



# **NATIVE Command Line Interface Reference Manual**

Revision Date: 08.04.04



---

## NOTICE

Enterasys Networks reserves the right to make changes in specifications and other information contained in this document and its web site without prior notice. The reader should in all cases consult Enterasys Networks to determine whether any such changes have been made.

The hardware, firmware, or software described in this document is subject to change without notice.

IN NO EVENT SHALL ENTERASYS NETWORKS BE LIABLE FOR ANY INCIDENTAL, INDIRECT, SPECIAL, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING BUT NOT LIMITED TO LOST PROFITS) ARISING OUT OF OR RELATED TO THIS DOCUMENT, WEB SITE, OR THE INFORMATION CONTAINED IN THEM, EVEN IF ENTERASYS NETWORKS HAS BEEN ADVISED OF, KNEW OF, OR SHOULD HAVE KNOWN OF, THE POSSIBILITY OF SUCH DAMAGES.

Enterasys Networks, Inc.  
50 Minuteman Road  
Andover, MA 01810

© 2004 Enterasys Networks, Inc. All rights reserved.

Part Number: 9032553-26 August 2004

ENTERASYS NETWORKS, X-PEDITION, and any logos associated therewith, are trademarks or registered trademarks of Enterasys Networks, Inc. in the United States and other countries.

All other product names mentioned in this manual may be trademarks or registered trademarks of their respective companies.

---

## CODE COPYRIGHTS AND ACKNOWLEDGEMENTS

The SSH implementation contained in this software is derived from OpenSSH. Copyright (c) 1999-2000 Markus Friedl, Theo de Raadt, Niels Provos, Dug Song, Aaron Campbell, Damien Miller, and Kevin Steves.

Portions of this software are derived from Secure Shell. Copyright (c) 1995 Tatu Ylonen <ylo@cs.hut.fi>, Espoo, Finland.

This product contains cryptographic software written by Eric A. Young. Copyright (c) 1995-1998 Eric Young (eay@cryptsoft.com).

Portions of this software are derived from ssh-keygen. Copyright (c) 1995, 1996 by David Mazieres <dm@lcs.mit.edu>.

This software contains the Cryptographic Attack Detector for SSH. Copyright (c) 1998 CORE SDI S.A., Buenos Aires, Argentina.

THE SOFTWARE COMPONENTS LISTED ABOVE ARE PROVIDED BY THE AUTHORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THE SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.



---

## **ENTERASYS NETWORKS, INC. FIRMWARE LICENSE AGREEMENT**

### **BEFORE OPENING OR UTILIZING THE ENCLOSED PRODUCT, CAREFULLY READ THIS LICENSE AGREEMENT.**

This document is an agreement (“Agreement”) between the end user (“You”) and Enterasys Networks, Inc. on behalf of itself and its Affiliates (as hereinafter defined) (“Enterasys”) that sets forth Your rights and obligations with respect to the Enterasys software program/firmware installed on the Enterasys product (including any accompanying documentation, hardware or media) (“Program”) in the package and prevails over any additional, conflicting or inconsistent terms and conditions appearing on any purchase order or other document submitted by You. “Affiliate” means any person, partnership, corporation, limited liability company, or other form of enterprise that directly or indirectly through one or more intermediaries, controls, or is controlled by, or is under common control with the party specified. This Agreement constitutes the entire understanding between the parties, and supersedes all prior discussions, representations, understandings or agreements, whether oral or in writing, between the parties with respect to the subject matter of this Agreement. The Program may be contained in firmware, chips or other media.

BY INSTALLING OR OTHERWISE USING THE PROGRAM, YOU REPRESENT THAT YOU ARE AUTHORIZED TO ACCEPT THESE TERMS ON BEHALF OF THE END USER (IF THE END USER IS AN ENTITY ON WHOSE BEHALF YOU ARE AUTHORIZED TO ACT, “YOU” AND “YOUR” SHALL BE DEEMED TO REFER TO SUCH ENTITY) AND THAT YOU AGREE THAT YOU ARE BOUND BY THE TERMS OF THIS AGREEMENT, WHICH INCLUDES, AMONG OTHER PROVISIONS, THE LICENSE, THE DISCLAIMER OF WARRANTY AND THE LIMITATION OF LIABILITY. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT OR ARE NOT AUTHORIZED TO ENTER INTO THIS AGREEMENT, ENTERASYS IS UNWILLING TO LICENSE THE PROGRAM TO YOU AND YOU AGREE TO RETURN THE UNOPENED PRODUCT TO ENTERASYS OR YOUR DEALER, IF ANY, WITHIN TEN (10) DAYS FOLLOWING THE DATE OF RECEIPT FOR A FULL REFUND.

