show ipv6 mld snooping groups** [*group-address*] [**explicit**] [**link-local**] [**summary**] [**vlan**]

Parameters

group-address	(OPTIONAL) Enter the multicast group address in the **x:x:x:x::x** format. The **::** notation specifies successive hexadecimal fields of zero.
explicit	(OPTIONAL) Enter the keyword **explicit** to display explicit tracking information.
link-local	(OPTIONAL) Enter the keyword **link-local** to display link local groups.
summary	(OPTIONAL) Enter the keyword **summary** to display a summary of groups.
vlan	(OPTIONAL) Enter the keyword **vlan** followed by the VLAN number to display information on that specific VLAN. Range: 1 - 4094

Defaults No default values or behavior

Command Modes EXEC

EXEC privilege

Command History

Version 7.4.1.0	Introduced

Example

```
Force10#show ipv6 mld snooping groups summary
MLD snooping connected groups summary:
  (*,G) routes :12
Force10#
```

show ipv6 mld snooping mrouter

C-Series	**No**
E-Series	✓

Display information on the MLD Snooping router.

Syntax **show ipv6 mld snooping mrouter** [**vlan**]

Parameters

vlan	(OPTIONAL) Enter the keyword **vlan** followed by the VLAN number to display information on that specific VLAN. Range: 1 - 4094

Defaults No default values or behavior

Command Modes EXEC

EXEC privilege

Command History

Version 7.4.1.0	Introduced

Example

```
Force10#show ipv6 mld snooping mrouter
Interface       Ports (* - Dynamic)
Vlan 2          Gi 13/18
Force10#
```

Chapter 47 Protocol Independent Multicast

Platform Specific Feature: Protocol Independent Multicast is supported on the E-Series only.

FTOS supports Protocol Independent Multicast version 2 in both Sparse-Mode (PIM-SM) and Dense Mode (PIM-DM).

- PIM Sparse-Mode on page 1317
- PIM-SSM on page 1330
- PIM Dense-Mode on page 1332

PIM Sparse-Mode

PIM-SM on VLAN interfaces is supported on TeraScale platforms only. The commands are:

- clear ip pim rp-mapping on page 1318
- clear ip pim tib on page 1318
- debug ip pim on page 1318
- lp pim bsr-border on page 1319
- lp pim bsr-candidate on page 1320
- ip pim dr-priority on page 1320
- ip pim query-interval on page 1321
- ip pim rp-address on page 1321
- ip pim rp-candidate on page 1322
- ip pim sparse-mode on page 1323
- ip pim spt-threshold on page 1324
- show ip pim bsr-router on page 1324
- show ip pim interface on page 1325
- show ip pim neighbor on page 1326
- show ip pim rp on page 1327
- show ip pim tib on page 1328

clear ip pim rp-mapping

C-Series	No
E-Series	✓

Used by the bootstrap router (BSR) to remove all or particular Rendezvous Point (RP) Advertisement.

Syntax **clear ip pim rp-mapping** *rp-address*

Parameters

rp-address	(OPTIONAL) Enter the RP address in dotted decimal format (A.B.C.D)

Command Modes EXEC

clear ip pim tib

C-Series	No
E-Series	✓

Clear PIM tree information from the PIM database.

Syntax **clear ip pim tib** [*group*]

Parameters

group	(OPTIONAL) Enter the multicast group address in dotted decimal format (A.B.C.D)

Command Modes EXEC privilege

debug ip pim

C-Series	No
E-Series	✓

View IP PIM debugging messages.

Syntax **debug ip pim** [**bsr** | **events** | **group** | **packet** [**in** | **out**] | **register** | **state** | **timer** [**assert** | **hello** | **joinprune** | **register**]]

To disable PIM debugging, enter **no debug ip pim** or enter **undebug all** to disable all debugging.

Parameters

bsr	(OPTIONAL) Enter the keyword **bsr** to view PIM Candidate RP/BSR activities.
events	(OPTIONAL) Enter the keyword **events** to view PIM events.
group	(OPTIONAL) Enter the keyword **group** to view PIM messages for a specific group.
packet [**in** | **out**]	(OPTIONAL) Enter the keyword **packet** to view PIM packets. Enter one of the optional parameters • in: to view incoming packets • out: to view outgoing packets.
register	(OPTIONAL) Enter the keyword **register** to view PIM register address in dotted decimal format (A.B.C.D).
state	(OPTIONAL) Enter the keyword **state** to view PIM state changes.
timer [**assert** | **hello** | **joinprune** | **register**]	(OPTIONAL) Enter the keyword **timer** to view PIM timers. Enter one of the optional parameters: • assert: to view the assertion timer. • hello: to view the PIM neighbor keepalive timer. • joinprune: to view the expiry timer (join/prune timer) • register: to view the register suppression timer.

Defaults Disabled

Command Modes EXEC privilege

Ip pim bsr-border

C-Series	No
E-Series	✓

Define the border of PIM domain by filtering inbound and outbound PIM-BSR messages per interface.

Syntax **ip pim bsr-border**

To return to the default value, enter **no ip pim bsr-border**.

Defaults Disabled

Command Modes INTERFACE

Usage Information This command is applied to the subsequent PIM-BSR. Existing BSR advertisements are cleaned up by time out. Candidate RP advertisements can be cleaned using the clear ip pim rp-mapping command.

Ip pim bsr-candidate

C-Series	No
E-Series	✓

Configure the PIM router to join the Bootstrap election process.

Syntax **ip pim bsr-candidate** *interface* [*hash-mask-length*] [*priority*]

To return to the default value, enter **no ip pim bsr-candidate**.

Parameters

interface	Enter the following keywords and slot/port or number information: • For a Fast Ethernet interface, enter the keyword **FastEthernet** followed by the slot/port information. • For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For a Loopback interface, enter the keyword **loopback** followed by a number from 0 to 16383. • For a SONET interface, enter the keyword **sonet** followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information. • For a VLAN, enter the keyword **vlan** followed by a number from 1 to 4094.
hash-mask-length	(OPTIONAL) Enter the hash mask length. Range: zero (0) to 32 Default: 30
priority	(OPTIONAL) Enter the priority used in Bootstrap election process. Range: zero (0) to 255 Default: zero (0)

Defaults Not configured.

Command Modes CONFIGURATION

Command History

Version 6.1.1.0	Added support for VLAN interface

ip pim dr-priority

C-Series	No
E-Series	✓

Change the Designated Router (DR) priority for the interface.

Syntax **ip pim dr-priority** *priority-value*

To remove the DR priority value assigned, use the **no ip pim dr-priority** command.

Parameters

priority-value	Enter a number. Preference is given to larger/higher number. Range: 0 to 4294967294 Default: 1

Defaults 1

Command Modes INTERFACE

Usage Information The router with the largest value assigned to an interface becomes the Designated Router. If two interfaces contain the same DR priority value, the interface with the largest interface IP address becomes the Designated Router.

ip pim query-interval

C-Series	**No**
E-Series	✓

Change the frequency of PIM Router-Query messages.

Syntax **ip pim query-interval** *seconds*

To return to the default value, enter **no ip pim query-interval** *seconds* command.

Parameters

seconds	Enter a number as the number of seconds between router query messages. Default: 30 seconds Range: 0 to 65535

Defaults 30 seconds

Command Modes INTERFACE

ip pim rp-address

C-Series	**No**
E-Series	✓

Configure a static PIM Rendezvous Point (RP) address for a group. This address is used by first-hop routers to send Register packets on behalf of source multicast hosts.

Syntax **ip pim rp-address** *address* **group-address** *group-address mask* **override**

To remove an RP address, use the **no ip pim re-address** *address* **group-address** *group-address mask* **override**.

Parameters

address	Enter the RP address in dotted decimal format (A.B.C.D).
group-address *group-address mask*	Enter the keyword **group-address** followed by a group-address mask, in dotted decimal format (/xx), to assign that group address to the RP.
override	Enter the keyword **override** to override the BSR updates with static RP. The override will take effect immediately during enable/diable. **Note:** This option is applicable to multicast group range.

Defaults Not configured.

Command Modes CONFIGURATION

Usage Information The RP addresses are stored in the order in which they are entered. RP addresses learned via BSR take priority over static RP addresses.

Without the override option, RPs advertised by the BSR updates take precedence over the statically configured RPs.

ip pim rp-candidate

C-Series	No
E-Series	✓

Configure PIM router to send out Candidate-RP-Advertisement message to the Bootstrap (BS) router.

Syntax **ip pim rp-candidate** *interface* [*priority*]

To return to the default value, enter **no ip pim rp-candidate**.

Parameters

interface	Enter the following keywords and slot/port or number information: • For a Fast Ethernet interface, enter the keyword **FastEthernet** followed by the slot/port information. • For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For a Loopback interface, enter the keyword **loopback** followed by a number from 0 to 16383. • For a SONET interface, enter the keyword **sonet** followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information. • For a VLAN, enter the keyword **vlan** followed by a number from 1 to 4094.
priority	(OPTIONAL) Enter the priority used in Bootstrap election process. Range: zero (0) to 255 Default: 192

Defaults Not configured.

Command Modes CONFIGURATION

Usage Information Priority is stored at BSR router when receiving a Candidate-RP-Advertisement.

ip pim sparse-mode

C-Series	**No**
E-Series	✓

Enable PIM sparse mode and IGMP on the interface.

Syntax **ip pim sparse-mode**

To disable PIM sparse mode and IGMP, enter **no ip pim sparse-mode**.

Defaults Disabled.

Command Modes INTERFACE

Usage Information The interface must be enabled (**no shutdown** command) and not have the **switchport** command configured. Multicast must also be enabled globally (using the ip multicast-lag-hashing command). PIM is supported on the port-channel interface.

Related Commands

ip multicast-lag-hashing	Enable multicast globally.

ip pim spt-threshold

C-Series	No
E-Series	✓

Configure PIM router to switch to shortest path tree when the traffic reaches the specified threshold value.

Syntax **ip pim spt-threshold** *value* | **infinity**

To return to the default value, enter **no ip pim spt-threshold**.

Parameters

value	(OPTIONAL) Enter the traffic value in kilobits per second. Default: 10 packets per second. A value of zero (0) will cause a switchover on the first packet.
infinity	(OPTIONAL) To never switch to the source-tree, enter the keyword **infinity**.

Defaults Not configured.

Command Modes CONFIGURATION

Usage Information This is applicable to last hop routers on the shared tree towards the Rendezvous Point (RP).

show ip pim bsr-router

C-Series	No
E-Series	✓

View information on the Bootstrap router.

Syntax **show ip pim bsr-router**

Command Modes EXEC

EXEC privilege

Example

```
E600-7-rpm0#show ip pim bsr-router
PIMv2 Bootstrap information
This system is the Bootstrap Router (v2)
   BSR address: 7.7.7.7 (?)
   Uptime:     16:59:06, BSR Priority: 0, Hash mask length: 30
   Next bootstrap message in 00:00:08

This system is a candidate BSR
   Candidate BSR address: 7.7.7.7, priority: 0, hash mask length: 30
```

Figure 407 show ip pim bsr-router Command Example

show ip pim interface

C-Series	**No**
E-Series	✔

View information on the interfaces with IP PIM enabled.

Syntax **show ip pim interface**

Command Modes EXEC

EXEC privilege

Example

```
E600-7-RPM0#show ip pim interface
Address         Interface Ver/   Nbr    Query  DR   DR
                          Mode   Count  Intvl  Prio
172.21.200.254  Gi 7/9    v2/S    0      30     1   172.21.200.254
172.60.1.2      Gi 7/11   v2/S    0      30     1   172.60.1.2
192.3.1.1       Gi 7/16   v2/S    1      30     1   192.3.1.1
192.4.1.1       Gi 13/5   v2/S    0      30     1   192.4.1.1
172.21.110.1    Gi 13/6   v2/S    0      30     1   172.21.110.1
172.21.203.1    Gi 13/7   v2/S    0      30     1   172.21.203.1
```

Figure 408 show ip pim interface Command Example

Table 128 describes the fields in Figure 408.

Table 128 show ip pim interface Command Example Fields

Field	Description
Address	Lists the IP addresses of the interfaces participating in PIM.
Interface	List the interface type, with either slot/port information or ID (VLAN or Port Channel), of the interfaces participating in PIM.

Table 128 show ip pim interface Command Example Fields

Field	Description
Ver/Mode	Displays the PIM version number and mode for each interface participating in PIM. • v2 = PIM version 2 • S = PIM Sparse mode
Nbr Count	Displays the number of PIM neighbors discovered over this interface.
Query Intvl	Displays the query interval for Router Query messages on that interface (configured with ip pim query-interval command).
DR Prio	Displays the Designated Router priority value configured on the interface (ip pim dr-priority command).
DR	Displays the IP address of the Designated Router for that interface.

show ip pim neighbor

C-Series	No
E-Series	✓

View PIM neighbors.

Syntax **show ip pim neighbor**

Command Modes EXEC

EXEC privilege

Example

```
Force10#show ip pim neighbor
Neighbor          Interface      Uptime/Expires     Ver  DR
Address                                                 Prio/Mode
127.87.3.4        Gi 7/16        09:44:58/00:01:24  v2   1  / S
Force10#
```

Figure 409 show ip pim neighbor Command Example

Table 129 describes the fields in Figure 408.

Table 129 show ip pim neighbor Command Example Fields

Field	Description
Neighbor address	Displays the IP address of the PIM neighbor.
Interface	List the interface type, with either slot/port information or ID (VLAN or Port Channel), on which the PIM neighbor was found.
Uptime/expires	Displays the amount of time the neighbor has been up followed by the amount of time until the neighbor is removed from the multicast routing table (that is, until the neighbor hold time expires).
Ver	Displays the PIM version number. • v2 = PIM version 2
DR prio/Mode	Displays the Designated Router priority and the mode. • 1 = default Designated Router priority (use ip pim dr-priority) • DR = Designated Router • S = source

show ip pim rp

C-Series	**No**
E-Series	✓

View all multicast groups-to-RP mappings.

Syntax **show ip pim rp [mapping** | *group-address*]

Parameters

mapping	(OPTIONAL) Enter the keyword **mapping** to display the multicast groups-to-RP mapping and information on how RP is learnt.
group-address	(OPTIONAL) Enter the multicast group address mask in dotted decimal format to view RP for a specific group.

Command Modes EXEC

EXEC privilege

Example 1

```
Force10#sh ip pim rp
Group           RP
224.2.197.115   165.87.20.4
224.2.217.146   165.87.20.4
224.3.3.3       165.87.20.4
225.1.2.1       165.87.20.4
225.1.2.2       165.87.20.4
229.1.2.1       165.87.20.4
229.1.2.2       165.87.20.4
Force10#
```

Figure 410 show ip pim rp mapping Command Example 1

Example 2

```
Force10#sh ip pim rp mapping
Group(s): 224.0.0.0/4
  RP: 165.87.20.4, v2
    Info source: 165.87.20.5, via bootstrap, priority 0
         Uptime: 00:03:11, expires: 00:02:46
  RP: 165.87.20.3, v2
    Info source: 165.87.20.5, via bootstrap, priority 0
         Uptime: 00:03:11, expires: 00:03:03

Force10#
```

Figure 411 show ip pim rp mapping Command Example 2

Example 3

```
Force10#sh ip pim rp 229.1.2.1
Group           RP
229.1.2.1       165.87.20.4

Force10#
```

Figure 412 show ip pim rp *group-address* Command Example 3

show ip pim tib

C-Series	**No**
E-Series	✓

View the PIM tree information base (TIB).

Syntax **show ip pim tib** [*group-address* [*source-address*]]

Parameters

group-address	(OPTIONAL) Enter the group address in dotted decimal format (A.B.C.D)
source-address	(OPTIONAL) Enter the source address in dotted decimal format (A.B.C.D).

Command Modes EXEC

EXEC privilege

Example

```
Force10#show ip pim tib

PIM Multicast Routing Table
Flags: D - Dense, S - Sparse, C - Connected, L - Local, P - Pruned,
       R - RP-bit set, F - Register flag, T - SPT-bit set, J - Join SPT,
       M - MSDP created entry, A - Candidate for MSDP Advertisement,
       K - Ack-Pending State
Timers: Uptime/Expires
Interface state: Interface, next-Hop, State/Mode

(*, 226.1.1.1), uptime 01:29:19, expires 00:00:52, RP 10.211.2.1, flags: SCJ
  Incoming interface: GigabitEthernet 4/23, RPF neighbor 10.211.1.2
  Outgoing interface list:
    GigabitEthernet 8/0

(*, 226.1.1.2), uptime 00:18:08, expires 00:00:52, RP 10.211.2.1, flags: SCJ
  Incoming interface: GigabitEthernet 4/23, RPF neighbor 10.211.1.2
  Outgoing interface list:
    GigabitEthernet 8/0

(*, 226.1.1.3), uptime 00:18:08, expires 00:00:52, RP 10.211.2.1, flags: SCJ
  Incoming interface: GigabitEthernet 4/23, RPF neighbor 10.211.1.2
  Outgoing interface list:
    GigabitEthernet 8/0

(*, 226.1.1.4), uptime 00:18:08, expires 00:00:52, RP 10.211.2.1, flags: SCJ
  Incoming interface: GigabitEthernet 4/23, RPF neighbor 10.211.1.2
  Outgoing interface list:
    GigabitEthernet 8/0

Force10#
```

Figure 413 show ip pim tib Command Example

Table 130 explains the fields in Figure 413.

Table 130 show ip pim tib Command Example Fields

Field	Description
(S, G)	Displays the entry in the multicast PIM database.
uptime	Displays the amount of time the entry has been in the PIM route table.
expires	Displays the amount of time until the entry expires and is removed from the database.
RP	Displays the IP address of the RP/source for this entry.
flags	List the flags to define the entries: • D = PIM Dense Mode • S = PIM Sparse Mode • C = directly connected • L = local to the multicast group • P = route was pruned • R = the forwarding entry is pointing toward the RP • F = FTOS is registering this entry for a multicast source • T = packets were received via Shortest Tree Path • J = first packet from the last hop router is received and the entry is ready to switch to SPT • K=acknowledge pending state
Incoming interface	Displays the reverse path forwarding (RPF) interface towards the RP/source.

Table 130 show ip pim tib Command Example Fields (continued)

Field	Description
RPF neighbor	Displays the next hop from this interface towards the RP/source.
Outgoing interface list:	Lists the interfaces that meet one of the following criteria: • a directly connect member of the Group. • statically configured member of the Group. • received a (*,G) Join message.

PIM-SSM

PIM-SSM protocol is based on the source specific model for forwarding Multicast traffic across multiple domains on the Internet. It is restricted to shortest path trees (SPTs) to specific sources described by hosts using IGMPv3. PIM-SSM is essentially a subset of PIM-SM protocol, which has the capability to join SPTs. The only difference being register states and shared tree states for Multicast groups in SSM range are not maintained. End-hosts use version 3 of the IGMP protocol (IGMPv3) to register their interest in a particular source-group (S,G) pair. PIM-SSM protocol interacts with IGMPv3 to construct the multicast forwarding tree rooted at the source S.

The PIM-SSM commands are:

- ip pim ssm-range on page 1330
- show ip pim ssm-range on page 1331

ip pim ssm-range

C-Series	No
E-Series	✓

Specify the SSM group range using an access-list.