IF YOU HAVE ANY QUESTIONS ABOUT THIS AGREEMENT, CONTACT ENTERASYS NETWORKS, LEGAL DEPARTMENT AT (978) 684-1000.

**You and Enterasys agree as follows:**

- 1. LICENSE.** You have the non-exclusive and non-transferable right to use only the one (1) copy of the Program provided in this package subject to the terms and conditions of this Agreement.
- 2. RESTRICTIONS.** Except as otherwise authorized in writing by Enterasys, You may not, nor may You permit any third party to:
  - (i) Reverse engineer, decompile, disassemble or modify the Program, in whole or in part, including for reasons of error correction or interoperability, except to the extent expressly permitted by applicable law and to the extent the parties shall not be permitted by that applicable law, such rights are expressly excluded. Information necessary to achieve interoperability or correct errors is available from Enterasys upon request and upon payment of Enterasys’ applicable fee.
  - (ii) Incorporate the Program, in whole or in part, in any other product or create derivative works based on the Program, in whole or in part.
  - (iii) Publish, disclose, copy, reproduce or transmit the Program, in whole or in part.
  - (iv) Assign, sell, license, sublicense, rent, lease, encumber by way of security interest, pledge or otherwise transfer the Program, in whole or in part.
  - (v) Remove any copyright, trademark, proprietary rights, disclaimer or warning notice included on or embedded in any part of the Program.
- 3. APPLICABLE LAW.** This Agreement shall be interpreted and governed under the laws and in the state and federal courts of the Commonwealth of Massachusetts without regard to its conflicts of laws provisions. You accept the personal jurisdiction and venue of the Commonwealth of Massachusetts courts. None of the 1980 United Nations Convention on Contracts for the International Sale of Goods, the United Nations Convention on the Limitation Period in the International Sale of Goods, and the Uniform Computer Information Transactions Act shall apply to this Agreement.

---

**4. EXPORT RESTRICTIONS.** You understand that Enterasys and its Affiliates are subject to regulation by agencies of the U.S. Government, including the U.S. Department of Commerce, which prohibit export or diversion of certain technical products to certain countries, unless a license to export the Program is obtained from the U.S. Government or an exception from obtaining such license may be relied upon by the exporting party.

If the Program is exported from the United States pursuant to the License Exception CIV under the U.S. Export Administration Regulations, You agree that You are a civil end user of the Program and agree that You will use the Program for civil end uses only and not for military purposes.

If the Program is exported from the United States pursuant to the License Exception TSR under the U.S. Export Administration Regulations, in addition to the restriction on transfer set forth in Sections 1 or 2 of this Agreement, You agree not to (i) reexport or release the Program, the source code for the Program or technology to a national of a country in Country Groups D:1 or E:2 (Albania, Armenia, Azerbaijan, Belarus, Bulgaria, Cambodia, Cuba, Estonia, Georgia, Iraq, Kazakhstan, Kyrgyzstan, Laos, Latvia, Libya, Lithuania, Moldova, North Korea, the People's Republic of China, Romania, Russia, Rwanda, Tajikistan, Turkmenistan, Ukraine, Uzbekistan, Vietnam, or such other countries as may be designated by the United States Government), (ii) export to Country Groups D:1 or E:2 (as defined herein) the direct product of the Program or the technology, if such foreign produced direct product is subject to national security controls as identified on the U.S. Commerce Control List, or (iii) if the direct product of the technology is a complete plant or any major component of a plant, export to Country Groups D:1 or E:2 the direct product of the plant or a major component thereof, if such foreign produced direct product is subject to national security controls as identified on the U.S. Commerce Control List or is subject to State Department controls under the U.S. Munitions List.

**5. UNITED STATES GOVERNMENT RESTRICTED RIGHTS.** The enclosed Program (i) was developed solely at private expense; (ii) contains "restricted computer software" submitted with restricted rights in accordance with section 52.227-19 (a) through (d) of the Commercial Computer Software-Restricted Rights Clause and its successors, and (iii) in all respects is proprietary data belonging to Enterasys and/or its suppliers. For Department of Defense units, the Program is considered commercial computer software in accordance with DFARS section 227.7202-3 and its successors, and use, duplication, or disclosure by the Government is subject to restrictions set forth herein.

**6. DISCLAIMER OF WARRANTY.** EXCEPT FOR THOSE WARRANTIES EXPRESSLY PROVIDED TO YOU IN WRITING BY ENTERASYS, ENTERASYS DISCLAIMS ALL WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON- INFRINGEMENT WITH RESPECT TO THE PROGRAM. IF IMPLIED WARRANTIES MAY NOT BE DISCLAIMED BY APPLICABLE LAW, THEN ANY IMPLIED WARRANTIES ARE LIMITED IN DURATION TO THIRTY (30) DAYS AFTER DELIVERY OF THE PROGRAM TO YOU.

**7. LIMITATION OF LIABILITY.** IN NO EVENT SHALL ENTERASYS OR ITS SUPPLIERS BE LIABLE FOR ANY DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS, PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR RELIANCE DAMAGES, OR OTHER LOSS) ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM, EVEN IF ENTERASYS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THIS FOREGOING LIMITATION SHALL APPLY REGARDLESS OF THE CAUSE OF ACTION UNDER WHICH DAMAGES ARE SOUGHT.

THE CUMULATIVE LIABILITY OF ENTERASYS TO YOU FOR ALL CLAIMS RELATING TO THE PROGRAM, IN CONTRACT, TORT OR OTHERWISE, SHALL NOT EXCEED THE TOTAL AMOUNT OF FEES PAID TO ENTERASYS BY YOU FOR THE RIGHTS GRANTED HEREIN.

---

**8. AUDIT RIGHTS.** You hereby acknowledge that the intellectual property rights associated with the Program are of critical value to Enterasys and, accordingly, You hereby agree to maintain complete books, records and accounts showing (i) license fees due and paid, and (ii) the use, copying and deployment of the Program. You also grant to Enterasys and its authorized representatives, upon reasonable notice, the right to audit and examine during Your normal business hours, Your books, records, accounts and hardware devices upon which the Program may be deployed to verify compliance with this Agreement, including the verification of the license fees due and paid Enterasys and the use, copying and deployment of the Program. Enterasys' right of examination shall be exercised reasonably, in good faith and in a manner calculated to not unreasonably interfere with Your business. In the event such audit discovers non-compliance with this Agreement, including copies of the Program made, used or deployed in breach of this Agreement, You shall promptly pay to Enterasys the appropriate license fees. Enterasys reserves the right, to be exercised in its sole discretion and without prior notice, to terminate this license, effective immediately, for failure to comply with this Agreement. Upon any such termination, You shall immediately cease all use of the Program and shall return to Enterasys the Program and all copies of the Program.

**9. OWNERSHIP.** This is a license agreement and not an agreement for sale. You acknowledge and agree that the Program constitutes trade secrets and/or copyrighted material of Enterasys and/or its suppliers. You agree to implement reasonable security measures to protect such trade secrets and copyrighted material. All right, title and interest in and to the Program shall remain with Enterasys and/or its suppliers. All rights not specifically granted to You shall be reserved to Enterasys.

**10. ENFORCEMENT.** You acknowledge and agree that any breach of Sections 2, 4, or 9 of this Agreement by You may cause Enterasys irreparable damage for which recovery of money damages would be inadequate, and that Enterasys may be entitled to seek timely injunctive relief to protect Enterasys' rights under this Agreement in addition to any and all remedies available at law.

**11. ASSIGNMENT.** You may not assign, transfer or sublicense this Agreement or any of Your rights or obligations under this Agreement, except that You may assign this Agreement to any person or entity which acquires substantially all of Your stock or assets. Enterasys may assign this Agreement in its sole discretion. This Agreement shall be binding upon and inure to the benefit of the parties, their legal representatives, permitted transferees, successors and assigns as permitted by this Agreement. Any attempted assignment, transfer or sublicense in violation of the terms of this Agreement shall be void and a breach of this Agreement.