Syntax **ip pim ssm-range** {*access list name*}

To reset, use the **no ip pim ssm-range** {*access list name*} command.

Parameters

access list name	Enter the name of the access list. Maximum 16 characters.

Defaults Default SSM range is 232/8 and ff3x/32

Command Modes CONFIGURATION (conf)

Command History

Version 7.5.1.0	Introduced

Usage Information FTOS supports standard access list for the SSM range. Extended ACL cannot be used for configuring SSM range. If an Extended ACL is configured and then used in the **ip pim ssm-range** {*access list name*} configuration, an error is reported.

However, if **ip pim ssm-range** {*access list name*} is configured first and then the ACL is configured as an Extended ACL, an error is *not* reported and the ACL is not applied to the SSM range.

FTOS recommended best-practices are to configure the standard ACL, and then apply the ACL to the SSM range. Once the SSM range is applied, the changes are applied internally without requiring clearing of the TIB.

When ACL rules change, the ACL and PIM modules apply the new rules automatically.

When SSM range is configured, FTOS supports SSM for configured group range as well as default SSM range.

When the SSM ACL is removed, PIM SSM is supported for default SSM range only

show ip pim ssm-range

C-Series	**No**
E-Series	✓

Display the non-default groups added using the SSM range feature.

Syntax **show ip pim ssm-range** .

Defaults No default behavior or values

Command Modes EXEC

EXEC privilege

Command History

Version 7.5.1.0	Introduced

PIM Dense-Mode

FTOS supports PIM Dense-Mode (PIM-DM) for the specific interface under which the command is issued.

ip pim dense-mode

C-Series	No
E-Series	✓

Enable PIM Dense-Mode (PIM-DM) Multicast capability for the specified interface.

Syntax **ip pim dense-mode**

To disable PIM-DM, use the **no ip pim dense-mode** command.

Defaults Disabled

Command Modes INTERFACE

Command History

Version 6.5.1.0	Introduced

Example

```
Force10#conf
Force10(conf)# interface gigabitethernet 3/27
Force10(gigabitethernet 3/27)# ip address 10.1.1.1 /24
Force10(gigabitethernet 3/27)# no shut
Force10(gigabitethernet 3/27)# ip pim dense-mode

Force10#
```

Usage Information Currently, the chassis operates in either PIM Dense-Mode or PIM Sparse-Mode. The mode configuration for the first PIM enabled interface determines the mode for the entire chassis. Subsequent configurations, on other interfaces, to enable PIM is only accepted if the mode is the same as the original configuration mode. The chassis PIM mode can be changed if PIM-configuration from all interfaces are removed prior to applying a new PIM mode configuration.

Related Commands

ip pim sparse-mode	Configure sparse-mode
show ip pim tib	Display PIM tree information.

Chapter 48 IPv6 Protocol Independent Multicast

C-Series	NO
E-Series	✓

Note: IPv6 Protocol Independent Multicast is supported on E-Series only.

PIM-SSM protocol is based on the source specific model for forwarding Multicast traffic across multiple domains on the Internet. It is restricted to shortest path trees (SPTs) to specific sources described by hosts using IGMPv3. PIM-SSM is essentially a subset of PIM-SM protocol, which has the capability to join SPTs. The only difference being register states and shared tree states for Multicast groups in SSM range are not maintained. End-hosts use version 3 of the IGMP protocol (IGMPv3) to register their interest in a particular source-group (S,G) pair. PIM-SSM protocol interacts with IGMPv3 to construct the multicast forwarding tree rooted at the source S.

FTOS supports 2000 IPv6 multicast forwarding entries, with up to 128 PIM-SSM (Protocol Independent Multicast-Source Specific Multicast) neighbors/interfaces.

Note: IPv6 Multicast is not supported on SONET interfaces.

The IPv6 PIM-SSM commands are:

- clear ipv6 pim tib on page 1334
- debug ipv6 pim on page 1334
- ipv6 pim bsr-candidate on page 1335
- ipv6 pim dr-priority on page 1336
- ipv6 pim query-interval on page 1336
- ipv6 pim rp-address on page 1337
- ipv6 pim rp-candidate on page 1338
- ipv6 pim sparse-mode on page 1338
- ipv6 pim spt-threshold on page 1339
- ipv6 pim ssm-range on page 1339

- show ipv6 pim bsr-router on page 1340
- show ipv6 pim interface on page 1341
- show ipv6 pim neighbor on page 1342
- show ipv6 pim rp on page 1342
- show ipv6 pim tib on page 1343

clear ipv6 pim tib

C-Series	No
E-Series	✓

Clear the IPv6 PIM multicast-routing database (tree information base—tib).

Syntax **clear ipv6 pim tib** [*group-address*]

Parameters

group-address	(OPTIONAL) Enter the multicast group address in the *x:x:x:x::x* format. The *::* notation specifies successive hexadecimal fields of zero.

Defaults No default values or behavior

Command Modes EXEC privilege

Command History

Version 7.4.1.0	Introduced

Related Commands

show ipv6 pim tib	Display the IPv6 PIM tree information base (tib)

debug ipv6 pim

C-Series	No
E-Series	✓

Invoke IPv6 PIM debugging.

Syntax **debug ipv6 pim** [**bsr** | **events** | **group** *group* | **packet** | **register** *[group]* | **state** | | **timer** [**assert** | **hello** | **joinprune** | **register**]]

To disable IPv6 PIM debugging, enter **no debug ipv6 pim**.

Parameters

bsr	(OPTIONAL) Enter the keyword **bsr** to invoke debugging of IPv6 PIM Candidate RP/BSR activities.
events	(OPTIONAL) Enter the keyword **events** to invoke debugging of IPv6 PIM events.
group *group*	(OPTIONAL) Enter the keyword **group** followed by the group address to invoke debugging on that specific group.
packet	(OPTIONAL) Enter the keyword **packet** to invoke debugging of IPv6 PIM packets.
register *[group]*	(OPTIONAL) Enter the keyword **register** and optionally the group address to invoke debugging of IPv6 PIM register messages for a particular group.
state	(OPTIONAL) Enter the keyword **state** to view IPv6 PIM state changes.
timer [**assert** | **hello** | **joinprune** | **register**]	(OPTIONAL) Enter the keyword **timer** to view IPv6 PIM timers. Enter one of the optional parameters: • assert: to view the assertion timer. • hello: to view the IPv6 PIM neighbor keepalive timer. • joinprune: to view the expiry timer (join/prune timer) • register: to view the register suppression timer.

Defaults Disabled

Command Modes EXEC privilege

Command History

Version 7.4.1.0	Introduced

Related Commands

debug ipv6 mld	Turn on debugging of multicast listener discovery (MLD) protocol transactions.

ipv6 pim bsr-candidate

C-Series	**No**
E-Series	✓

Configure the router as a bootstrap (bsr) candidate.

Syntax **ipv6 pim bsr-candidate** *interface* [*hash-mask-length*] [*priority*]

To disable the bootstrap candidate, use the **no ipv6 pim bsr-candidate** command.

Defaults As above

Command Modes CONFIGURATION

Command History

Version 7.4.1.0	Introduced

ipv6 pim dr-priority

C-Series	No
E-Series	✓

Change the Designated Router (DR) priority for the IPv6 interface.

Syntax **ipv6 pim dr-priority** *priority-value*

To remove the DR priority value assigned, use the **no ipv6 pim dr-priority** command.

Parameters

priority-value	Enter a number. Preference is given to larger/higher number. Range: 0 to 4294967294 Default: 1

Defaults 1

Command Modes INTERFACE

Command History

Version 7.4.1.0	Introduced

Usage Information The router with the largest value assigned to an interface becomes the Designated Router. If two interfaces contain the same DR priority value, the interface with the largest interface IP address becomes the Designated Router.

ipv6 pim query-interval

C-Series	No
E-Series	✓

Change the frequency of IPv6 PIM Router-Query messages.

Syntax **ipv6 pim query-interval seconds**

To return to the default value, enter **no ipv6 pim query-interval seconds** command.

Parameters

seconds	Enter a number as the number of seconds between router query messages. Default: 30 seconds Range: 0 to 65535

Defaults 30 seconds

Command Modes INTERFACE

Command History

Version 7.4.1.0	Introduced

ipv6 pim rp-address

C-Series	**No**
E-Series	✓

Configure a static PIM Rendezvous Point (RP) address for a group. This address is used by first-hop routers to send Register packets on behalf of the source multicast host.

Syntax **ipv6 pim rp-address** *address* **group-address** *group-address mask* **override**

To remove an RP address, use the **no ipv6 pim re-address** *address* **group-address** *mask* **override**.

Parameters

address	Enter the IPv6 RP address in the *x:x:x:x::x* format. The *::* notation specifies successive hexadecimal fields of zero.
group-address *group-address mask*	Enter the keyword **group-address** followed by the group address in the *x:x:x:x::x* format and then the mask in /nn format to assign that group address to the RP. The *::* notation specifies successive hexadecimal fields of zero.
override	Enter the keyword **override** to override the BSR updates with static RP. The override will take effect immediately during enable/disable. **Note:** This option is applicable to multicast group range.

Defaults No default values or behavior

Command Modes CONFIGURATION

Command History

Version 7.4.1.0	Introduced

Usage Information

The RP addresses are stored in the order in which they are entered. RP addresses learnt via BSR take priority over static RP addresses.

Without the override option, RPs advertised by the BSR updates take precedence over the statically configured RPs.

ipv6 pim rp-candidate

C-Series	No
E-Series	✓

Specify an interface as an RP candidate.

Syntax **ipv6 pim rp-candidate** *interface* [*priority-value*]

Defaults No default values or behavior

Command Modes CONFIGURATION

Command History

Version 7.4.1.0	Introduced

ipv6 pim sparse-mode

C-Series	No
E-Series	✓

Enable IPv6 PIM sparse mode on the interface.

Syntax **ipv6 pim sparse-mode**

To disable IPv6 PIM sparse mode, enter **no ipv6 pim sparse-mode**.

Defaults Disabled

Command Modes INTERFACE

Command History

Version 7.4.1.0	Introduced

Usage Information The interface must be enabled (**no shutdown** command) and not have the **switchport** command configured. Multicast must also be enabled globally. PIM is supported on the port-channel interface.

ipv6 pim spt-threshold

C-Series	No
E-Series	✓

Specifies when a PIM leaf router should join the shortest path tree.

Syntax **ipv6 pim spt-threshold** {*kbps* | **infinity**}

To return to the default value, enter **no ipv6 pim spt-threshold**.

Defaults 10 kbps

Command Modes CONFIGURATION

Command History

Version 7.4.1.0	Introduced

Usage Information PIM leaf routers join the shortest path tree immediately after the first packet arrives from a new source.

ipv6 pim ssm-range

C-Series	No
E-Series	✓

Specify the SSM group range using an access-list.

Syntax **ipv6 pim ssm-range** {*access list name*}

To reset, use the **no ipv6 pim ssm-range** {*access list name*} command.

Parameters

access list name	Enter the name of the access list. Maximum 16 characters.

Defaults Default SSM range is 232/8 and ff3x/32

Command Modes CONFIGURATION (conf)

Command History

Version 7.5.1.0	Introduced

Usage Information FTOS supports standard access list for the SSM range. Extended ACL cannot be used for configuring SSM range. If an Extended ACL is used with this command, an error is generated. However, if the ACL is applied to SSM range first and then configured as extended, no error is generated, and the ACL is *not* applied to the SSM range. FTOS recommended best-practices are to configure the standard ACL, and then apply the ACL to the SSM range.

Once the SSM range is applied, the changes are applied internally without requiring clearing of the TIB. SSM ACL overrides the default range. To use the default range while SSM range is active, add the default range to the SSM ACL.

When ACL rules change, the ACL manager and PIM modules apply the new rules automatically.

When the SSM ACL is removed, the default range is restored. When SSM range is configured, FTOS supports SSM for configured group range as well as default SSM range.

show ipv6 pim bsr-router

C-Series	No
E-Series	✓

View information on the bootstrap router (v2).

Syntax **show ipv6 pim bsr-router**

Command Modes EXEC

EXEC privilege

Command History

Version 7.4.1.0	Introduced

Example

```
Force10#show ipv6 pim bsr-router
PIMv2 Bootstrap information
This system is the Bootstrap Router (v2)
  BSR address: 14::2
  Uptime:      00:02:54, BSR Priority: 0, Hash mask length: 126
  Next bootstrap message in 00:00:06

This system is a candidate BSR
  Candidate BSR address: 14::2, priority: 0, hash mask length: 126
Force10#
```

show ipv6 pim interface

C-Series	**No**
E-Series	✔

Display IPv6 PIM enabled interfaces.

Syntax **show ipv6 pim interface**

Command Modes EXEC

EXEC privilege

Command History

Version 7.4.1.0	Introduced

Example

```
Force10#show ipv6 pim interface
Interface Ver/   Nbr    Query  DR
          Mode   Count  Intvl  Prio

Gi 10/3   v2/S   1      30     1
  Address : fe80::201:e8ff:fe02:140f
  DR      : this router

Gi 10/11  v2/S   0      30     1
  Address : fe80::201:e8ff:fe02:1417
  DR      : this router
Force10#
```

show ipv6 pim neighbor

C-Series	No
E-Series	✓

DisplaysIPv6 PIM neighbor information.

Syntax **show ipv6 pim neighbor** [**detail**]

Command Modes EXEC

EXEC privilege

Command History

Version 7.4.1.0	Introduced

Example

```
Force10#Force10#show ipv6 pim neighbor detail
Neighbor                  Interface      Uptime/Expires     Ver  DR
Address                                                        Prio/Mode
fe80::201:e8ff:fe00:6265  Gi 10/3        00:07:39/00:01:42  v2   1  / S
165:87:50::6
Force10#
```

show ipv6 pim rp

C-Series	No
E-Series	✓

View all IPv6 multicast groups-to-rendezvous point (RP) mappings.

Syntax **show ipv6 pim rp** [**mapping** | *group-address]*

Parameters

mapping	(OPTIONAL) Enter the keyword **mapping** to display the multicast groups-to-RP mapping and information on how RP is learnt.
group-address	(OPTIONAL) Enter the multicast group address in the *x:x:x:x::x* format to view RP mappings for a specific group. The *::* notation specifies successive hexadecimal fields of zero.

Command Modes EXEC

EXEC privilege

Command History

Version 7.4.1.0	Introduced

Example 1

```
Force10#show ipv6 pim rp
Group              RP
ff0e::225:1:2:1    14::1
ff0e::225:1:2:2    14::1
ff0e::226:1:2:1    14::1
ff0e::226:1:2:2    14::1
Force10#
```

Example 2

```
Force10#show ipv6 pim rp mapping
PIM Group-to-RP Mappings
Group(s): ff00::/8
  RP: 14::1, v2
    Info source: 14::1, via bootstrap, priority 192
         Uptime: 00:03:37, expires: 00:01:53
Group(s): ff00::/8, Static
  RP: 14::2, v2
Force10#
```

show ipv6 pim tib

C-Series	**No**
E-Series	✓

View the IPv6 PIM multicast-routing database (tree information base—tib).

Syntax **show ipv6 pim tib** [*group-address* [*source-address*]]

Parameters

group-address	(OPTIONAL) Enter the IPv6 group address in the *x:x:x:x::x* format. The *::* notation specifies successive hexadecimal fields of zero
source-address	(OPTIONAL) Enter the source address in the *x:x:x:x::x* format. The *::* notation specifies successive hexadecimal fields of zero

Command Modes

EXEC

EXEC privilege

Command History

Version 7.4.1.0	Introduced

Example

```
Force10#show ipv6 pim tib

PIM Multicast Routing Table
Flags: D - Dense, S - Sparse, C - Connected, L - Local, P - Pruned,
       R - RP-bit set, F - Register flag, T - SPT-bit set, J - Join SPT,
       M - MSDP created entry, A - Candidate for MSDP Advertisement
       K - Ack-Pending State
Timers: Uptime/Expires
Interface state: Interface, next-Hop, State/Mode

(25::1, ff0e::225:1:2:1), uptime 00:09:53, expires 00:00:00,flags: CJ
  RPF neighbor: GigabitEthernet 10/3, fe80::201:e8ff:fe00:6265
  Outgoing interface list:
    GigabitEthernet 10/11

(25::1, ff0e::225:1:2:2), uptime 00:09:54, expires 00:00:00,flags: CJ
  RPF neighbor: GigabitEthernet 10/3, fe80::201:e8ff:fe00:6265
  Outgoing interface list:
    GigabitEthernet 10/11

(25::2, ff0e::225:1:2:2), uptime 00:09:54, expires 00:00:00,flags: CJ
  RPF neighbor: GigabitEthernet 10/3, fe80::201:e8ff:fe00:6265
  Outgoing interface list:
    GigabitEthernet 10/11

(25::1, ff0e::226:1:2:1), uptime 00:09:54, expires 00:00:00,flags: CJ
  RPF neighbor: GigabitEthernet 10/3, fe80::201:e8ff:fe00:6265
  Outgoing interface list:
    GigabitEthernet 10/11
Force10#
```

Chapter 49 MSDP

C-Series	NO
E-Series	✓

Note: MSDP is supported on E-Series only.

MSDP (Multicast Source Discovery Protocol) connects multiple PIM Sparse-Mode (PIM-SM) domains together. MSDP peers connect using TCP port 639. Peers send keepalives every 60 seconds. A peer connection is reset after 75 seconds if no MSDP packets are received. MSDP connections are parallel with MBGP connections. FTOS MSDP commands are:

- clear ip msdp peer on page 1345
- clear ip msdp sa-cache on page 1346
- ip msdp cache-rejected-sa on page 1347
- ip msdp default-peer on page 1348
- ip msdp log-adjacency-changes on page 1348
- ip msdp mesh-group on page 1349
- ip msdp originator-id on page 1349
- ip msdp peer on page 1350
- ip msdp sa-limit on page 1352
- ip msdp shutdown on page 1352
- ip multicast-msdp on page 1353
- show ip msdp on page 1353
- show ip msdp sa-cache rejected-sa on page 1355

clear ip msdp peer

C-Series	No
E-Series	✓

Reset the TCP connection to the peer and clear all the peer statistics.

Syntax **clear ip msdp peer** {*peer address*}

Parameters		
	peer address	Enter the peer address in a dotted decimal format (A.B.C.D.)

Defaults Not configured

Command Modes EXEC

Command History		
	Version 6.2.1.1	Introduced

clear ip msdp sa-cache

C-Series	No
E-Series	✓

Clear the source-active entries from the source-active cache of the Multicast group.

Syntax **clear ip msdp sa-cache** {*group address*}

Parameters		
	group address	Enter the group IP address in a dotted decimal format (A.B.C.D.)

Defaults Not configured

Command Modes EXEC

Command History		
	Version 6.2.1.1	Introduced

debug ip msdp

C-Series	No
E-Series	✓

Turn on MSDP debugging.

Syntax **debug ip msdp** {**event** *peer address* | **packet** *peer address* | **pim**}

To turn debugging off, use the **no debug ip msdp** {**event** *peer address* | **packet** *peer address* | **pim**} command.

Parameters

event *peer address*	Enter the keyword **event** followed by the peer address in a dotted decimal format (A.B.C.D.).
packet *peer address*	Enter the keyword **packet** followed by the peer address in a dotted decimal format (A.B.C.D.).
pim	Enter the keyword **pim** to debug advertisement from PIM.