**12. WAIVER.** A waiver by Enterasys of a breach of any of the terms and conditions of this Agreement must be in writing and will not be construed as a waiver of any subsequent breach of such term or condition. Enterasys' failure to enforce a term upon Your breach of such term shall not be construed as a waiver of Your breach or prevent enforcement on any other occasion.

**13. SEVERABILITY.** In the event any provision of this Agreement is found to be invalid, illegal or unenforceable, the validity, legality and enforceability of any of the remaining provisions shall not in any way be affected or impaired thereby, and that provision shall be reformed, construed and enforced to the maximum extent permissible. Any such invalidity, illegality or unenforceability in any jurisdiction shall not invalidate or render illegal or unenforceable such provision in any other jurisdiction.

**14. TERMINATION.** Enterasys may terminate this Agreement immediately upon Your breach of any of the terms and conditions of this Agreement. Upon any such termination, You shall immediately cease all use of the Program and shall return to Enterasys the Program and all copies of the Program.



# Contents

|   |              |
|---|--------------|
| <b>About This Manual .....</b>              | <b>xxvii</b> |
| What's New (July 2004) .....                | xxvii        |
| Who Should Read This Manual? .....          | xxxiv        |
| How to Use This Manual .....                | xxxiv        |
| Related Documentation .....                 | xxxiv        |
| CLI Parameter Types .....                   | xxxv         |
| Command Syntax and Conventions .....        | xxxvii       |
| Getting Help .....                          | xxxviii      |
| <br><b>Chapter 1: acl Commands .....</b>    | <br><b>1</b> |
| Command Summary .....                       | 1            |
| acl apply interface .....                   | 3            |
| acl apply interface-are .....               | 7            |
| acl apply port.....                         | 9            |
| acl apply service.....                      | 12           |
| acl clearCounters.....                      | 15           |
| acl logging set deny-trap .....             | 16           |
| acl logging set syslog-only .....           | 17           |
| acl logging set deny-report-frequency ..... | 18           |
| acl permit deny appletalk nbp .....         | 19           |
| acl permit deny appletalk cable-range.....  | 21           |
| acl permit deny appletalk zone.....         | 23           |
| acl permit deny icmp .....                  | 25           |
| acl permit deny igmp.....                   | 27           |
| acl permit deny ip .....                    | 29           |
| acl permit deny ipv6.....                   | 32           |
| acl permit deny ip-protocol .....           | 34           |
| acl permit deny ipx .....                   | 36           |
| acl permit deny ipxgns .....                | 38           |
| acl permit deny ipxrip .....                | 40           |
| acl permit deny ipxsap.....                 | 42           |
| acl permit deny ipxtype20.....              | 44           |
| acl permit deny tcp .....                   | 45           |
| acl permit deny udp .....                   | 48           |
| acl-policy enable external .....            | 50           |
| acl show .....                              | 51           |

|  |               |
|--|---------------|
| <b>Chapter 2: acl-edit Commands.....</b>                     | <b>53</b>     |
| Command Summary.....   | 53            |
| acl-edit.....  | 54            |
| acl permit  deny .....                                       | 56            |
| delete .....   | 57            |
| exit.....  | 59            |
| move .....   | 61            |
| save.....  | 63            |
| show .....   | 65            |
| <br><b>Chapter 3: aging Commands .....</b>                   | <br><b>67</b> |
| Command Summary.....   | 67            |
| aging l2 disable.....  | 68            |
| aging l2 set aging-timeout .....                             | 70            |
| aging l2 show status .....                                   | 71            |
| aging l3 set timeout .....                                   | 72            |
| aging l3 set nat-flow-timeout .....                          | 73            |
| aging l3 show status .....                                   | 74            |
| <br><b>Chapter 4: appletalk Commands .....</b>               | <br><b>75</b> |
| Command Summary.....   | 75            |
| appletalk aarp clear.....                                    | 76            |
| appletalk aarp show.....                                     | 77            |
| appletalk ping .....   | 78            |
| appletalk qos internal-queue-priority .....                  | 80            |
| appletalk show aarp-globals .....                            | 81            |
| appletalk show interfaces .....                              | 82            |
| appletalk show routes .....                                  | 83            |
| appletalk show rtmp .....                                    | 84            |
| appletalk show zip-query-interval.....                       | 85            |
| appletalk show zone interface .....                          | 86            |
| appletalk show zone network .....                            | 87            |
| <br><b>Chapter 5: appletalk Configuration Commands .....</b> | <br><b>89</b> |
| Command Summary.....   | 89            |
| appletalk add aarp.....                                      | 91            |
| appletalk add route .....                                    | 92            |
| appletalk aarp interval .....                                | 94            |
| appletalk aarp timeout .....                                 | 95            |
| appletalk checksum disable .....                             | 96            |
| appletalk rtmp jitter .....                                  | 97            |
| appletalk rtmp update-disable .....                          | 98            |
| appletalk rtmp update-interval .....                         | 99            |
| appletalk rtmp valid-interval .....                          | 100           |
| appletalk split-horizon disable .....                        | 101           |
| appletalk zip query-interval.....                            | 102           |