Defaults Not configured

Command Modes EXEC

Command History

Version 6.2.1.1	Introduced

ip msdp cache-rejected-sa

C-Series	No
E-Series	✓

Enable a MSDP cache for the rejected souce-active entries.

Syntax **ip msdp cache-rejected-sa** {*number*}

To clear the MSDP rejected source-active entries, use the **no ip msdp cache-rejected-sa** {*number*}command followed by the **ip msdp cache-rejected-sa** {*number*} command.

Parameters

number	Enter the number of rejected SA entries to cache. Range: 0 to 32766

Defaults No default values or behavior

Command Modes CONFIGURATION

Command History

Version 7.4.1.0	Introduced

Related Commands

show ip msdp sa-cache rejected-sa	Description.

ip msdp default-peer

C-Series	No
E-Series	✓

Define a default peer from which to accept all Source-Active (SA) messages.

Syntax **ip msdp default-peer** {*peer address*} [**prefix-list** *name*]

To remove the default peer, use the **no ip msdp default-peer** {*peer address*} [**prefix-list** *name*] command.

Parameters

peer address	Enter the peer address in a dotted decimal format (A.B.C.D.)
prefix-list *name*	(OPTIONAL) Enter the keyword **prefix-list** followed by a string of up to 16 characters long for the prefix list name.

Defaults Not configured

Command Modes CONFIGURATION

Command History

Version 6.2.1.1	Introduced

Usage Information If the prefix list option is not specified, all SA messages received from the default peer are accepted. You can enter multiple default peer commands.

ip msdp log-adjacency-changes

C-Series	No
E-Series	✓

Enable logging of MSDP adjacency changes.

Syntax **ip msdp log-adjacency-changes**

To disable logging, use the **no ip msdp log-adjacency-changes** command.

Defaults Not configured

Command Modes CONFIGURATION

Command History

Version 6.2.1.1	Introduced

ip msdp mesh-group

C-Series	No
E-Series	✓

Configure a peer to be a member of a mesh group.

Syntax **ip msdp mesh-group** {*name*} {*peer address*}

To remove the peer from a mesh group, use the **no ip msdp mesh-group** {*name*} {*peer address*} command.

Parameters

name	Enter a string of up to 16 characters long for as the mesh group name.
peer address	Enter the peer address in a dotted decimal format (A.B.C.D.)

Defaults Not configured

Command Modes CONFIGURATION

Command History

Version 6.2.1.1	Introduced

Usage Information A MSDP mesh group is a mechanism for reducing SA flooding, typically in an intra-domain setting. When some subset of a domain's MSDP speakers are fully meshed, they can be configured into a mesh-group. If member *X* of a mesh-group receives a SA message from an MSDP peer that is also a member of the mesh-group, member *X* accepts the SA message and forwards it to all of its peers that are not part of the mesh-group.However, member *X* can not forward the SA message to other members of the mesh-group.

ip msdp originator-id

C-Series	No
E-Series	✓

Configure the MSDP Originator ID.

Syntax **ip msdp originator-id** {*interface*}

To remove the originator-id, use the **no ip msdp originator-id** {*interface*} command.

Parameters

interface	Enter the following keywords and slot/port or number information: • For a Fast Ethernet interface, enter the keyword **FastEthernet** followed by the slot/port information. • For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For a Loopback interface, enter the keyword **loopback** followed by a number from 0 to 16383. • For a Port Channel interface, enter the keyword **port-channel** followed by a number from 1 to 32 for EtherScale, 1 to 255 for TeraScale. • For a SONET interface, enter the keyword **sonet** followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information. • For a VLAN, enter the keyword **vlan** followed by a number from 1 to 4094.

Defaults Not configured

Command Modes CONFIGURATION

Command History

Version 6.2.1.1	Introduced

ip msdp peer

C-Series	**No**
E-Series	✓

Configure an MSDP peer.

Syntax **ip msdp peer** *peer address* [**connect-source**] [**description**] [**sa-limit** *number*]

To remove the MSDP peer, use the **no ip msdp peer** *peer address* [**connect-source** *interface*] [**description** *name*] [**sa-limit** *number*] command.

Parameters

peer address	Enter the peer address in a dotted decimal format (A.B.C.D.)
connect-source *interface*	(OPTIONAL) Enter the keyword **connect-source** followed by one of the interfaces and slot/port or number information: • For a Fast Ethernet interface, enter the keyword **FastEthernet** followed by the slot/port information. • For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For a Loopback interface, enter the keyword **loopback** followed by a number from 0 to 16383. • For a Port Channel interface, enter the keyword **port-channel** followed by a number from 1 to 32 for EtherScale, 1 to 255 for TeraScale. • For a SONET interface, enter the keyword **sonet** followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information. • For a VLAN, enter the keyword **vlan** followed by a number from 1 to 4094.
description *name*	(OPTIONAL) Enter the keyword **description** followed by a description name (max 80 characters) to designate a description for the MSDP peer.
sa-limit *number*	(OPTIONAL) Enter the maximum number of SA entries in SA-cache. Range 0 to 40000 Default: 50000

Defaults

As above

Command Modes

CONFIGURATION

Command History

Version 7.5.1.0	Added option for SA upper limit and description option
Version 6.2.1.1	Introduced

Usage Information

The **connect-source** option is used to supply a source IP address for the TCP connection. When an interface is specified uising the **connect-source** option, the primary configured address on the interface is used.

If the total number of SA messages received from the peer is already larger than the limit when this command is applied, those SA messages will continue to be accepted. To enforce the limit in such situation, use command **clear ip msdp peer** command to reset the peer.

Related Commands

ip msdp sa-limit	Configure the MSDP SA Limit
clear ip msdp peer	Clear the MSDP peer.
show ip msdp	Display the MSDP information

ip msdp sa-limit

C-Series	No
E-Series	✓

Configure the upper limit of SA (Source-Active) entries in SA-cache.

Syntax **ip msdp sa-limit** *number*

To return to the default, use the **no ip msdp sa-limit** *number* command.

Parameters

number	Enter the maximum number of SA entries in SA-cache. Range 0 to 40000

Defaults Default 50000

Command Modes CONFIGURATION

Command History

Version 7.5.1.0	Introduced

Usage Information FTOS counts the SA messages originated by itself and those received from the MSDP peers. When the total SA messages reach this limit, the subsequent SA messages are dropped (even if they pass RPF checking and policy checking). If the total number of SA messages is already larger than the limit when this command is applied, those SA messages that are already in FTOS will continue to be accepted. To enforce the limit in such situation, use the **clear ip msdp sa-cache** command.

Related Commands

ip msdp peer	Configure the MSDP peer
clear ip msdp peer	Clear the MSDP peer.
show ip msdp	Display the MSDP information

ip msdp shutdown

C-Series	No
E-Series	✓

Administratively shutdown a configured MSDP peer.

Syntax **ip mdsp shutdown** {*peer address*}

To return to the default, use the **no ip mdsp shutdown** {*peer address*} command.

Parameters		
	peer address	Enter the peer address in a dotted decimal format (A.B.C.D.)

Defaults Not configured

Command Modes CONFIGURATION

Command History		
	Version 6.2.1.1	Introduced

ip multicast-msdp

C-Series	No
E-Series	✓

Enable MSDP.

Syntax **ip multicast-msdp**

To exit MSDP, use the **no ip multicast-msdp** command.

Defaults Not configured

Command Modes CONFIGURATION

Command History		
	Version 6.2.1.1	Introduced

show ip msdp

C-Series	No
E-Series	✓

Display the MSDP peer status, SA cache, or peer summary.

Syntax **show ip msdp** {**peer** *peer address* | **sa-cache** | **summary**}

Parameters

peer *peer address*	Enter the keyword **peer** followed by the peer address in a dotted decimal format (A.B.C.D.)
sa-cache	Enter the keyword **sa-cache** to display the Source-Active cache.
summary	Enter the keyword **summary** to display a MSDP peer summary.

Defaults Not configured

Command Modes EXEC

Command History

Version 6.2.1.1	Introduced

Example 1

```
Force10#show ip msdp peer 100.1.1.1

Peer Addr: 100.1.1.1
    Local Addr: 100.1.1.2(639)  Connect Source: none
    State: Established  Up/Down Time: 00:00:08
    Timers: KeepAlive  60 sec, Hold time  75 sec
    SourceActive packet count (in/out): 0/0
    SAs learned from this peer: 0
    SA Filtering:
    Input (S,G) filter: none
    Output (S,G) filter: none
Force10#
```

Example 2

```
Force10#show ip msdp sa-cache
MSDP Source-Active Cache - 1 entries
GroupAddr       SourceAddr      RPAddr          LearnedFrom   Expire UpTime
224.1.1.1       172.21.220.10   172.21.3.254    172.21.3.254    102 00:02:52
Force10#
```

Example 3

```
Force10#show ip msdp summary
Peer Addr Local Addr State       Source SA Up/Down    Description
72.30.1.2 72.30.1.1  Established none    0 00:00:03   peer1
72.30.2.2 72.30.2.1  Established none    0 00:00:03   peer2
72.30.3.2 72.30.3.1  Established none    0 00:00:02   test-peer-3
Force10#
```

show ip msdp sa-cache rejected-sa

C-Series	No
E-Series	✔

Display the rejected SAs in the SA cache.

Syntax **show ip mdsp sa-cache rejected-sa**

Defaults No default values or behavior

Command Modes EXEC

Command History

Version 7.4.1.0	Introduced

Example

```
Force10#sh ip msdp sa-cache rejected-sa
MSDP Rejected SA Cache  200 rejected SAs received, cache-size 1000
UpTime      GroupAddr       SourceAddr      RPAddr          LearnedFrom     Reason
00:00:13    225.1.2.1       10.1.1.3        110.1.1.1       13.1.1.2        Rpf-Fail
00:00:13    225.1.2.2       10.1.1.4        110.1.1.1       13.1.1.2        Rpf-Fail
00:00:13    225.1.2.3       10.1.1.3        110.1.1.1       13.1.1.2        Rpf-Fail
00:00:13    225.1.2.4       10.1.1.4        110.1.1.1       13.1.1.2        Rpf-Fail
00:00:13    225.1.2.5       10.1.1.3        110.1.1.1       13.1.1.2        Rpf-Fail
00:00:13    225.1.2.6       10.1.1.4        110.1.1.1       13.1.1.2        Rpf-Fail
00:00:13    225.1.2.7       10.1.1.3        110.1.1.1       13.1.1.2        Rpf-Fail
00:00:13    225.1.2.8       10.1.1.4        110.1.1.1       13.1.1.2        Rpf-Fail
00:00:13    225.1.2.9       10.1.1.3        110.1.1.1       13.1.1.2        Rpf-Fail
00:00:13    225.1.2.10      10.1.1.4        110.1.1.1       13.1.1.2        Rpf-Fail
00:00:13    225.1.2.11      10.1.1.3        110.1.1.1       13.1.1.2        Rpf-Fail
00:00:13    225.1.2.11      10.1.1.3        110.1.1.1       13.1.1.2        Rpf-Fail
00:00:13    225.1.2.12      10.1.1.4        110.1.1.1       13.1.1.2        Rpf-Fail
00:00:13    225.1.2.13      10.1.1.3        110.1.1.1       13.1.1.2        Rpf-Fail
00:00:13    225.1.2.14      10.1.1.4        110.1.1.1       13.1.1.2        Rpf-Fail
00:00:13    225.1.2.15      10.1.1.3        110.1.1.1       13.1.1.2        Rpf-Fail
00:00:13    225.1.2.16      10.1.1.4        110.1.1.1       13.1.1.2        Rpf-Fail
00:00:13    225.1.2.17      10.1.1.3        110.1.1.1       13.1.1.2        Rpf-Fail
00:00:13    225.1.2.18      10.1.1.4        110.1.1.1       13.1.1.2        Rpf-Fail
00:00:13    225.1.2.19      10.1.1.3        110.1.1.1       13.1.1.2        Rpf-Fail
Force10#
```

Chapter 50 NDP and RAD

C-Series	NO
E-Series	✓

Platform Specific Feature: NDP and RAD are supported on E-Series only.

This release of FTOS IPv6 supports both:

- Neighbor Discovery Protocol on page 1357
- Router Advertisement Daemon on page 1360

Neighbor Discovery Protocol

The Neighbor Discovery Protocol (NDP) commands for FTOS IPv6 include:

- clear ipv6 neighbors on page 1357
- ipv6 neighbor on page 1358
- show ipv6 neighbors on page 1359

clear ipv6 neighbors

C-Series	No
E-Series	✓

Delete all entries in the IPv6 neighbor discovery cache, or neighbors of a specific interface.

Syntax **clear ipv6 neighbors** [*ipv6-address*] [*interface*]

ipv6-address	Enter the IPv6 address of the neighbor in the **x:x:x:x::x** format. The **::** notation specifies successive hexadecimal fields of zero
interface *interface*	Enter the keyword **interface** followed by the interface type and slot/port or number information of the neighbor interface: • For a Fast Ethernet interface, enter the keyword **fastEthernet** followed by the slot/port information. • For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For a Port Channel interface, enter the keyword **port-channel** followed by a number from 1 to 255. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information. • For a VLAN, enter the keyword **vlan** followed by the VLAN ID. The range is from 1 to 4094.

Command Modes

EXEC

EXEC privilege

ipv6 neighbor

C-Series	No
E-Series	✓

Configure a static entry in the IPv6 neighbor discovery.

Syntax

ipv6 neighbor {*ipv6-address*} {**interface** *interface*} {*hardware address*}

To remove a static IPv6 entry from the IPv6 neighbor discovery, use the **no ipv6 neighbor** {*ipv6-address*} {**interface** *interface*} command.

Parameters

ipv6-address	Enter the IPv6 address of the neighbor in the **x:x:x:x::x** format. The **::** notation specifies successive hexadecimal fields of zero

interface *interface*	Enter the keyword **interface** followed by the interface type and slot/port or number information: • For a Fast Ethernet interface, enter the keyword **fastEthernet** followed by the slot/port information. • For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For a Port Channel interface, enter the keyword **port-channel** followed by a number from 1 to 255. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information. • For a VLAN, enter the keyword **vlan** followed by the VLAN ID. The range is from 1 to 4094.
hardware address	Enter a 48-bit hardware MAC address in nn:nn:nn:nn:nn:nn format.

Defaults No default behavior or values

Command Modes EXEC

EXEC privilege

show ipv6 neighbors

C-Series	No
E-Series	✓

Display IPv6 discovery information.

Syntax **show ipv6 neighbors** [*ipv6-address*] [**cpu**] [**interface** *interface*]

Parameters

ipv6-address	Enter the IPv6 address of the neighbor in the **x:x:x:x::x** format. The **::** notation specifies successive hexadecimal fields of zero
cpu	Enter the keyword **cpu** to display the neighbor entries for this CPU.
interface *interface*	• For a 1-Gigabit Ethernet interface, enter the keyword **GigabitEthernet** followed by the slot/port information. • For the null interface, enter the keyword **null** followed by zero (0). • For loopback interfaces, enter the keyword **loopback** followed by a number from 0 to 16383. • For a Port Channel interface, enter the keyword **port-channel** followed by a number from 1 to 255. • For a SONET interface, enter the keyword **sonet** followed by the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword **TenGigabitEthernet** followed by the slot/port information. • For a VLAN, enter the keyword **vlan** followed by the VLAN ID. The range is from 1 to 4094.

Defaults No default behavior or values

Command Modes EXEC

EXEC privilege

Example

```
Force10#show ipv6 neighbors

IPv6 Address    Expires(min)    Hardware Address    State    Interface  VLAN    CPU
-------------------------------------------------------------------------------
fe80::201:e8ff:fe17:5bc6
                    1439        00:01:e8:17:5b:c6   STALE    Gi 1/9        -    CP
fe80::201:e8ff:fe17:5bc7
                    1439        00:01:e8:17:5b:c7   STALE    Gi 1/10       -    CP
fe80::201:e8ff:fe17:5bc8
                    1439        00:01:e8:17:5b:c8   STALE    Gi 1/11       -    CP
fe80::201:e8ff:fe17:5caf
                    0.3         00:01:e8:17:5c:af   REACH    Po 1          -    CP
fe80::201:e8ff:fe17:5cb0
                    1439        00:01:e8:17:5c:b0   STALE    Po 32         -    CP
fe80::201:e8ff:fe17:5cb1
                    1439        00:01:e8:17:5c:b1   STALE    Po 255        -    CP
fe80::201:e8ff:fe17:5cae
                    1439        00:01:e8:17:5c:ae   STALE    Gi 1/3     Vl 100 CP
fe80::201:e8ff:fe17:5cae
                    1439        00:01:e8:17:5c:ae   STALE    Gi 1/5     Vl 1000 CP
fe80::201:e8ff:fe17:5cae
                    1439        00:01:e8:17:5c:ae   STALE    Gi 1/7     Vl 2000 CP
Force10#
```

Router Advertisement Daemon

The Router Advertisement Daemon (RAD) commands for FTOS IPv6 include:

- ipv6 nd managed-config-flag on page 1361
- ipv6 nd max-ra-interval on page 1361
- ipv6 nd other-config-flag on page 1362
- ipv6 nd prefix on page 1362
- ipv6 nd ra-lifetime on page 1363
- ipv6 nd reachable-time on page 1363
- ipv6 nd suppress-ra on page 1364

ipv6 nd managed-config-flag

C-Series	No
E-Series	✓

Set the managed address configuration flag in the IPv6 router advertisement.

Syntax **ipv6 nd managed-config-flag**

To clear the flag from the IPv6 router advertisements, use the **no ipv6 nd managed-config-flag** command.

Defaults No default behavior or values

Command Modes CONFIGURATION (conf-if-)

ipv6 nd max-ra-interval

C-Series	No
E-Series	✓

Configure the intervals between the IPv6 router advertisement (RA) transmissions on an interface.

Syntax **ipv6 nd max-ra-interval** {*interval*} **min-ra-interval** {*interval*}

To restore the default interval, use the **no ipv6 nd max-ra-interval** command.

Parameters

max-ra-interval {*interval*}	Enter the keyword **max-ra-interval** followed by the interval in seconds. Range: 4 to 1800 seconds
min-ra-interval {*interval*}	Enter the keyword **min-ra-interval** followed by the interval in seconds. Range: 3 to 1350 seconds

Defaults Not configured

Command Modes CONFIGURATION (conf-if-)

ipv6 nd other-config-flag

C-Series	No
E-Series	✓

Set the other statefull configuration flag in the IPv6 router advertisement.

Syntax **ipv6 nd other-config-flag**

To clear the flag from the IPv6 router advertisements, use the **no ipv6 nd other-config-flag** command.

Defaults Not configured

Command Modes CONFIGURATION (conf-if-)

ipv6 nd prefix

C-Series	No
E-Series	✓

Configure how IPv6 prefixes are advertised in the IPv6 router advertisements.

Syntax **ipv6 nd prefix** {*ipv6-address prefix-length* | **default**} [**no-advertise** {**valid-lifetime** *seconds* | **preferred-lifetime** *seconds*}] | [**no-autoconfig** | **no-rtr-address** | **off-link**]

To prevent a prefix (or prefixes) from being advertised, use the **no ipv6 nd prefix** {*ipv6-address prefix-length* | **default**} [**no-advertise** {**valid-lifetime** *seconds* | **preferred-lifetime** *seconds*}] | [**no-autoconfig** | **no-rtr-address** | **off-link**] command.