---

|                                |            |
|--------------------------------|------------|
| <b>Chapter 6: are Commands</b> | <b>103</b> |
| Command Summary                | 103        |
| are enable protocol appletalk  | 104        |
| are-config                     | 106        |
| system are-promimage upgrade   | 107        |
| <b>Chapter 7: arp Commands</b> | <b>109</b> |
| Command Summary                | 109        |
| arp add                        | 110        |
| arp clear                      | 112        |
| arp set drop-unresolved        | 114        |
| arp set interface              | 116        |
| arp set max-unresolved         | 117        |
| arp set unresolve-threshold    | 119        |
| arp set unresolve-timer        | 120        |
| arp show                       | 121        |
| <b>Chapter 8: atm Commands</b> | <b>123</b> |
| Command Summary                | 123        |
| atm apply service              | 124        |
| atm create vcl port            | 126        |
| atm define service             | 128        |
| atm set peer-addr              | 131        |
| atm set port cell-mapping      | 133        |
| atm set port pdh-cell-scramble | 134        |
| atm set port vpi-bits          | 136        |
| atm set vcl                    | 138        |
| atm show                       | 139        |
| <b>Chapter 9: bgp Commands</b> | <b>143</b> |
| Command Summary                | 143        |
| bgp add network                | 145        |
| bgp add peer-host              | 146        |
| bgp clear peer-host            | 147        |
| bgp create peer-group          | 148        |
| bgp set bad-aspath             | 150        |
| bgp set cluster-id             | 151        |
| bgp set dampenflap             | 152        |
| bgp set default-metric         | 154        |
| bgp set internal-set-pref      | 155        |
| bgp set multipath              | 156        |
| bgp set peer-group             | 157        |
| bgp set peer-host              | 161        |
| bgp set preference             | 165        |
| bgp show aspaths               | 166        |
| bgp show cidr-only             | 167        |
| bgp show community             | 169        |
| bgp show flap-statistics       | 171        |
| bgp show peer-as               | 173        |
| bgp show peer-group-type       | 174        |

|   |            |
|---|------------|
| bgp show peer-host.....                   | 175        |
| bgp show regexp.....                      | 177        |
| bgp show routes.....                      | 179        |
| bgp show summary.....                     | 180        |
| bgp show sync-tree.....                   | 181        |
| bgp start stop.....                       | 184        |
| bgp trace .....                           | 185        |
| <b>Chapter 10: cdp Commands .....</b>     | <b>189</b> |
| Command Summary.....                      | 189        |
| cdp set global-status .....               | 190        |
| cdp set transmit-frequency .....          | 191        |
| cdp set authentication-code .....         | 192        |
| cdp set port-status.....                  | 193        |
| cdp show neighbors.....                   | 194        |
| cdp show global-info.....                 | 196        |
| cdp show stats.....                       | 197        |
| cdp show port-status.....                 | 198        |
| <b>Chapter 11: cli Commands .....</b>     | <b>201</b> |
| Command Summary.....                      | 201        |
| cli search command.....                   | 202        |
| cli set command completion.....           | 205        |
| cli set common .....                      | 206        |
| cli set history .....                     | 207        |
| cli set terminal .....                    | 208        |
| cli show history .....                    | 209        |
| cli show terminal .....                   | 210        |
| cli terminal monitor.....                 | 211        |
| <b>Chapter 12: comment Commands.....</b>  | <b>213</b> |
| Command Summary.....                      | 213        |
| comment in.....                           | 214        |
| comment line .....                        | 216        |
| comment move .....                        | 218        |
| comment out.....                          | 219        |
| <b>Chapter 13: configure Command.....</b> | <b>221</b> |
| <b>Chapter 14: copy Command.....</b>      | <b>223</b> |
| <b>Chapter 15: dhcp Commands.....</b>     | <b>227</b> |
| Command Summary.....                      | 227        |
| dhcp attach superscope.....               | 228        |
| dhcp define parameters.....               | 229        |
| dhcp define pool .....                    | 231        |
| dhcp define static-ip .....               | 233        |
| dhcp flush .....                          | 235        |
| dhcp global set commit-interval.....      | 236        |
| dhcp global set lease-database.....       | 237        |