Parameters

ipv6-address prefix-length	Enter the IPv6 address in the **x:x:x:x::x** format followed by the prefix length in the **/x** format. Range: /0 to /128 The **::** notation specifies successive hexadecimal fields of zeros
default	(OPTIONAL) Enter the keyword **default** to specify the prefix default parameters.
no-advertise {**valid-lifetime** *seconds* | **preferred-lifetime** *seconds*}	(OPTIONAL) Enter the keyword **no-advertise** to not advertise prefixes followed by either **valid-lifetime** seconds or the **preferred-lifetime** seconds. Range: 0 to 4294967295
no-autoconfig	(OPTIONAL) Enter the keyword **no-autoconfig** to not use prefixes for auto configuration.

no-rtr-address	(OPTIONAL) Enter the keyword **no-rtr-address** to not send full router addresses in prefix advertisement.
off-link	(OPTIONAL) Enter the keyword **off-link** to not use prefixes for onlink determination.

Defaults Not configured

Command Modes CONFIGURATION (conf-if-)

ipv6 nd ra-lifetime

C-Series	No
E-Series	✓

Configure the router lifetime value in the IPv6 router advertisements on an interface.

Syntax **ipv6 nd ra-lifetime** {*seconds*}

To restore the default values, use the **no pv6 nd ra-lifetime** command.

Parameters

seconds	Enter the lifetime value in seconds. Range: 0 to 4294967295

Defaults Not configured

Command Modes CONFIGURATION (conf-if-)

ipv6 nd reachable-time

C-Series	No
E-Series	✓

Configure the amount of time that a remote IPv6 node is considered available after a reachability confirmation event has occurred.

Syntax **ipv6 nd reachable-time** {*milliseconds*}

To restore the default time, use the **no ipv6 nd reachable-time** command.

Parameters		
	milliseconds	Enter the leachability time in milliseconds. Range: 0 to 3600000

Defaults Not configured

Command Modes CONFIGURATION (conf-if-)

ipv6 nd suppress-ra

C-Series	**No**
E-Series	✓

Suppress the IPv6 router advertisement transmissions on an interface.

Syntax **ipv6 nd suppress-ra**

To enable the sending of IPv6 router advertisement transmissions on an interface, use the **no ipv6 nd suppress-ra** command.

Defaults Not configured

Command Modes CONFIGURATION (conf-if-)

Chapter 51 Service Agent

Platform Specific Feature: Service Agent is supported on E-Series only.

The Force10 Service Agent (FTSA), commonly called a call-home service, resides on the switch and collects information from the chassis manager, constructs email messages, and sends these messages to Force10 Technical Support and/or other designated servers (if configured).

The FTSA commands are listed alphabetically in this chapter for easy access:

- admin-email on page 1366
- call-home on page 1366
- debug call-home on page 1367
- domain-name on page 1368
- enable on page 1369
- enable-all on page 1369
- encrypt (TeraScale only) on page 1370
- frequency on page 1371
- keyadd (TeraScale only) on page 1371
- recipient on page 1372
- server on page 1373
- show configuration on page 1374
- show debugging on page 1374
- show keys (TeraScale only) on page 1375
- smtp on page 1375

For the sequence in which you would use the FTSA commands, see the FTSA chapter in the *FTOS Configuration Guide*.

admin-email

C-Series	No
E-Series	✓

Enter the Administrator's email address.

Syntax **admin-email** *email address*

To remove the Administrator's email address, use the **no admin-email** command.

Parameters

email address	You have two choices: • Enter the administrator's full email address, for example, *admin@domain_name.com*. • Enter just the username component, for example, *admin*.

Defaults No default behavior or values

Command Modes CONFIGURATION (conf-callhome)

Command History

Version 6.3.1.0	Introduced

Usage Information The domain name part of the email address can be specified here or by using the command **domain-name**. In either case, if you specify a domain name by using the **domain-name** command, that name will be used for the email address instead of a domain name that you might enter here.

When FTSA is unable to send a message to an email address specified by the **recipient** command (unreachable destination), FTSA forwards the message to the Administrator.

Related Commands

domain-name	Specify the domain name to be used for the Administrator's email address.
server	Configure a recipient.

call-home

C-Series	No
E-Series	✓

This command has two functions:

- Start FTSA.
- Enter the CONFIGURATION (conf-callhome) mode.

Syntax **call-home**

To stop FTSA, use the **no call-home** command. Stopping FTSA removes all FTSA configuration from the running configuration.

Defaults No default behavior or values

Command Modes CONFIGURATION (conf-callhome)

Command History

Version 6.3.1.0	Introduced

Example

```
Force10(conf)#call-home
Apr 28 15:32:21: %RPM1-P:CP %CALL-HOME-3-CALLHOME: Call-home service started
Force10(conf-callhome)#
```

Figure 1 call-home Command Example

Usage Information If executing the **call-home** command starts FTSA (this only happens if FTSA is not already started), FTOS returns a verification message (see Figure 1), and FTSA generates an email message to the default recipient, ftsa@force10networks.com.

If FTSA is already started, executing the **call-home** command simply puts the user in CONFIGURATION (conf-callhome) mode.

If FTSA is running and the **no call-home** command is executed, FTSA sends an alert email message to all designated recipients, then stops. The user is returned to CONFIGURATION mode, and FTOS removes the current FTSA configuration from the running configuration.

Related Commands

smtp	Identify the local SMTP (Simple Mail Transfer Protocol) server from which FTSA email messages will be forwarded.
admin-email	Enter the Administrator's email address.

debug call-home

C-Series	**No**
E-Series	✓

Monitor FTSA email messages through the CLI.

Syntax **debug call-home**

To turn message monitoring off, use the **no debug call-home** command.

Defaults **no debug call-home**

Command Modes EXEC

EXEC Privilege

Command History

Version 6.3.1.0	Introduced

domain-name

C-Series	**No**
E-Series	✓

Specify the domain name for the Administrator's email address.

Syntax **domain-name** *domain_name*

To remove the domain name, use the **no domain-name** command.

Parameters

domain name	Enter the keyword **domain-name** followed by the complete domain name of the Administrator's email address, for example, *domain_name.com.*

Defaults The domain name specified in the **admin-email** command

Command Modes CONFIGURATION (conf-callhome)

Command History

Version 6.3.1.0	Introduced

Usage Information If you use this command to specify a domain name, that domain name is used instead of any domain name that you might have specified using the **admin-email** command.

Related Commands

admin-email	Enter the Administrator's email address.

enable

C-Series	No
E-Series	✓

Enable the sending of FTSA email messages to the selected recipient.

Syntax **enable**

To disable (end) the sending of FTSA email messages to the selected recipient, use the **no enable** command.

Defaults **no enable**

Command Modes CONFIGURATION Server (conf-callhome-*server_name*)

Command History

Version 6.3.1.0	Introduced

Usage Information If you leave the selected recipient in the default condition of disabled (no FTSA email messages to the selected recipient), you can either come back to this command later, or you can use the **enable-all** command. If you use the **enable-all** command, you can then disable email messages to the recipient with the **no enable** command at the server-specific prompt.

FTSA sends an email notification to the selected recipient whenever the enable status changes.

Note: Execute the **enable** command only *after* the **SMTP** and **admin-email** commands are executed.

Related Commands

admin-email	Specify the Administrator's email address.
smtp	Configure the SMTP server detail.

enable-all

C-Series	No
E-Series	✓

Enable (start) the sending of FTSA email messages to all designated recipients.

Syntax **enable-all**

To disable (end) the sending of FTSA email messages to all designated recipients, use the **no enable** command.

Defaults

no enable-all

Command Modes

CONFIGURATION (conf-callhome)

Command History

Version 6.3.1.0	Introduced

Usage Information

FTSA sends an email notification to all designated recipients whenever the enable-all status changes.

Note: Execute the **enable-all** command only *after* the **SMTP** and **admin-email** commands are executed.

Related Commands

admin-email	Specify the Administrator's email address.
smtp	Identify the SMTP server.
server	Configure each recipient.

encrypt (TeraScale only)

C-Series	No
E-Series	✓

Specify email encryption for this server.

Syntax

encrypt

To remove email encryption for this server, use the **no encrypt** command.

Defaults

no encrypt

Command Modes

CONFIGURATION Server (conf-callhome-*server_name*)

Command History

Version 6.3.1.0	Introduced

Usage Information

Encryption is supported through PGP (Pretty Good Privacy). Encryption cannot be enabled without a public key for the server.

Note: Execute the **encrypt** command only *after* the **keyadd** command is executed.

Related Commands		
	keyadd (TeraScale only)	Add a public key to the server.
	server	Configure each recipient.

frequency

C-Series	No
E-Series	✓

Select the interval (frequency) with which email messages are sent to all designated recipients.

Syntax **frequency** *minutes*

To return to the default frequency, use the **no frequency** command.

Parameters

minutes	Enter the time interval, in minutes, that you want between FTSA status emails. Range: 2 to 10080 minutes Default: 1440 minutes (24 hours)

Defaults 1440 minutes (24 hours)

Command Modes CONFIGURATION (conf-callhome)

Command History

Version 6.3.1.0	Introduced

Usage Information The frequency is immediately set once the **frequency** command is executed. For example, if you set the frequency to 120 minutes, the 120 minutes begins as soon as the command is executed. In this example, email messages will be sent to all designated recipients exactly two hours after executing the command.

keyadd (TeraScale only)

C-Series	No
E-Series	✓

Add the server public key for encryption.

Syntax **keyadd** *public key*

To remove the public key, use the **no keyadd** *public key* command.

Parameters

public key	Enter the filename of the public key (must be PGP compatible) created for the selected server.

Defaults No default behavior or values

Command Modes CONFIGURATION Server (conf-callhome-*server_name*)

Command History

Version 6.3.1.0	Introduced

Usage Information The Force10 server associated with the default Force10 Support recipient has a public key that is shipped as part of FTOS, so you do not need to enter the key's filename for that server. However, if the Force10 public key is changed, a notification will be made to download the new key from the Force10 website, and to replace the old key with that new key. Also, for other servers, you would need to use this command to enter their key filenames.

Note: Execute the **encrypt** command *after* the **keyadd** command to ensure email encryption.

Related Commands

encrypt (TeraScale only)	Enable email encryption.
server	Configure recipients.

recipient

C-Series	**No**
E-Series	✓

Enter the email address of the recipient associated with the selected server.

Syntax **recipient** *email address*

To remove the recipient, use the **no recipient** *email address* command.

Parameters

email address	Enter the recipient's full email address. For example, *name@domain_name.com*.

Defaults ftsa@force10networks.com (associated with the Force10 server only)

Command Modes CONFIGURATION Server (conf-callhome-*server_name*)

Command History

Version 6.3.1.0	Introduced

Usage Information After using the **server** command to create a server name, you are placed at that server-specific prompt, where you can use this command to enter the email address of the recipient associated with that server name.

server

C-Series	No
E-Series	✓

Use this command to create a server name to be associated with a particular recipient.

Syntax

server *name*

To remove a server and the associated recipient, use the **no server** *name* command.

Parameters

name	Enter the name of the server in alphanumeric format, up to 25 characters long.

Defaults

Force10

Command Modes

CONFIGURATION Server (conf-callhome)

Command History

Version 6.3.1.0	Introduced

Example

```
Force10(conf-callhome)#
Force10(conf-callhome)#server freedom_bird
Force10(conf-callhome-freedom_bird)#?
```

Related Commands

enable	Enable FTSA (call home) email for the selected recipient.
recipient	Enter the recipient's email address.

Usage Information

The Force10 server name is configured for FTSA messages to be sent by default to Force10 Support at ftsa@force10networks.com. If you want to change that address, enter the command **server Force10**. You will be placed at that server-specific prompt (conf-callhome-Force10), where you would then use the **recipient** command to enter a new address.

In addition to modifying the Force10 server recipient, you can identify up to four more server names and associated recipients.

If you want to use encryption for a particular recipient's email messages, the server name must match the server name that is in the encryption file that the recipient will use to decrypt the messages. Use the **keyadd** command to designate the encryption file.

show configuration

C-Series	No
E-Series	✓

Display the FTSA (call-home) configuration.

Syntax **show configuration**

Defaults No default behavior or values

Command Modes CONFIGURATION (conf-callhome)

Command History

Version 6.3.1.0	Introduced

Example

```
Force10(conf-callhome)#show configuration
!
call-home
   admin-email traza
   domain-name force10networks.com
   smtp server-address 10.0.2.6
   no enable-all
   server Force10
     recipient ftsa@force10networks.com
     keyadd Force10DefaultPublicKey
     no encrypt
     enable
Force10(conf-callhome)#
```

show debugging

C-Series	No
E-Series	✓

Display the status of FTSA (call-home) debugging.

Syntax **show debugging**

Defaults No default behavior or values

Command Modes CONFIGURATION (conf-callhome)

Command History

Version 6.3.1.0	Introduced

Example

```
Force10(conf-callhome)#show debugging

CALLHOME:
    Callhome service debugging is on

Force10(conf-callhome)#
```

show keys (TeraScale only)

C-Series	No
E-Series	✓

Display the email encryption (PGP) keys.

Syntax **show keys**

Defaults No default behavior or values

Command Modes CONFIGURATION (conf-callhome)

Command History

Version 6.3.1.0	Introduced

Example

```
Force10(conf-callhome)#show keys

Type Bits KeyID      Created    Expires    Algorithm       Use

sec+  768 0x64CE09D9 2005-06-27 ---------- RSA             Sign & Encrypt
uid  E000000003209
pub  1024 0xA8E48C2F 2004-12-08 ---------- DSS             Sign & Encrypt
sub  1024 0xD832BB91 2004-12-08 ---------- Diffie-Hellman
uid  Force10

2 matching keys found
Force10(conf-callhome)#
```

smtp

C-Series	No
E-Series	✓

Identify the local SMTP (Simple Mail Transfer Protocol) server from which FTSA email messages will be forwarded.

Syntax **smtp server-address** *server-address* [**smtp-port** *port number*]

To remove the SMTP address, use the **no smtp server-address** command. This action will disable email messaging until you enter a new SMTP server address.

Parameters

server-address *server address*	Enter the keyword **server-address** followed by the SMTP server address, such as smtp.yourco.com.
smtp-port *port number*	Optionally, enter the keyword **smtp-port** followed by the SMTP port number. Range: 0 to 65535 Default: 25

Defaults

smtp-port = 25

Command Modes

CONFIGURATION (conf-callhome)

Command History

Version 6.3.1.0	Introduced

Usage Information

The chassis only plays the part of an SMTP client to send email messages to the SMTP server designated here. This SMTP server is required in order to receive the email messages and forward them to local and remote designated recipients. The default port number on an SMTP server is 25. If a host name is given (instead of an IP address), DNS should be enabled to resolve the host name.

Related Commands

admin-email	Specify the Administrator's email address.
enable	Enable FTSA email messages for the selected recipient.
enable-all	Enable FTSA email messages for all designated recipients.

Chapter 52 Power Over Ethernet

C-Series	✓
E-Series	NO

Platform Specific Feature: Power over Ethernet is supported on the C-Series only.

The following commands configure and monitor Power over Ethernet (PoE)as described by IEEE 802.3af.

- power inline on page 1377
- show hardware linecard poe-status on page 1378
- show power detail on page 1379
- show power inline on page 1380
- show power supply on page 1380

power inline

C-Series	✓
E-Series	No

Enables power to be supplied to a device connected to a port.

Syntax **power inline** {**auto** [**max milli-watts**] | **never** | **static** [**max milli-watts**]}

Parameters

auto	Enter the keyword **auto** to allow the port to determine how much power the connected Class 0,1, 2, 3, or 4 device requires, and supply it (up to 15.4 Watts).
max milli-watts	(OPTIONAL) Enter the keyword **max milli-watts** to fix the maximum amount of power that a port can provide.
never	Enter the keyword **never** to disable power to a port.
static	Enter the keyword **static** to supply the maximum amount of power (15.4 Watts) to a connected device.

Defaults Never—that is power is disabled to the port

Command Modes INTERFACE

Command History

Version 7.5.1.0	Introduced

Usage Information Ports configured with **power inline auto** have a lower priority than those configured with **power inline static**.

show hardware linecard poe-status

C-Series	✓
E-Series	No

Display the status of the 4 PoE controllers and the entire registers associated with each controllers.

Syntax **show hardware linecard** *number* **poe-status**

Parameters

linecard *number*	Enter the keywrod **linecard** followed by the line card slot number.

Defaults No default behavior or values

Command Modes EXEC

Command History

Version 7.5.1.0	Introduced

Example

```
Force10#show hardware linecard 7 poe-status

HW Status for POE Controller 0

The HW Status is
----------------
The Internal address is - 0x0000
The I2C address is - 0x003c
Is Master - Yes
The I2C Mode is - I2C
The mode is configured properly
The address is configured properly
The Controller and I2C is configured properly
Force10#
```

Usage Information If the command is executed on a non-POE line card, the following error message is generated:

```
Force10#sh hardware linecard 6 poe-status
% Error: POE is not supported for this card.
```

show power detail

C-Series	✓
E-Series	No

View the total power consumption and power consumption by component.

Syntax **show power detail**

Command Modes EXEC

EXEC privilege

Command History

Version 7.5.1.0	Introduced

Example

```
R1#show power detail

Catalog  Slot    Logic Power     Inline Power Inline Power
Name Id Consumed        Allocated Consumed
-------------------------------------------------------------------------
E48VB 0  150 W15.40 W3.90 W
E48VB 1 150 W 7.80 W7.80 W
RPM0 1 200 W  0.00 W0.00 W
CC-C300-FAN-  100 W  0.00 W0.00 W

Total Inline Power Available: 1200.00 W
Total Inline Power Used     :23.20 W
Total Inline Power Remaining: 1176.80 W
```

Figure 2 show power detail Command Example

Table 3 describes the information found in Figure 2.

Table 3 show power detail Command Output Field Description

Catalog Number	Displays the component's Force10 catalog number.
Slot ID	Displays the slot number in which the line card or RPM is installed.
Logic Power Consumed	Displays the power that the chassis component consumes during basic operation.
Inline Power Allocated	Displays the amount of power allocated to ports for PoE.
Inline Power Consumed	Displays the amount of power that is consumed by connected devices.

show power inline

C-Series	✓
E-Series	No

View the ports that are enabled with PoE and the amount of power each is consuming.

Syntax **show power inline**

Command Modes EXEC

EXEC privilege

Command History

Version 7.5.1.0	Introduced

Example

```
InterfaceAdminOperInline PowerInline PowerClass
AllocatedConsumed
------------------------------------------------------------
Gi1/1staticon16.173.92
```

Table 4 describes the information shown in the figure.

Table 4 show power inline Command Output Field Description

Interface	Displays the line card slot and port number.
Admin	Displays the PoE mode of the port. The mode can be either *auto* or *static*. See power inline.
Oper	Displays the operation status. The status can be either *on* or *off*.
Inline Power Allocated	Displays the amount of power allocated to the port.
Inline Power Consumed	Displays the amount of power that is consumed by the connected device.
Class	Displays the power classification of the connected device. Valid classes are 0-4.

show power supply

C-Series	✓
E-Series	No

View power supply status..

Syntax **show power supply**

Command Modes EXEC

EXEC privilege

Command History

Version 7.5.1.0	Introduced

Example

```
Power     Model
Supply  Number Type Status
-------------------------------------------------
PS0    -- -- Absent
PS1      CC-C300-PWR-ACAC  Active
PS2      CC-C300-PWR-ACAC  Fail
PS3     CC-C300-PWR-ACAC  Remote Off
PS4              -- --  Absent
PS5              -- --  Absent
PS6              -- -- Absent
```

The Table below describes the 9 possible power supply conditions.

Table 5 Power Supply Conditions

AC Fail	The PSU is unplugged.
Active	The PSU is supplying power to the chassis.
Fail	The PSU has failed.
Not Present	The PSU is not installed in the chassis.
Over Current Shutdown	The PSU has turned off due to an high input current condition.
Over Temperature Shutdown	The PSU has turned off due to an high temperature condition.
Over Temperature Warning	The temperature of the PSU is greater than the recommended maximum operating temperature.
OverCurrent Warning	The current being supplied to the PSU is greater than the recommended maximum input current.
Power Off	The PSU is present but no not on.

Chapter 53 BOOT_USER

All commands listed in this chapter are found in the BOOT_USER mode. You access this mode when you enter a control break sequence (for example, CNTL^ or CNTL~) when the E-Series is booting and the following line appears on the console:

```
Send the Break Signal to stop Operating System auto-boot...
```

In the BOOT_USER mode, you cannot use the TAB key to complete commands.

- boot change on page 1384
- boot messages on page 1385
- boot selection on page 1385
- default-gateway on page 1386
- delete on page 1386
- dir on page 1387
- enable on page 1388
- format on page 1388
- ignore enable-password on page 1388
- interface management ethernet ip address on page 1389
- interface management port config on page 1389
- reload on page 1390
- rename on page 1390
- show boot selection on page 1391
- show bootflash on page 1391
- show bootvar on page 1392
- show default-gateway on page 1393
- show interfaces management ethernet on page 1393

boot change

Change the primary, secondary or default boot image configuration.

Syntax **boot change** {**primary** | **secondary** | **default**}

Parameters

primary	Enter the keyword **primary** to configure the boot parameters used in the first attempt to boot the system.
secondary	Enter the keyword **secondary** to configure boot parameters used if the primary operating system boot selection is not available.
default	Enter the keyword **default** to configure boot parameters used if the secondary operating system boot parameter selection is not available. The default parameters always reside on the internal flash device (flash:).

Defaults Not configured.

Command Modes BOOT_USER

Usage Information After entering the **boot change** keywords and parameters, press ENTER and the software prompts you to enter the following:

- the boot device (ftp, tftp, flash, slot0),
- the image file name,
- the IP address of the server containing the image,
- the username, and password. Usernames and passwords are needed only for remote file locations, such as FTP and TFTP.

Note: When you enter a new parameter that extends beyond 80 characters, you cannot use the BACKSPACE key to correct any mistakes. If you make a mistake, you must re-enter the parameter.

Figure 6 shows the first field after you enter boot change primary. At this point, you have the choice of accepting the information already configured (press ENTER) or changing that information (press . (period) and enter new information.). After you type the information, press ENTER.

```
BOOT_USER # boot change primary

'.' = clear field;  '-' = go to previous field

boot device                    : ftp
```

Figure 6 First Field in the boot change command

Figure 7 shows the completed command.

```
BOOT_USER # boot change primary

'.' = clear field;  '-' = go to previous field

boot device                   : ftp
file name                     : tt/latestlabel
Server IP address             : 10.16.1.209
username                      : amsterdam
password                      : ******

BOOT_USER #
```

Figure 7 Completed boot change Command Example

In the runtime CLI, use the boot system command to change the boot image file and location.

To view the current Boot configuration, use the show bootvar command.

boot messages

Limit the number of messages seen during system boot-up.

Syntax **boot messages** {**disable** | **enable**}

Parameters

disable	Enter the keyword **disable** to view fewer messages during boot-up.
enable	Enter the keyword **enable** to view all messages during boot-up.

Defaults enable (that is, all messages are displayed during boot up)

Command Modes BOOT_USER

boot selection

Change the boot flash image on the internal Flash.

Syntax **boot selection** [**a** | **b**]

Parameters		
	a	Enter the keyword **a** to select the boot flash image in partition A.
	b	Enter the keyword **b** to select the boot flash image in partition B.

Defaults None.

Command Modes BOOT_USER

Usage Information To view the current boot flash image, enter the show boot selection command.

default-gateway

Assign an IP address as the default gateway for the E-Series.

Syntax **default-gateway** *ip-address*

To delete the default gateway address, enter **no default-gateway**.

Parameters		
	ip-address	Enter the IP address of the gateway router in dotted decimal format (A.B.C.D).

Defaults Not configured.

Command Modes BOOT_USER

Usage Information To view the current default gateway configured, enter the show default-gateway command.

delete

Erase a file on the internal or external Flash.

Syntax **delete** *file-url*

Parameters		
	file-url	Enter the location keywords and information: • For a file on the internal Flash, enter **flash://** followed by the filename. • For a file on the external Flash, enter **slot0://** followed by the filename.

Defaults Not configured.

Command Modes BOOT_USER

dir

View files in a directory

Syntax **dir** *file-url*

Parameters

file-url	Enter the location keywords and information: • For a file on the internal Flash, enter **flash://** followed by the filename. • For a file on the external Flash, enter **slot0://** followed by the filename.

Defaults Not configured.

Command Modes BOOT_USER

Usage Information The maximum number of files allowed on an MMC card (internal or external flash) is 100 files.

Example

```
BOOT_USER # dir flash:
Displaying files in flash:
  size          date       time       name
--------      ------     ------     --------
 8681647    MAR-21-2004  11:08:50   E1200-3.1.a3.78.bin
    4905    MAR-17-2004  18:16:34   nimule
 1182431    FEB-29-2004  22:08:14   dohuk
 8807825    MAR-30-2004  12:49:14   E1200-3.1.0.309.bin
 1182431    FEB-24-2004  22:52:00   t1
   14729    MAR-14-2004  17:55:26   erbil
 1182431    MAR-10-2004  10:57:30   vW
    6858    MAR-07-2004  09:52:58   RPM0CP1
 1182431    MAR-22-2004  12:17:34   tunis
 7819238    MAR-22-2004  12:23:14   E1200-3.1.0.316.bin
 8989646    MAR-17-2004  15:13:06   E1200-3.1.0.390.bin.dos2
   14517    MAR-30-2004  09:48:44   RPM0CPlog1
   14506    MAR-30-2004  09:49:34   RPM0CPlog2

BOOT_USER #
```

Figure 8 dir Command Example

enable

Change the privilege level.

Syntax **enable** {**user** | **admin**}

Parameters

admin	Used only by Force10 TAC personnel.
user	Used only by Force10 TAC personnel.

Defaults Not configured.

Command Modes BOOT_USER

Usage Information Only Force10 TAC staff use this command.

format

Format the internal or external Flash.

Syntax **format** *file-url*

Parameters

file-url	Enter the location keywords and information: • For a file on the internal Flash, enter **flash://** followed by the filename. • For a file on the external Flash, enter **slot0://** followed by the filename.

Defaults Not configured.

Command Modes BOOT_USER

Usage Information The maximum number of files allowed on an MMC card (internal or external flash) is 100 files.

ignore enable-password

Reload the system software without the enable password configured. This command hidden and is not listed when you enter ? or **help** in this mode.

Syntax **ignore enable-password**

Defaults Not configured.

Command Modes BOOT_USER

Usage Information Enter the reload command to re-boot the system. You will not be prompted for a password to enter the EXEC privilege mode (normally you are required to enter the enable command.)

If your console or Telnet session expires after you used the ignore enable-password command, when you re-establish the session, you are prompted for an **enable** password.

interface management ethernet ip address

Assign an IP address to the Management Ethernet interface.

Syntax **interface management ethernet ip address** *ip-address mask*

To delete the IP address, enter **no interface management ethernet ip address**.

Parameters

ip-address mask	Enter the IP address in dotted decimal format (A.B.C.D) and the mask in / prefix-length format (/x).

Defaults Not configured.

Command Modes BOOT_USER

Usage Information In the runtime CLI, use the ip address command in the INTERFACE mode to change the Management interface's IP address.

To view the current IP address configured on the Management interface, enter the show interfaces management ethernet command.

interface management port config

Configure speed, duplex and negotiation settings for the management interface.

Syntax **interface management port config** {**half-duplex** | **full-duplex** | **10m** | **100m** | **auto-negotiation** | **no auto-negotiation** | **show**}

Parameters

half-duplex	Enter the keyword **half-duplex** to set the Management interface to half-duplex mode.
full-duplex	Enter the keyword **full-duplex** to set the Management interface to full-duplex mode.
10m	Enter the keyword **10m** to set the speed on the Management interface to 10 Mb/s.
100m	Enter the keyword **100m** to set the speed of the Management interface to 100 Mb/s.
auto-negotiation	Enter the keyword **auto-negotiation** to enable negotiation on the Management interface.
no auto-negotiation	Enter the keyword **no auto-negotiation** to disable auto-negotiation on the Management interface.
show	Enter the keyword **show** to view the settings on the Management interface.

Defaults full duplex; auto-negotiation

Command Modes BOOT_USER

Usage Information This command is only available in Boot Flash version 2.0.0.21 and higher.

reload

Reload the FTOS.

Syntax **reload**

Command Modes BOOT_USER

rename

Rename a file.

Syntax **rename** *file-url*

Parameters		
	file-url	Enter the location keywords and information: • For a file on the internal Flash, enter **flash://** followed by the filename. • For a file on the external Flash, enter **slot0://** followed by the filename.

Defaults None.

Command Modes BOOT_USER

show boot selection

View current Boot Flash image selected.

Syntax **show boot selection**

Command Modes BOOT_USER

Example

```
BOOT_USER # show boot selection

ROM BOOTSTRAP SELECTOR PARMETERS:
================================
Current ROM bootstrap selection set to Bootflash partition B.

Last ROM bootstrap occurred from Bootflash partition B.

BOOT_USER #
```

Figure 9 show boot selection Command Example

show bootflash

View information on the boot flash.

Syntax **show bootflash**

Command Modes BOOT_USER

Example

```
BOOT_USER # show bootflash

GENERAL BOOTFLASH INFO
======================
Bootflash Partition A:
    Force10 Networks System Boot
    Copyright 1999-2004 Force10 Networks, Inc.
    ROM Header Version 1.0
    Engineering CP_IMG_BOOT, BSP Release 2.0.0.19, Checksum 0x39303030
    Created Mon Mar 20 10:56:53 US/Pacific 2004 by xxx on Unknown host

Bootflash Partition B:
    Force10 Networks System Boot
    Copyright 1999-2004 Force10 Networks, Inc.
    ROM Header Version 1.0
    Engineering CP_IMG_BOOT, BSP Release 2.0.0.19, Checksum 0x36313031
    Created Mon Mar 6 18:15:10 2004 by xxx on hostname

Boot Selector Partition:
    Force10 Networks System Boot
    Copyright 1999-2004 Force10 Networks, Inc.
    ROM Header Version 1.0
    Official CP_IMG_BOOT_SELECTOR, BSP Release 2.0.0.15, Checksum 0x30314348
    Created Mon Jan 21 17:15:47 US/Pacific 2004 by xxx on Unknown host

BOOT_USER #
```

Figure 10 show bootflash Command Example

show bootvar

View boot configuration information.

Syntax **show bootvar**

Command Modes BOOT_USER

Example

```
BOOT_USER # show bootvar

PRIMARY OPERATING SYSTEM BOOT PARAMETERS:
=========================================
boot device                     : ftp
file name                       : tt/latestlabel
Management Ethernet IP address : 10.16.1.181/24
Server IP address               : 10.16.1.209
username                        : amsterdam
password                        : ******

SECONDARY OPERATING SYSTEM BOOT PARAMETERS:
===========================================
boot device                     : flash
file name                       : /E1200-3.1.1.3.bin

DEFAULT OPERATING SYSTEM BOOT PARAMETERS:
=========================================
boot device                     : flash
file name                       : /E1200-3.1.1.2.bin

BOOT_USER #
```

Figure 11 show bootvar Command Example

show default-gateway

View the IP address configured for the default gateway.

Syntax **show default-gateway**

Command Mode BOOT_USER

Example

```
BOOT_USER # show default-gateway

Gateway IP address: 10.1.1.1

BOOT_USER #
```

Figure 12 show default-gateway Command Example

show interfaces management ethernet

View the IP address configured for the Management interface.

Syntax **show interfaces management ethernet**

Command Modes BOOT_USER

Example

```
BOOT_USER # show interfaces management ethernet
Management ethernet IP address: 10.16.1.181/24
BOOT_USER #
```

Figure 13 show interfaces management ethernet Command Example

Appendix A ICMP Message Types

Table 1 lists and describes the possible ICMP Message Type resulting from a ping. The first three columns list the possible symbol or type/code, for example, you would receive a ! or 03 as an echo reply from your Ping.

Table 1 ICMP Messages and their definitions

Symbol	Type	Code	Description	Query	Error
•			Timeout (no reply)		
!	0	3	echo reply	•	
U	3		destination unreachable:		
		0	network unreachable		•
		1	host unreachable		•
		2	protocol unreachable		•
		3	port unreachable		•
		4	fragmentation needed but don't fragment bit set		•
		5	source route failed		•
		6	destination network unknown		•
		7	destination host unknown		•
		8	source host isolated (obsolete)		•
		9	destination network administratively prohibited		•
		10	destination host administratively prohibited		•
		11	network unreachable for TOS		•
		12	host unreachable for TOS		•
		13	communication administratively prohibited by filtering		•
		14	host precedence violation		•
		15	precedence cutoff in effect		•
C	4	0	source quench		•
	5		redirect		•
		0	redirect for network		•
		1	redirect for host		•
		2	redirect for type-of-service and network		•
		3	redirect for type-of-service and host		•

Table 1 ICMP Messages and their definitions

Symbol	Type	Code	Description	Query	Error
	8	0	echo request	•	
	9	0	router advertisement	•	
	10	0	router solicitation	•	
&	11		time exceeded:		
		0	time-to-live equals 0 during Transit		•
		1	time-to-live equals 0 during reassembly		•
	12		parameter problem:		
		1	IP header bad (catchall error)		•
		2	required option missing		•
	13	0	timestamp request	•	
	14	0	timestamp reply	•	
	15	0	information request (obsolete)	•	
	16	0	information reply (obsolete)	•	
	17	0	address mask request	•	
	18	0	address mask reply	•	

Appendix B SNMP Traps

Table 2 lists the traps sent by FTOS. Each trap is listed by Message ID, Trap Type,Trap Option, and followed by the error message(s) associated with the trap.

Table 2 SNMP Traps and Error Messages

Message ID	Trap Type	Trap Option
COLD_START	**SNMP**	**COLDSTART**
%SNMP-5-SNMP_COLD_START: SNMP COLD_START trap sent.		
COPY_CONFIG_COMPLETE	**SNMP**	**NONE**
SNMP Copy Config Command Completed		
LINK_DOWN	**SNMP**	**LINKDOWN**
%IFA-1-PORT_LINKDN: changed interface state to down:%d		
LINK_UP	**SNMP**	**LINKUP**
%IFA-1-PORT_LINKUP: changed interface state to up:%d		
AUTHENTICATION_FAIL	**SNMP**	**AUTH**
%SNMP-3-SNMP_AUTH_FAIL: SNMP Authentication failed.Request with invalid community string.		
RMON_RISING_THRESHOLD	**SNMP**	**NONE**
%RPM0-P:CP %SNMP-4-RMON_RISING_THRESHOLD: RMON rising threshold alarm from SNMP OID <oid>		
RMON_FALLING_THRESHOLD	**SNMP**	**NONE**
%RPM0-P:CP %SNMP-4-RMON_FALLING_THRESHOLD: RMON falling threshold alarm from SNMP OID <oid>		
RMON_HC_RISHING_THRESHOLD	**SNMP**	**NONE**
%RPM0-P:CP %SNMP-4-RMON_HC_RISING_THRESHOLD: RMON high-capacity rising threshold alarm from SNMP OID <oid>		
RMON_HC_FALLING_THRESHOLD	**SNMP**	**NONE**
%RPM0-P:CP %SNMP-4-RMON_HC_FALLING_THRESHOLD: RMON high-capacity falling threshold alarm from SNMP OID <oid>		

Table 2 SNMP Traps and Error Messages (continued)

Message ID	Trap Type	Trap Option
RESV	**NONE**	**NONE**
N/A		
CHM_CARD_DOWN	**ENVMON**	**NONE**
%CHMGR-1-CARD_SHUTDOWN: %sLine card %d down - %s %CHMGR-2-CARD_DOWN: %sLine card %d down - %s		
CHM_CARD_UP	**ENVMON**	**NONE**
%CHMGR-5-LINECARDUP: %sLine card %d is up		
CHM_CARD_MISMATCH	**ENVMON**	**NONE**
%CHMGR-3-CARD_MISMATCH: Mismatch: line card %d is type %s - type %s required.		
CHM_RPM_UP	**ENVMON**	**NONE**
%RAM-6-RPM_STATE: RPM1 is in Active State %RAM-6-RPM_STATE: RPM0 is in Standby State		
CHM_RPM_DOWN	**ENVMON**	**NONE**
%CHMGR-2-RPM_DOWN: RPM 0 down - hard reset %CHMGR-2-RPM_DOWN: RPM 0 down - card removed		
CHM_RPM_PRIMARY	**ENVMON**	**NONE**
%RAM-5-COLD_FAILOVER: RPM Failover Completed %RAM-5-HOT_FAILOVER: RPM Failover Completed %RAM-5-FAST_FAILOVER: RPM Failover Completed		
CHM_SFM_ADD	**ENVMON**	**NONE**
%TSM-5-SFM_DISCOVERY: Found SFM 1		
CHM_SFM_REMOVE	**ENVMON**	**NONE**
%TSM-5-SFM_REMOVE: Removed SFM 1		
CHM_MAJ_SFM_DOWN	**ENVMON**	**NONE**
%CHMGR-0-MAJOR_SFM: Major alarm: Switch fabric down		
CHM_MAJ_SFM_DOWN_CLR	**ENVMON**	**NONE**
%CHMGR-5-MAJOR_SFM_CLR: Major alarm cleared: Switch fabric up		
CHM_MIN_SFM_DOWN	**ENVMON**	**NONE**
%CHMGR-2-MINOR_SFM: MInor alarm: No working standby SFM		

Table 2 SNMP Traps and Error Messages (continued)

Message ID	Trap Type	Trap Option
CHM_MIN_SFM_DOWN_CLR	**ENVMON**	**NONE**
%CHMGR-5-MINOR_SFM_CLR: Minor alarm cleared: Working standby SFM present		
CHM_PWRSRC_DOWN	**ENVMON**	**SUPPLY**
%CHMGR-2-PEM_PRBLM: Major alarm: problem with power entry module %s		
CHM_PWRSRC_CLR	**ENVMON**	**SUPPLY**
%CHMGR-5-PEM_OK: Major alarm cleared: power entry module %s is good		
CHM_MAJ_ALARM_PS	**ENVMON**	**SUPPLY**
%CHMGR-0-MAJOR_PS: Major alarm: insufficient power %s		
CHM_MAJ_ALARM_PS_CLR	**ENVMON**	**SUPPLY**
%CHMGR-5-MAJOR_PS_CLR: major alarm cleared: sufficient power		
CHM_MIN_ALARM_PS	**ENVMON**	**SUPPLY**
%CHMGR-1-MINOR_PS: Minor alarm: power supply non-redundant		
CHM_MIN_ALARM_PS_CLR	**ENVMON**	**SUPPLY**
%CHMGR-5-MINOR_PS_CLR: Minor alarm cleared: power supply redundant		
CHM_MIN_ALRM_TEMP	**ENVMON**	**TEMP**
%CHMGR-2-MINOR_TEMP: Minor alarm: chassis temperature		
CHM_MIN_ALRM_TEMP_CLR	**ENVMON**	**TEMP**
%CHMRG-5-MINOR_TEMP_CLR: Minor alarm cleared: chassis temperature normal (%s %d temperature is within threshold of %dC)		
CHM_MAJ_ALRM_TEMP	**ENVMON**	**TEMP**
%CHMGR-2-MAJOR_TEMP: Major alarm: chassis temperature high (%s temperature reaches or exceeds threshold of %dC)		
CHM_MAJ_ALRM_TEMP_CLR	**ENVMON**	**TEMP**
%CHMGR-2-MAJOR_TEMP_CLR: Major alarm cleared: chassis temperature lower (%s %d temperature is within threshold of %dC)		
CHM_FANTRAY_BAD	**ENVMON**	**FAN**
For E1200: %CHMGR-2-FAN_TRAY_BAD: Major alarm: fantray %d is missing or down %CHMGR-2-ALL_FAN_BAD: Major alarm: all fans in fan tray %d are down. For E600 and E300: %CHMGR-2-FANTRAYBAD: Major alarm: fan tray is missing %CHMGR-2-FANSBAD: Major alarm: most or all fans in fan tray are down		

Table 2 SNMP Traps and Error Messages (continued)

Message ID	Trap Type	Trap Option
CHM_FANTRAY_BAD_CLR	**ENVMON**	**FAN**
For the E1200: %CHMGR-5-FAN_TRAY_OK: Major alarm cleared: fan tray %d present For the E600 and E300: %CHMGR-5-FANTRAYOK: Major alarm cleared: fan tray present		
CHM_MIN_FANBAD	**ENVMON**	**FAN**
For the E1200: %CHMGR-2-FAN_BAD: Minor alarm: some fans in fan tray %d are down For the E600 and E300: %CHMGR- 2-1FANBAD: Minor alarm: fan in fan tray is down		
CHM_MIN_FANBAD_CLR	**ENVMON**	**FAN**
For E1200: %CHMGR-2-FAN_OK: Minor alarm cleared: all fans in fan tray %d are good For E600 and E300: %CHMGR-5-FANOK: Minor alarm cleared: all fans in fan tray are good		
TME_TASK_SUSPEND	**ENVMON**	**NONE**
%TME-2-TASK SUSPENDED: SUSPENDED - svce:%d - inst:%d - task:%s		
TME_TASK_TERM	**ENVMON**	**NONE**
%TME-2-ABNORMAL_TASK_TERMINATION: CRASH - task:%s %s		
CHM_CPU_THRESHOLD	**ENVMON**	**NONE**
%CHMGR-5-CPU_THRESHOLD: Cpu %s usage above threshold. Cpu5SecUsage (%d)		
CHM_CPU_THRESHOLD_CLR	**ENVMON**	**NONE**
%CHMGR-5-CPU_THRESHOLD_CLR: Cpu %s usage drops below threshold. Cpu5SecUsage (%d)		
CHM_MEM_THRESHOLD	**ENVMON**	**NONE**
%CHMGR-5-MEM_THRESHOLD: Memory %s usage above threshold. MemUsage (%d)		
CHM_MEM_THRESHOLD_CLR	**ENVMON**	**NONE**
%CHMGR-5-MEM_THRESHOLD_CLR: Memory %s usage drops below threshold. MemUsage (%d)		
MACMGR_STN_MOVE	**ENVMON**	**NONE**
%MACMGR-5-DETECT_STN_MOVE: Station Move threshold exceeded for Mac %s in vlan %d		
VRRP_BADAUTH	**PROTO**	**NONE**
%RPM1-P:RP2 %VRRP-3-VRRP_BAD_AUTH: vrid-1 on Gi 11/12 rcvd pkt with authentication type mismatch. %RPM1-P:RP2 %VRRP-3-VRRP_BAD_AUTH: vrid-1 on Gi 11/12 rcvd pkt with authentication failure.		
VRRP_GO_MASTER	**PROTO**	**NONE**
%VRRP-6-VRRP_MASTER: vrid-%d on %s entering MASTER		

Table 2 SNMP Traps and Error Messages (continued)

Message ID	Trap Type	Trap Option
BGP4_ESTABLISHED	**PROTO**	**NONE**
%TRAP-5-PEER_ESTABLISHED: Neighbor %a, state %s		
BGP4_BACKW_XSITION	**PROTO**	**NONE**
%TRAP-5-BACKWARD_STATE_TRANS: Neighbor %a, state %s		

Index

A

aaa authentication login 397
ABR 861
Access Control Lists
  see ACL 691
access control lists. See ACL.
access-class 644
access-group 399
ACCESS-LIST Mode 75
ACL 74, 75
  deny 692
  deny tcp 695
  deny udp 697
  Important Points to Remember 691
  ipv6 access-group 699
  permit 701
  permit tcp 703
  permit udp 705
  remark 707
  seq 709
  show ipv6 accounting access-list 712
ACL VLAN Group
  acl-vlan-group 307
  description 308
  Ip access-group 309
  member vlan 309
  show acl-vlan-grou 310
  show config 311
  show running config acl-vlan-group 312
Address Resolution Protocol, See ARP.
admin-email 1366
Administrator's email address 1366, 1367
advertise 943
advertise-interval 785
aggregate-address 1024, 1129
ais-shut 528
alarm-report 528
Area Border Router. See ABR.
area default-cost 861
area nssa 861
area range 862
area stub 862
area virtual-link 863
area-password 944, 988
arp 720
arp timeout 721
AS 859, 1021, 1127
ASBR 890
audience 63
authentication-type 786
auto negotiation 480
auto-cost 864
Autonomous System. See AS.
auto-summary 840

B

bandwidth-percentage 1228
BGP 1021, 1127
  passive peering 1063, 1169
  soft reconfiguration 1037, 1142, 1143, 1144
bgp always-compare-med 1025, 1131
bgp bestpath as-path ignore 1025, 1131
bgp bestpath med confed 1026, 1132
bgp client-to-client reflection 1027, 1133
bgp cluster-id 1027, 1036, 1037, 1133, 1141
bgp confederation identifier 1028, 1134
bgp confederation peers 1029, 1135
bgp dampening 1029, 1101, 1136, 1192
bgp default local-preference 1030, 1137
bgp fast-external-fallover 1032, 1137
bgp graceful-restart 1032, 1138
bgp log-neighbor-changes 1033, 1139
bgp non-deterministic-med 1034, 1139
bgp router-id 1035, 1140
boot change 1384
boot messages 1385
boot selection 1385
BPDU 799, 812, 818, 827
Bridge Protocol Data Units, *See BPDU.*
Bridge Protocol Data Units. *See BPDU.*
bridge-priority 797
Broadcast/Unknown Unicast Rate Limiting 447
Bulk Configuration
  see interface range 468
Bulk Configuration Macro
  see interface range macro 470

C

calendar set 376
call-home 1367
call-home service 1365
CAM Ipv4flow 295
CAM Profiling
  Important Points to Remember 272, 294
channel-member 500
chassis chassis-mode 110

clear arp-cache 721
clear config 944, 989
clear counters 456
clear counters ip access-group 645
clear counters ip trace-group 434
clear counters mac access-group 657
clear counters vrrp 787
clear host 722
clear ip bgp 1037
clear ip bgp * (asterisk) 1037, 1141
clear ip bgp as-number 1143
clear ip bgp dampening 1039
clear ip bgp flap-statistics 1039, 1103, 1194
clear ip bgp ipv4 multicast 1102, 1192
clear ip bgp ipv6 dampening 1145
clear ip bgp ipv6 flap-statistics 1146
clear ip bgp ipv6-address 1144
clear ip bgp peer-group 1103, 1145, 1194
clear ip fib linecard 723
clear ip igmp groups 1285
clear ip mroute 1278, 1300
clear ip ospf 865
clear ip pim rp-mapping 1318
clear ip pim tib 1318
clear ip prefix-list 659
clear ip rip 840
clear ip route 723
clear ipv6 neighbor 1357
clear isis 945, 990
clear logging 339
clear mac-address-table dynamic 556
clear tcp statistics 724
CLI
  case sensitivity 70
  partial keywords 70
CLI Modes
  AS-PATH ACL 76
  CONFIGURATION 73
  EXEC 72
  EXEC Privilege 72
  INTERFACE 73
  IP ACCESS LIST 75
  IP COMMUNITY LIST 76
  LINE 74
  MAC ACCESS LIST 74
  MULTIPLE SPANNING TREE 77
  PREFIX-LIST 75
  REDIRECT-LIST 76
  ROUTE-MAP 75
  ROUTER BGP 79
  ROUTER ISIS 79
  ROUTER OSPF 78
  ROUTER RIP 78
  SPANNING TREE 77
  TRACE-LIST 74
clns host 945, 990
clock read-calendar 377
clock set 377
clock source 530
clock summer-time date 378
clock summer-time recurring 379
clock timezone 380
clock update-calendar 381
Command Modes 72
Configuration
  multiple users 68
CONFIGURATION mode 73
control break sequence 1383
copy (Streamline Upgrade) 87
copy running-config startup-config duplicate 88
Core Dump Files
  naming conventions 92, 224
Core-Dump 91
CPU Traffic Statistics 112, 135, 207

D

debug arp 724
debug callhome 1367
debug ip bgp 1040
debug ip bgp (ipv6) 1147
debug ip bgp events 1042, 1148
debug ip bgp events (ipv6) 1148
debug ip bgp ipv6 dampening 1148
debug ip bgp keepalives 1042, 1149
debug ip bgp modify 1043, 1150
debug ip bgp updates 1044, 1104, 1150, 1195
debug ip icmp 726
debug ip igmp 1285, 1293
debug ip ospf 866
debug ip packet 727
debug ip pim 1318, 1334
debug ip rip 841
debug isis 946, 991
debug isis adj-packets 946, 992
debug isis local-updates 947, 949, 992, 994
debug isis snp-packets 948, 993
debug isis spf-triggers 948, 994
debug ntp 381
debug ppp 530
debug radius 408
debug spanning-tree 798
debug spanning-tree mstp 825
debug tacacs+ 412
debug vrrp 787
default logging buffered 340, 342
default logging console 340
default logging monitor 341

default logging trap 341, 348
default vlan-id 570
default-gateway 1386
default-information originate
BGP 1045
IS-IS 949, 995
OSPF 867
RIP 841
default-metric
BGP 1045, 1151
OSPF 868
RIP 842
delay triggers line 531
delete
BOOT_USER mode 1386
EXEC privilege mode 88
Denial of Service 434
deny
AS-Path Access list 682
Community Access list 686
IP ACL (extended) 613
IP ACL (standard) 606
MAC ACL (extended) 651
MAC ACL (standard) 648
Prefix List 659
Trace list 435
deny arp 615
deny ether-type 616
deny tcp
IP ACL 621
Trace list 436
deny udp
IP ACL 623
Trace list 437
description
INTERFACE 460
VRRP 788
DHCP 735
UDP ports 735
DHCP-Relay 735
dir
BOOT_USER mode 1387
EXEC privilege mode 89
disable
FVRP 586
Spanning Tree Protocol 798, 805
VRRP 788
display parameter 71
distance
IS-IS 950
OSPF 869
RIP 843
distance bgp 1045, 1152
distance ospf 869
distribute-list in
IS-IS 951
OSPF 870
RIP 843
distribute-list out
IS-IS 952
OSPF 871
RIP 844
distribute-list redistributed-override in 953
IS-IS 953
DNS
commands 732, 733, 738
do 113
Document conventions 63
domain-name 1368
domain-password 953, 996
DOS 434
dot1p-priority 1219
download alt-boot-image 89
down-when-looped 532
DSCP Mapping Table 1262
duplex 460

E

egress ACLs 645
email addresses
FTSA Administrator 1366, 1367
FTSA recipient, ftsa@force10networks.com 1372
email encryption keys 1375
email messages from the switch 1365
enable 114, 1369, 1388
enable inverse mask
OSPF 871
enable password 399, 401
enable restricted 400
enable-all 1369
encap 532
encrypt 1370
encryption keys, email 1375
end 116
except parameter 71
EXEC mode 72
exec-banner 117
exec-timeout 117
exit 118
external flash
number of files supported 86

F

Far-End Failure Detection (FEFD) 779
File naming convention
application core-dump 92, 225
files

number supported on external flash 86
find parameter 72
Force10 Service Agent (FTSA) 1365
format 1388
forward-delay 799
framing 533
frequency 1371
ftp-server enable 118
ftp-server topdir 119
ftp-server username 120
FTSA commands 1370
admin-email 1366
call-home 1367
debug callhome 1367
domain-name 1368
enable 1369
enable-all 1369
frequency 1371
keyadd 1371
recipient 1372
server 1373
show configuration 1374
show debugging 1374
show keys 1375
smtp server-address 1375
FVRP
Important Things to Remember 585
fvrp access 586
fvrp aware 587
fvrp control-vlan 588
fvrp core 588
fvrp core region 589
fvrp disable 589
fvrp domain 590
fvrp group 591
fvrp hello-time 591
fvrp preempt 592
fvrp priority
for a VLAN 592
for an interface 593
fvrp uplink 594

G

graceful-restart
OSPF 872, 873
graceful-restart grace-period
OSPF 872
graceful-restart helper-reject
OSPF 873
graceful-restart mode
OSPF 873
graceful-restart role
OSPF 873
grep parameter 72

H

hello padding 954, 996
hello-time 799
hitless upgrade 369
hold-time 789
hostname 120
hostname dynamic 955, 997

I

ICMP 741
IETF RFCs
1058 839
1142 941
2328 859
2453 839
2763 941
2966 941, 943, 988
3373 941
IGMP Snooping 1292
Important Things to Remember for IGMP Querier 1293
Important Things to Remember for IGMP Snooping 1292
IGMP Snooping Commands 1292
ignore enable-password 1388
ignore-lsp-errors 955, 998
ingress ACLs 645
interface
interface command 464
interface loopback 464
interface management ethernet ip address 1389
interface management port config 1389
interface ManagementEthernet 465
interface null 466
interface port-channel 467
interface range 468
interface rate-interval 472
interface sonet 534
Interface vlan 473
Interior Gateway Protocol 859
Internet Control Message Protocol. See ICMP.
Inter-packet gap 474
ip access-group 645
ip access-list extended 625
ip access-list standard 607
ip address 731
ip as-path access-list 682
ip community-list 687
ip default-network 733
ip directed-broadcast 732
ip domain-list 732

ip domain-name 734
ip fib download-igp-only 734
ip ftp password 121
ip ftp source-interface 121
ip ftp username 122
ip helper-address 735
ip helper-address hop-count disable 735
ip igmp immediate-leave 1286
ip igmp last-member-query-interval 1286
ip igmp querier-timeout 1287
ip igmp query-interval 1287
ip igmp query-max-resp-time 1288
ip igmp static-group 1288
ip max-frag-count 736
ip mroute 1278
ip multicast-lag-hashing 1279
ip multicast-routing 1279, 1280
ip name-server 738
ip ospf auth-change-wait-time
OSPF 874
ip ospf authentication-key 874
ip ospf cost 875
ip ospf dead-interval 875
ip ospf hello-interval 876
ip ospf message-digest-key 876
ip ospf mtu-ignore 877
ip ospf network 877
ip ospf priority 878
ip ospf retransmit-interval 879
ip ospf transmit-delay 879
ip pim dr-priority 1320, 1336
ip pim query-interval 1321, 1336
ip pim rp-address 1321
ip poison-reverse 845
ip prefix-list 660
ip proxy-arp 739
ip radius source-interface 408
ip redirect-group 770
ip redirect-list 771
ip redirects 739
ip rip receive version 845
ip rip send version 846
ip route 740
ip router isis 956
ip scp topdir 424
ip source-route 741
ip split-horizon 847
ip ssh server enable 429
ip tacacs source-interface 413
ip telnet server enable 123
ip telnet source-interface 123
ip tftp source-interface 124
ip trace-group 438
ip trace-list 439
ip unreachables 741
ipg 474
ipv6 nd managed-config-flag 1361
ipv6 nd max-ra-interval 1361
ipv6 nd other-config-flag 1362
ipv6 nd prefix 1362
ipv6 nd ra-lifetime 1363
ipv6 nd reachable-time 1363
ipv6 nd suppress-ra 1364
ipv6 neighbor 1358
IPv6 PIM debugging, set 1334
IPv6 PIM Router-Query messages, set frequency 1336
IPv6 PIM sparse mode, enable 1338
IPv6 Protocol Independent Multicast 1333
IS-IS
isis hello padding 959, 1002
isis circuit-type 956, 998
isis csnp 957, 999
isis hello-interval 958, 1000
isis hello-multiplier 959, 1001
isis metric 960, 1003
isis network point-to-point 961, 1003
isis password 961, 1004
isis priority 962, 1005
ISO/IEC 10589 941
is-type 963, 1006

K

keepalive 475, 534
kernel core-dump 92, 225
keyadd 1371

L

LACP
clear lacp counters 521
debug lacp 522
lacp port-priority 523
port-channel mode 524
port-channel-protocol lacp 525
show lacp 525
line 125
linecard 126
Link State Advertisements. See LSA.
load-balance 744
log-adjacency-changes 880, 963, 1006
logging 341
logging buffered 342
logging console 343
logging facility 343
logging history 344
logging history size 345
logging monitor 346
logging on 346

logging source-interface 347
logging synchronous 347
logging trap 348
login authentication 402
loopback 535
lp pim bsr-border 1319
LSA 862, 879
lsp-gen-interval 964, 1007
lsp-mtu 965, 1008
lsp-refresh-interval 965, 1009

M

mac access-group 657
mac access-list extended 653
mac access-list standard 649
mac accounting destination 559
mac cam fib-partition 559
mac learning-limit 560
mac-address-table aging-time 556
mac-address-table static 557
mac-address-table station-move 558
Management interface 465
management route 745
match as-path 666
match community 666
match interface 667
match ip access-group 1230
match ip address 667
match ip dscp 1231
match ip next-hop 668
match ip precedence 1232
match ip route-source 669
match metric 669
match origin 670
match route-type 670
match tag 671
max-age 800
max-area-addresses 966, 1010
maximum-paths
    BGP 1046, 1153
    IS-IS 967, 1011
    OSPF 880
    RIP 847
max-lsp-lifetime 967, 1010
MBGP Commands 1098, 1189
member 600
metric-style 968
MIB
    Force10-COPY-CONFIG-MIB 323
minimum-links 501
mirroring source port (deprecated) 507
module power-off 126
motd-banner 127
MSDP 1345
MSTP 825
    debug spanning-tree mstp 825
mtrace 1281
mtu 478
Multicast Source Discovery Protocol
    see MSDP 1345
MULTIPLE SPANNING TREE 77
Multiple Spanning Tree Protocol 825
    see MSTP 825

N

Naming conventions
    Core dump files 92, 224
NDP 1357
negotiation auto 480
neighbor 848
neighbor default-originate 1048, 1155
neighbor description 1049, 1156
Neighbor Discovery Protocol 1357
neighbor distribute-list 1049, 1156
neighbor ebgp-multihop 1050, 1157
neighbor filter-list 1051, 1159
neighbor graceful-restart 1052
neighbor maximum-prefix 1053, 1159
neighbor next-hop-self 1054, 1160
neighbor password 1054, 1161
neighbor peer-group 1055, 1057, 1162, 1163
neighbor remote-as 1058, 1164
neighbor remove-private-as 1059, 1165
neighbor route-map 1059, 1166
neighbor send-community 1061, 1168
neighbor shutdown 1061, 1168
neighbor subnet 1169
neighbor timers 1064, 1170
neighbor update-source 1065, 1171
neighbor weight 1066, 1171
net 969, 1012
network
    BGP 1066, 1113, 1172, 1204
    RIP 848
network area
    OSPF 880
network backdoor 1067, 1173
Network Time Protocol. *See NTP.*
no-more 72
no-more parameter 72
Not So Stubby Area. See NSSA.
NSSA 861
NTP 381
ntp authenticate 382
ntp authentication-key 382
ntp broadcast client 383

ntp disable 383
ntp multicast client 383
ntp server 384
ntp source 385
ntp trusted-key 385
ntp update-calendar 386

O

offline 127
Offline Diagnostics 239
offset-list 849
Open Shortest Path First. See OSPF.
OSPF 859
  clear ipv6 ospf process 914
  clear ospfv3 process 914
  ipv6 ospf area 916
  ipv6 router ospf 920
  link-state 859
  show ipv6 ospf database 923
  show ipv6 ospf neighbor 925
output-delay 850

P

passive-interface
  IS-IS 969, 1012
  OSPF 881
  RIP 850
password 402
permit
  AS-Path Access list 683
  Community Access list 687
  IP ACL (extended) 626
  IP ACL (standard) 608
  MAC ACL (extended) 654
  MAC ACL (standard) 649
  Prefix list 660
  Trace list 439
permit arp 628
permit ether-type 629
permit tcp
  IP ACL 632
  Trace list 440
permit udp
  IP ACL 635
  Trace list 442
PGP keys 1375
PIM
  Dense-Mode 1332
  Sparse-Mode 1317
ping 127
Policy-Based QoS 1227
policy-map-input 1235
Port Channel-Specific Commands 500
Port Mirroring
  Important Points to Remember 515
Port Mirroring (Deprecated) 507
Port-Channel-Specific Commands 500
power-off 129
power-on 129
ppp authentication 536
ppp chap hostname 537
ppp chap password 537
ppp chap rem-hostname 538
ppp chap rem-password 538
ppp next-hop 539
ppp pap hostname 540
ppp pap password 540
ppp pap rem-hostname 541
ppp pap rem-password 541
preempt 789
PREFIX-LIST Mode 75, 76
primary port 504
priority 790
privilege exec 395
privilege level (CONFIGURATION mode) 395
privilege level (LINE mode) 395
PROTOCOL
  Per-VLAN SPANNING TREE Mode 77
  SPANNING TREE Mode 77
PROTOCOL FVRP 78
protocol fvrp 594
PROTOCOL MULTIPLE SPANNING TREE Mode 77
protocol spanning-tree 800

Q

QoS
  clear qos statistics 1229
  Per Port 1219
  Policy-Based 1227
  rate-limit 1241
qos-policy-input 1236
qos-policy-output 1237
Queue Level Debugging 1264
  clear queue statistics ingress 1264, 1265
  show queue statistics egress 1266
Queuing Statistics 1264

R

RAD 1360
radius-server deadtime 409
radius-server host 409
radius-server key 410
radius-server retransmit 411
radius-server timeout 412
RAPID SPANNING TREE Mode 77
rate limit 1220

rate police 1221
rate shape 1223
rate-limit 1241
rate-police 1241
recipient 1372
redirect 773
redistribute
  BGP 1068, 1114, 1174, 1205
  IS-IS 970
  OSPF 883
  RIP 851
redistribute bgp 884
redistribute isis
  OSPF 884
  RIP 852
redistribute ospf
  BGP 1115
  IS-IS 973
  isis 1069
  RIP 852
redundancy auto-failover-limit 367
redundancy disable-auto-reboot 368
redundancy force-failover 369
redundancy primary 370
redundancy reset-counter 370
redundancy synchronize 371
reload 130, 1390
remark 609, 707
rename 1390
reset 130
RFC 1157 323
RFC 1195 941
RFC 2274 323
RFC-2328 872
RFCs. See IETF RFCs
RIP 839
  version 1 839
  version 2 839
RMON
  Important Points to Remember 354
Route Map
  match ip address 714
  match ipv6 next-hop 714
  match ipv6 route-source 715
  route-map 715
  set ipv6 next-hop 716
  show config 716
route-map 672
ROUTE-MAP Mode 75
Router Advertisement Daemon
  see RAD 1360
router bgp 1024, 1129
Router Information Protocol. See RIP.
router isis 974, 1013
ROUTER ISIS Mode 79
router ospf 886
router rip 853
ROUTER RIP Mode 78, 79
router-id 885

S

scramble-atm 542
searching show commands 72
  display 71
  except 71
  find 72
  grep 72
secure copy 86
Security
  aaa accounting 392
  aaa accounting suppress 393
  aaa authorization 394
  show accounting 393
see Neighbor Discovery Protocol 1357
see Storm-Control 447
seq
  IP ACL (extended) 642
  IP ACL (standard) 611
  MAC Access list (extended) 655
  MAC ACL (standard) 650
  Prefix list 661
  Redirect list 774
  Trace list 443
seq arp 638
seq ether-type 640
server 1373
service password-encryption 404
service timestamps 131
service-class dynamic dot1p 1223
service-policy input 1243
service-policy output 1243
service-queue 1244
set as-path 673
set automatic-tag 673
set comm-list delete 674
set level 676
set metric 677
set metric-type 677
set next-hop 678
set origin 679
set tag 679
set weight 680
set-overload-bit 975, 1014
sFlow 260
SFM 129
show alarms 132
show arp 747

show boot selection 1391
show bootflash 1391
show bootvar
BOOT_USER mode 1392
show chassis 133
show config 711
Access list 646
AS-PATH ACL 684
BGP 1072, 1177
Community-list 688
FVRP 595
Interface 483
IS-IS 976, 1015
OSPF 887
Prefix list 662
RIP 854
Route map 680
Spanning Tree 801, 820
Trace list 444
VRRP 790
show configuration 1374
show controllers sonet 543
show debugging 136, 153, 1374
show default-gateway 1393
show diag 136
show environment 137
show fvrp 595
show interface management ethernet 1393
show interface rate 1224
show interfaces 484
show interfaces configured 490
show interfaces description 492
show interfaces linecard 493
show interfaces port-channel 502
show interfaces sonet 545
show interfaces switchport 494
show ip accounting access-list 646
show ip accounting access-lists 445
show ip as-path-access-lists 685
show ip bgp 1073, 1115, 1206
show ip bgp cluster-list 1075, 1117, 1178, 1208
show ip bgp community 1076, 1117, 1179, 1208
show ip bgp community-list 1078, 1118, 1179, 1209
show ip bgp dampened-paths 1079, 1118, 1180, 1210
show ip bgp detail 1079
show ip bgp filter-list 1081, 1119, 1180, 1211
show ip bgp flap-statistics 1082, 1119, 1181, 1212
show ip bgp inconsistent-as 1084, 1120, 1182, 1213
show ip bgp ipv4 multicast 1115
show ip bgp ipv6 1071, 1176, 1178
show ip bgp ipv6 unicast 1206
show ip bgp neighbor 1085, 1120, 1182, 1213
show ip bgp next-hops 1089, 1183
show ip bgp paths 1089, 1123, 1184, 1216
show ip bgp paths as-path 1091, 1185
show ip bgp paths community 1092, 1185
show ip bgp peer-group 1093, 1123, 1185, 1216
show ip bgp summary 1096, 1124, 1187, 1217
show ip cam 750
show ip community-lists 689
show ip fib linecard 178, 753
show ip flow 754
show ip igmp groups 1290
show ip igmp interface 1291
show ip interface 755
show ip management-route 757
show ip mroute 1281
show ip ospf 887
show ip ospf database 889
show ip ospf database asbr-summary 890
show ip ospf database database-summary 900
show ip ospf database external 892
show ip ospf database network 893
show ip ospf database nssa-external 895
show ip ospf database opaque-area 896
show ip ospf database opaque-as 897
show ip ospf database opaque-link 898
show ip ospf database router 898
show ip ospf interface 902
show ip ospf neighbor 904
show ip ospf virtual-links 909
show ip pim interface 1325, 1341
show ip pim neighbor 1326, 1342
show ip pim rp mapping 1327, 1342
show ip pim tib 1328, 1343
show ip prefix-list detail 662
show ip prefix-list summary 663
show ip protocols 758
show ip redirect-list 777
show ip rip database 854
show ip route 758
show ip route list 760
show ip route summary 761
show ip ssh 431
show ip traffic 762
show ipv6 accounting access-list 712
show ipv6 neighbors 1359
show isis database 976, 1015
show isis hostname 978, 1016
show isis interface 978, 1016
show isis neighbors 979, 1017
show isis protocol 980, 1018
show isis traffic 981
show keys 1375
show linecard 140
show logging 349
show mac accounting access-list 658
show mac accounting destination 566

show mac learning-limit 568
show mac-address-table 564
show mac-address-table aging-time 566
show memory 144
show ntp associations 388
show ntp status 389
show port-channel-flow 505
show privilege 405
show processes cpu 146
show processes memory 150
show processes switch-utilization 153
show qos class-map 1248
show qos policy-map 1249
show qos policy-map-input 1251
show qos policy-map-output 1252
show qos qos-policy-input 1253
show qos qos-policy-output 1253
show qos statistics 1254
show qos wred-profile 1257
show redundancy 369
show route-map 681, 717
show rpm 153
show run mirroring (deprecated) 507
show running-config acl 713
show sfm 155
show snmp 324, 325, 326
show spanning-tree 0 801
show tcp statisitics 765
show tech-support 157, 237
show users 405
show vlan 571
show vrrp 791
shutdown 496
SMTP (Simple Mail Transfer Protocol) server 1367, 1375
smtp server-address 1375
SNMP
  number of traps supported 323
  versions supported 323
SNMP SET requests 323
snmp trap link-status 338
snmp-server community 326
snmp-server contact 328
snmp-server enable traps 328
snmp-server host 332
snmp-server location 334
snmp-server trap-source 334
Spanning Tree Protocol
  BPDU guard 804
  interface cost 803
  portfast 804
spanning-tree 803
speed 547
  100/1000 Base-T Ethernet interfaces 497
  Management interface 498
spf-interval 983, 1019
SSH
  ssh-peer-rpm 160
ssh 433
Storm-Control 447
  Important Points to Remember 447
Streamline Upgrade 87
summary-address 910
switchport 498

T

tacacs-server host 413
tacacs-server key 414
tagged 572
TDR
  Important Points to Remember 508
Telnet
  number of Telnet sessions supported 125
telnet 160
terminal length 162
terminal monitor 350
threshold 1260
Time Domain Reflectometer (TDR) 507
timeout login response 406
timers basic 855
timers bgp 1188
timers spf 911
TOS 891, 893, 895, 897, 899, 901
traceroute 163
track 793
Troubleshooting 1395, 1397
trust diffserv 1261
trust ipv6-diffserv 182
Type of Service. *See TOS.*

U

undebug all 164
untagged 574
username 406

V

version 856
Virtual LANs. *See VLANs.*
Virtual Router Redundancy Protocol. *See VRRP.*
virtual-address 794
VLANs
  ACL support 473
  definition 569
  IP features not supported 569
vlan-stack access 600
vlan-stack compatible 601

vlan-stack protocol-type 602
vlan-stack trunk 603
VLAN-Stack VLANs
Important Points to Remember 599
VRRP 785
vrrp-group 795

W

warm upgrade 369
WRED
pre-defined profile names 1260
wred 1262
wred-profile 1263
write 167

X

XML
terminal xml 162

Command Index

A

aaa accounting 392
aaa accounting suppress 393
aaa authorization 394
Access list
- access-class 399, 644
- clear counters ip access-group 645
- ip access-group 645
- show config 646, 680
- show ip accounting access-list 646

Access list (extended)
- deny 613
- deny tcp 436, 621
- deny udp 623
- ip access-list extended 625
- permit 439, 626
- permit arp 628
- permit tcp 632
- permit udp 442, 635
- seq 642

Access list (standard)
- deny 606
- ip access-list standard 607
- permit 608
- seq 611

Access-list (extended)
- deny arp 615
- deny ether-type 616
- permit ether-type 629
- seq arp 638
- seq ether-type 640

acl-vlan-group 307
admin-email 1366
Alarms
- audible cut-off 107
- clear alarms 111
- show alarms 132

ARP
- arp 720
- arp timeout 721
- clear arp-cache 721
- debug arp 724
- show arp 747

AS-PATH Access list
- deny 682
- ip as-path access-list 682
- permit 683
- show config 684
- show ip as-path-access-list 685

B

bandwidth-percentage 1228
banner exec 107
banner login 108
banner motd 109
BGP
- aggregate-address 1024, 1100, 1129, 1190
- bgp always-compare-med 1025, 1131
- bgp bestpath as-path ignore 1025, 1131
- bgp bestpath med confed 1026, 1132
- bgp client-to-client reflection 1027, 1133
- bgp cluster-id 1027, 1133
- bgp confederation identifier 1028, 1134
- bgp confederation peers 1029, 1135
- bgp dampening 1029, 1101, 1136, 1192
- bgp default local-preference 1030, 1137
- bgp fast-external-fallover 1032, 1137
- bgp graceful-restart 1032, 1138
- bgp log-neighbor-changes 1033, 1139
- bgp non-deterministic-med 1034, 1139
- bgp router-id 1035, 1140
- capture bgp-pdu max-buffer-size 1037, 1141
- capture bgp-pdu neighbor (ipv4) 1036
- capture bgp-pdu neighbor (ipv6) 1141
- clear ip bgp dampening 1039
- clear ip bgp flap-statistics 1039, 1103, 1194
- clear ip bgp ipv6 dampening 1145
- clear ip bgp ipv6 flap-statistics 1146
- clear ip bgp peer-group 1038, 1145
- debug ip bgp 1040, 1147
- debug ip bgp dampening 1041
- debug ip bgp events 1042
- debug ip bgp events (ipv6) 1148
- debug ip bgp ipv6 dampening 1148
- debug ip bgp keepalives 1042, 1149
- debug ip bgp notifications 1043, 1150
- debug ip bgp updates 1044, 1104, 1150, 1195, 1196
- default-metric 1045, 1151
- distance bgp 1045, 1152
- maximum-paths 1046, 1153
- neighbor activate 1047, 1153
- neighbor advertisement-interval 1047, 1154
- neighbor default-originate 1048, 1155
- neighbor description 1049, 1156

neighbor distribute-list 1049, 1108, 1156, 1199
neighbor ebgp-multihop 1050, 1157
neighbor filter-list 1051, 1159
neighbor graceful-restart 1052
neighbor maximum-prefix 1053, 1159
neighbor next-hop self 1054, 1160
neighbor password 1054, 1161
neighbor peer-group
assigning peers 1055, 1162
creating group 1057, 1163
neighbor remote-as 1058, 1164
neighbor remove-private-as 1059, 1165
neighbor route-map 1059, 1111, 1166, 1203
neighbor route-reflector-client 1060, 1167
neighbor send-community 1061, 1168
neighbor shutdown 1061, 1168
neighbor subnet 1063
neighbor timers 1064, 1170
neighbor update-source 1065, 1171
neighbor weight 1066, 1171
network 1066, 1113, 1172, 1204
network backdoor 1067, 1173
redistribute 1068, 1114, 1174, 1205
redistribute ospf 1069, 1070, 1115, 1175
router bgp 1071, 1176
show capture bgp-pdu neighbor (ipv4) 1071
show config 1072, 1177
show ip bgp 1073
show ip bgp cluster-list 1075, 1117, 1178
show ip bgp community 1076, 1117, 1179, 1208
show ip bgp community-list 1078, 1118, 1179, 1209
show ip bgp dampened-paths 1079, 1118, 1180, 1210
show ip bgp filter-list 1081, 1119, 1180, 1211
show ip bgp flap-statistics 1082, 1119, 1212
show ip bgp inconsistent-as 1084, 1120, 1182, 1213
show ip bgp ipv6 1176, 1178
show ip bgp ipv6 flap-statistics 1181
show ip bgp ipv6 unicast detail 1210
show ip bgp neighbor 1085, 1120, 1182, 1213
show ip bgp next-hops 1089, 1183
show ip bgp paths 1089, 1184
show ip bgp paths as-path 1091, 1185
show ip bgp paths community 1092, 1185
show ip bgp peer-group 1093, 1123, 1185, 1216
show ip bgp regexp 1095, 1186
show ip bgp summary 1096, 1124, 1187, 1217
timers bgp 1188
boot config 82, 1377
boot host 82
boot network 83
boot system 84
boot system gateway 85
BOOT_USER
boot change 1384
boot messages 1385
boot selection 1385
default-gateway 1386
delete 1386
dir 1387
enable 1388
format 1388
ignore enable-password 1388
interface management ethernet ip address 1389
interface management port config 1389
reload 1390
rename 1390
show boot selection 1391
show bootflash 1391
show bootvar 1392
show default-gateway 1393
show interfaces management ethernet 1393

C

calendar set 376
call-home 1366
cam ipv4flow chassis (EtherScale) 297
cam ipv4flow chassis (TeraScale) 299
cam ipv4flow linecard (EtherScale) 300
cam ipv4flow linecard (TeraScale) 302
capture bgp-pdu max-buffer-size 1037, 1141
capture bgp-pdu neighbor (ipv4) 1036
capture bgp-pdu neighbor (ipv6) 1141
cd 85
change bootflash-image 85
chassis chassis-mode 110
class-map 1228
clear counters ipv6 access-group 692
clear ip bgp 1037, 1102, 1193
clear ip bgp * (asterisk) 1142
clear ip bgp as-number 1143
clear ip bgp ipv4 multicast 1102, 1192
clear ip bgp ipv6-address 1144
clear ip fib linecard 723
clear ip route 723
clear ipv6 ospf process 914
clear lacp counters 521
clear line 111
clear mac-address-table dynamic 556
clear qos statistics 1229
clear queue statistics ingress 1264, 1265
clear tcp statistics 724
clock read-calendar 377
clock set 377

clock summer-time date 378
clock summer-time recurring 379
clock timezone 380
clock update-calendar 381
Community Access list
deny 686
ip community-list 687
permit 687
show config 688
show ip community-lists 689
configure 111
copy 86
copy (Streamline Upgrade) 87
copy running-config startup-config duplicate 88
Core-Dump 93

D

Debug
debug arp 724
debug ftpserver 113
debug ip bgp 1040
debug ip bgp (ipv6) 1147
debug ip bgp dampening 1041
debug ip bgp events 1042
debug ip bgp events (ipv6) 1148
debug ip bgp ipv6 dampening 1148
debug ip bgp keepalives 1042, 1149
debug ip bgp notifications 1043, 1150
debug ip bgp updates 1044, 1104, 1150, 1195, 1196
debug ip icmp 726
debug ip igmp 1285, 1293
debug ip msdp 1346
debug ip ospf 866
debug ip packet 727
debug ip pim 1318
debug ip rip 841
debug ipv6 pim 1334
debug isis 946, 991
debug isis adj-packets 946, 992
debug isis local-updates 947, 992
debug isis snp-packets 948, 993
debug isis spf-triggers 948, 994
debug isis update-packets 949, 994
debug multiple spanning-tree 825
debug ntp 381
debug radius 408
debug spanning-tree 798
debug vrrp 787
show debugging 136
undebug all 164
debug callhome 1367
debug cpu-traffic-stats 112, 207
debug fefd 779
debug ipv6 pim 1334
delete 88
deny 692
deny tcp 695
deny udp 697
description 308
dir 89
disable 113
DNS
clear host 722
ip domain-list 732
ip domain-lookup 733
ip domain-name 734
domain-name 1368
download alt-boot-image 89
download alt-full-image 90
duplex (10/100 Interfaces) 461
duplex (Management) 460

E

enable 114, 1369
enable-all 1369
encrypt 1370
end 116
exec-banner 117
exec-timeout 117
exit 118

F

FEFD 779
debug fefd 779
fefd 780
fefd disable 781
fefd interval 782
fefd reset 783
fefd-global 781
fefd-global interval 782
show fefd 783
format 91
frequency 1371
FTP
debug ftpserver 113
ftp-server enable 118
ftp-server topdir 119
ftp-server username 120
ip ftp password 121
ip ftp source-interface 121
ip ftp username 122
FVRP

disable 586
fvrp access 586
fvrp aware 587
fvrp control-vlan 588
fvrp core 588
fvrp core region 589
fvrp disable 589
fvrp domain 590
fvrp group 591
fvrp hello-time 591
fvrp preempt 592
fvrp priority
for a VLAN 592
for an interface 593
fvrp uplink 594
protocol fvrp 594
show config 595
show fvrp 595

H

hostname 120

I

IGMP
clear ip igmp groups 1285
debug ip igmp 1285, 1293
igmp snooping fast-leave 1295
ip igmp immediate-leave 1286
ip igmp last-member-query-interval 1286
ip igmp querier-timeout 1287
ip igmp query-interval 1287
ip igmp query-ma-resp-time 1288
ip igmp static-group 1288
show ip igmp groups 1289, 1290
show ip igmp interface 1291
IGMP Snooping
igmp snooping flood 1295
igmp snooping last-member-query-interval 1296
igmp snooping querier 1297
ip igmp snooping enable 1294
ip igmp snooping mroute 1296
show ip igmp snooping mrouter 1297
Interface
clear counters 456
description 460
dot1p-priority 1219
interface 464
interface loopback 464
interface ManagementEthernet 465
interface null 466
interface port-channel 467
interface sonet 534
interface vlan 473
ip unreachables 741
ipg 474
negotiation auto 480
show config 483
show interfaces 253, 254, 256, 484
show interfaces linecard 493
show interfaces switchport 494
shutdown 496
switchport 498
interface range 468
interface range macro (define) 470
interface range macro name 472
interface rate-interval 472
interface vlan 473
ip access-group 309
ip address 731
ip directed-broadcast 732
ip fib download-igp-only 734
ip helper-address 735
ip helper-address hop-count disable 735
ip host 736
ip igmp snooping enable 1294
ip igmp snooping fast-leave 1295
ip igmp snooping flood 1295
ip igmp snooping last-member-query-interval 1296
ip igmp snooping mrouter 1296
ip igmp snooping querier 1297
ip max-frag-count 736
ip mroute 1278
ip multicast-lag-hashing 1279
ip multicast-routing 1280
ip name-server 738
ip pim bsr-border 1319
ip proxy-arp 739
ip redirects 739
ip route 740
ip source-route 741
ipv6 access-list 700
ipv6 ospf area 916
IPv6 PIM
debug ipv6 pim 1334
ipv6 pim dr-priority 1336
ipv6 pim query-interval 1336
ipv6 pim sparse-mode 1338
show ipv6 pim bsr-router 1340
show ipv6 pim interface 1341
show ipv6 pim neighbor 1342
show ipv6 pim rp 1342
show ipv6 pim tib 1343
ipv6 pim dr-priority 1336
ipv6 pim query-interval 1336
ipv6 pim sparse-mode 1338

ipv6 router ospf 920, 923
IS-IS
advertise 943, 988
area-password 944, 988
clear config 944, 989
clear isis 945, 990
clns host 945, 990
debug isis 946, 991
debug isis adj-packets 946, 992
debug isis local-updates 947, 992
debug isis snp-packets 948, 993
debug isis spf-triggers 948, 994
debug isis update-packets 949, 994
default-information originate 949, 995
distance 950
distribute-list in 951
distribute-list out 952
domain-password 953, 996
hello padding 954, 996
hostname dynamic 955, 997
ignore-lsp-errors 955, 998
ip router isis 956
isis circuit-type 956, 998
isis csnp-interval 957, 999
isis hello-interval 958, 1000
isis hello-multiplier 959, 1001
isis metric 960, 1003
isis network point-to-point 961, 1003
isis password 961, 1004
isis priority 962, 1005
is-type 963, 1006
log-adjacency-changes 963, 1006
lsp-gen-interval 964, 1007
lsp-mtu 965, 1008
lsp-refresh-interval 965, 1009
max-area-addresses 966, 1010
maximum-paths 967, 1011
max-lsp-lifetime 967, 1010
metric-style 968
net 969, 1012
passive-interface 969, 1012
redistribute 970
redistribute ospf 973
router isis 974, 1013
set-overload-bit 975, 1014
show config 976, 1015
show isis database 976, 1015
show isis hostname 978, 1016
show isis interface 978, 1016
show isis neighbors 979, 1017
show isis protocol 980, 1018
spf-interval 983, 1019
isis hello padding 959, 1002

K

keepalive 475, 534
keyadd 1371

L

lacp port-priority 523
lacp system-priority 524
lfs enable 475
line 125
linecard 126
load-balance 744
Logging
clear logging 339
default logging buffered 340
default logging console 340
default logging monitor 341
default logging trap 341
logging 341
logging buffered 342
logging console 343
logging facility 343
logging history 344
logging history size 345
logging monitor 346
logging on 346
logging source-interface 347
logging synchronous 347
logging trap 348
no logging on 346
show logging 349
logging kernel-coredump 91
logging kernel-coredump server 93

M

MAC Access list
clear counters mac access-group 657
mac access-group 657
show mac accounting access-list 658
MAC Access list (extended)
deny 651
mac-access-list extended 653
permit 654
seq 655
MAC Access list (standard)
deny 648
mac-access-list standard 649
permit 649
seq 650
mac accounting destination 559
mac cam fib-partition 559

mac learning-limit 560
mac-address-table aging-time 556
mac-address-table static 557
mac-address-table station-move 558
match ip access-group 1230
match ip dscp 1231
match ip precedence 1232
match ipv6 address 714
match ipv6 next-hop 714
match ipv6 route-source 715
MBGP Commands 1098, 1189
member 600
member vlan 309
monitor 476
motd-banner 127
MSDP
clear ip msdp peer 1345
clear ip msdp sa-cache 1346
debug ip msdp 1346
ip msdp default-peer 1348
ip msdp log-adjacency-changes 1348
ip msdp mesh-group 1349
ip msdp originator-id 1349
ip msdp peer 1350, 1352
ip msdp shutdown 1352
ip multicast-msdp 1353
show ip msdp 1353
MSTP
debug spanning-tree mstp 825
disable 826
forward-delay 827
hello-time 827
max-age 828
max-hops 828
name 830
protocol spanning-tree mstp 830
revision 831
show config 832
show spanning-tree mst configuration 832
show spanning-tree msti 833
spanning-tree 835
spanning-tree msti 836
spanning-tree mstp edge-port 837
mtrace 1281
mtu 478
Multiple Spanning Tree Protocol
see MSTP 825

N

NTP
debug ntp 381
ntp authenticate 382
ntp authentication-key 382
ntp broadcast client 383
ntp disable 383
ntp multicast client 383
ntp server 384
ntp source 385
ntp trusted-key 385
ntp update-calendar 386
show ntp associations 388
show ntp status 389

O

OSPF
area default-cost 861
area nssa 861
area range 862
area stub 862
area virtual-link 863
auto-cost 864
clear ip ospf 865
debug ip ospf 866
default-information originate 867
default-metric 868
distance 869
distance ospf 869
distribute-list in 870
distribute-list out 871
enable inverse mask 871
graceful-restart grace-period 872
graceful-restart helper-reject 873
graceful-restart mode 873
graceful-restart role 873
ip ospf auth-change-wait-time 874
ip ospf authentication-key 874
ip ospf cost 875
ip ospf dead-interval 875
ip ospf hello-interval 876
ip ospf message-digest-key 876
ip ospf mtu-ignore 877
ip ospf network 878
ip ospf priority 878
ip ospf retransmit-interval 879
ip ospf transmit-delay 879
log-adjacency-changes 880
maximum-paths 880
network area 880
passive-interface 881
redistribute 883
redistribute isis 884
router ospf 886
show config 887
show ip ospf 887

show ip ospf database 889
show ip ospf database asbr-summary 890
show ip ospf database database-summary 900
show ip ospf database external 892
show ip ospf database network 893
show ip ospf database nssa-external 895
show ip ospf database opaque-area 896
show ip ospf database opaque-as 897
show ip ospf database opaque-link 897, 898
show ip ospf database router 898
show ip ospf interface 902
show ip ospf neighbor 904
show ip ospf virtual-links 909
summary-address 910
timers spf 911

P

permit 701
permit tcp 703
permit udp 705
PIM-DM
ip pim dense-mode 1332
PIM-SM
clear ip pim rp-mapping 1318
clear ip pim tib 1318
debug ip pim 1318
ip pim dr-priority 1320
ip pim query-interval 1321
ip pim rp-address 1321, 1337
ip pim sparse-mode 1323
show ip pim bsr-router 1324
show ip pim interface 1325
show ip pim neighbor 1326
show ip pim rp 1327
show ip pim tib 1328
ping 127
Policy based Routing
ip redirect-group 770
ip redirect-list 771
redirect 773
seq 774
show ip redirect-list 777
policy-aggregate 1234
policy-map-input 1235
policy-map-output 1236
Port Channel
channel-member 500
interface port-channel 467
minimum-links 501
minimum-links command 501
show interfaces port-channel 502
port-channel mode 524
port-channel-protocol lacp 525
power-off 129
power-on 129
Prefix list
clear ip prefix-list 659
deny 659
ip prefix-list 660
permit 660
seq 661
show config 662
show ip prefix-list detail 662
show ip prefix-list summary 663
pwd 93

Q

QoS
bandwidth-percentage 1228
class-map 1228
match ip access-group 1230
match ip dscp 1231
match ip precedence 1232
policy-aggregate 1234
policy-map-input 1235
policy-map-output 1236
qos-policy-output 1237
rate limit 1220
rate police 1221
rate shape 1223
rate-police 1241
rate-shape 1242
service-class dynamic dot1p 1223
service-policy input 1243
service-policy output 1243
service-queue 1244
show interfaces rate 1224
show qos class-map 1248
show qos policy-map 181, 1249
show qos policy-map-input 1251
show qos policy-map-output 1252
show qos qos-policy-input 1253
show qos qos-policy-output 1253
show qos statistics 1254
strict-priority queue 1226
threshold 1260
trust diffserv 1261
wred 1262
wred-profile 1263
qos 1237
qos-policy-input 1236
qos-policy-output 1237

R

RADIUS
- debug radius 408
- ip radius source-interface 408
- radius-server deadtime 409
- radius-server host 409
- radius-server key 410
- radius-server retransmit 411
- radius-server timeout 412

rate-limit 1241
rate-police 1241
recipient 1372
redistribute bgp 884
redistribute ospf
- BGP 1070, 1176

Redundancy
- redundancy primary 370
- show redundancy 372

reload 130
remark 609
rename 94
reset 130, 168
RIP
- auto-summary 840
- clear ip rip 840
- debug ip rip 841
- default-information originate 841
- default-metric 842
- distance 843
- distribute-list in 843
- distribute-list out 844
- ip poison-reverse 845
- ip rip receive version 845
- ip rip send version 846
- ip split-horizon 847
- maximum-paths 847
- neighbor 848
- network 848
- offset-list 849
- output-delay 850
- passive-interface 850
- redistribute 851
- redistribute isis 852
- redistribute ospf 852
- router rip 853
- show config 854
- show ip rip database 854
- timers basic 855
- version 856

rmon alarm 354
rmon collection history 355
rmon collection statistic 356
rmon collection statistics 356
RMON Commands 353
rmon event 356
rmon hc-alarm 357
Route map
- match as-path 666
- match community 666
- match interface 667
- match ip address 667
- match ip next-hop 668
- match ip route-source 669
- match metric 669
- match origin 670
- match route-type 670
- match tag 671
- route-map 672
- set as-path 673
- set automatic-tag 673
- set comm-list delete 674
- set community 675
- set level 676
- set local-preference 676
- set metric 677
- set metric-type 677
- set next-hop 678
- set origin 679
- set tag 679
- set weight 680
- show route-map 681

route-map 715
router-id 885
RSTP
- bridge-priority 815
- debug spanning-tree rstp 816
- disable 817
- forward-delay 817
- hello-time 818
- max-age 818
- protocol spanning-tree rstp 819
- show config 820
- show spanning-tree rstp 820
- spanning-tree rstp 822

S

SCP
- ip scp topdir 424

Security
- aaa authentication login 397
- enable password 399
- enable restricted 400
- login authentication 402
- password 402
- privilege level 395

service password-encryption 404
show privilege 405
show users 405
timeout login response 406
username 406
seq 709
server 1373
service power-off 126
service timestamps 131
service-policy-input 1225, 1243, 1255, 1256, 1257
service-policy-output 1243
service-queue 1244
set ipv6 next-hop 716
sflow collector 260
sflow enable (Global) 261
sflow enable (Interface) 262
sflow polling-interval (Global) 265
sflow polling-interval (Interface) 265
sflow sample-rate (Global) 266
sflow sample-rate (Interface) 267
show accounting 393
show acl-vlan-group 310
show bootvar 94
show calendar 386
show cam ipv4flow 303
show capture bgp-pdu neighbor (ipv4) 1071
show chassis 133
show clock 387
show config 311, 711, 716
show configuration 1374
show cpu-traffic-stats 135
show debugging 1374
show environment 137
show fefd 783
show file 95
show file-systems 96
show hosts 749
show interfaces configured 490
show interfaces description 492
show interfaces rate 1224
show ip bgp 1073
show ip bgp detail 1079
show ip bgp ipv4 multicast 1115, 1206
show ip bgp ipv6 1178
show ip bgp ipv6 unicast detail 1210
show ip cam 750
show ip fib linecard 178, 753
show ip flow 754
show ip interface 755
show ip management-route 757
show ip mroute 1278, 1281, 1283, 1285, 1286, 1287, 1288, 1289, 1290, 1291, 1300
show ip protocols 758
show ip route 758
show ip route list 760
show ip route summary 761
show ip traffic 762
show ipv6 ospf database 923
show ipv6 ospf neighbor 925
show ipv6 pim bsr-router 1340
show ipv6 pim interface 1341
show ipv6 pim neighbor 1342
show ipv6 pim rp 1342
show ipv6 pim tib 1343
show isis traffic 981
show keys 1375
show lacp 525
show linecard 140
show mac accounting destination 566
show mac cam 567
show mac learning-limit 568
show mac-address-table 564
show mac-address-table aging-time 566
show memory 144
show os-version 97
show port-channel-flow 505
show processes cpu 146
show processes memory 150
show processes switch-utilization 153
show qos class-map 1248
show qos policy-map 181, 1249
show qos policy-map-input 182, 1251
show qos policy-map-output 1252
show qos qos-policy-input 1253
show qos qos-policy-output 1253
show qos statistics 1254
show qos wred-profile 1257
show queue statistics egress 1266
show rmon 358
show rmon alarms 359
show rmon events 360
show rmon hc-alarm 361
show rmon history 362
show rmon log 363
show rmon statistics 364
show route-map 717
show rpm 153
show running config acl-vlan-group 312
show running-config 98
show sflow 267
show sflow linecard 269
show sfm 155
show startup-config 102
show tcp statistics 765
show tdr 509
show tech-support 157, 158, 237
show version 100
smtp 1375

SNMP
show snmp 324, 325
show snmp user 326
snmp trap link-status 338
snmp-server community 326
snmp-server contact 328
snmp-server enable traps 328
snmp-server host 332
snmp-server location 334
snmp-server trap-source 334
SONET
ais-shut 528
alarm-report 528
clock source 530
debug ppp 530
delay triggers 531
down-when-looped 532
encap 532
flag 533
framing 533
interface sonet 534
loopback 535
ppp authentication 536
ppp chap hostname 537
ppp chap password 537
ppp chap rem-hostname 538
ppp chap rem-password 538
ppp next-hop 539
ppp pap hostname 540
ppp pap password 540
ppp pap rem-hostname 541
ppp pap rem-password 541
scramble-atm 542
show controllers 543
show interfaces sonet 545
speed 547
Spanning Tree
bridge-priority 797
debug spanning-tree 798
disable 798, 805
forward-delay 799
hello-time 799
max-age 800
protocol spanning-tree 800
show config 801
show spanning-tree 0 801
spanning-tree 803
speed
10/100/1000 Base-T Ethernet Interfaces 497
Management interface 498
SSH
show ip ssh 431
ssh 433
ssh-peer-rpm 160
strict-priority queue 1226

T

TACACS
ip tacacs source-interface 413
tdr-cable-test 508
Telnet
ip telnet server enable 123
ip telnet source-interface 123
telnet 160
telnet-peer-rpm 161
terminal length 162
terminal monitor 350
TFTP
ip tftp source-interface 124
threshold 1260
Time Domain Reflectometer
show tdr 509
tdr-cable-test 508
Trace list
clear counters ip trace-group 434
deny 435
deny udp 437
ip trace-group 438
ip trace-list 439
permit tcp 440
seq 443
show config 444
show ip accounting trace-lists 445
traceroute 163
trust diffserv 1261

U

upgrade 103

V

VLAN
default vlan-id 570
interface vlan 473
show vlan 571
tagged 572
untagged 574
vrrp-group 795
VLAN-stack VLANs
member 600
vlan-stack access 600
vlan-stack compatible 601
vlan-stack protocol-type 602
vlan-stack trunk 603

VRRP
advertise-interval 785
authentication-type 786
clear vrrp counters 787
debug vrrp 787
description 788
disable 788
hold-time 789
preempt 789
priority 790
show config 790
show vrrp 791
track 793
virtual-address 794

W

WAN Port 499
wred 1244, 1262
wred-profile 1263
write 167