---

|   |            |
|---|------------|
| dhcp show binding .....                 | 238        |
| dhcp show num-clients.....              | 240        |
| <b>Chapter 16: diff Command .....</b>   | <b>241</b> |
| <b>Chapter 17: dvmrp Commands .....</b> | <b>243</b> |
| Command Summary .....                   | 243        |
| dvmrp create tunnel.....                | 244        |
| dvmrp enable interface.....             | 246        |
| dvmrp enable tunnel.....                | 248        |
| dvmrp set interface .....               | 249        |
| dvmrp set neighbor-timeout .....        | 251        |
| dvmrp set prunetime.....                | 252        |
| dvmrp show .....                        | 253        |
| dvmrp start .....                       | 255        |
| dvmrp trace .....                       | 256        |
| dvmrp trace local-options.....          | 257        |
| <b>Chapter 18: enable Command .....</b> | <b>259</b> |
| <b>Chapter 19: erase Command .....</b>  | <b>261</b> |
| <b>Chapter 20: exit Command.....</b>    | <b>263</b> |
| <b>Chapter 21: fddi Commands .....</b>  | <b>265</b> |
| Command Summary .....                   | 265        |
| fddi reset.....                         | 267        |
| fddi set fddi-mode .....                | 268        |
| fddi set fddi-fdx-mode .....            | 270        |
| fddi set mac-group .....                | 271        |
| fddi set mac-restricted-token.....      | 273        |
| fddi set path-group .....               | 275        |
| fddi set port-group.....                | 277        |
| fddi set ring-purger.....               | 279        |
| fddi set smt-group .....                | 280        |
| fddi set translation.....               | 282        |
| fddi show fddi-mode .....               | 284        |
| fddi show fddi-status .....             | 285        |
| fddi show fddi-fdx-mode .....           | 286        |
| fddi show mac-group .....               | 288        |
| fddi show mac-restricted token .....    | 289        |
| fddi show media-type.....               | 290        |
| fddi show path-group .....              | 291        |
| fddi show port-group.....               | 293        |
| fddi show ring-purger.....              | 295        |
| fddi show smt-config .....              | 296        |
| fddi show smt-group .....               | 298        |
| fddi show translation .....             | 300        |
| fddi show version .....                 | 301        |

|   |            |
|---|------------|
| <b>Chapter 22: file Commands .....</b>          | <b>303</b> |
| Command Summary .....                           | 303        |
| file copy .....                                 | 304        |
| file delete .....                               | 306        |
| file dir .....                                  | 308        |
| file rename .....                               | 310        |
| file type .....                                 | 312        |
| <b>Chapter 23: filters Commands .....</b>       | <b>315</b> |
| Command Summary .....                           | 316        |
| filters add address-filter .....                | 317        |
| filters add port-address-lock .....             | 318        |
| filters add secure-port .....                   | 319        |
| filters add static-entry .....                  | 320        |
| filters show address-filter .....               | 322        |
| filters show port-address-lock .....            | 323        |
| filters show secure-port .....                  | 324        |
| filters show static-entry .....                 | 325        |
| <b>Chapter 24: frame-relay Commands .....</b>   | <b>327</b> |
| Command Summary .....                           | 327        |
| frame-relay apply service ports .....           | 329        |
| frame-relay clear stats-counter .....           | 330        |
| frame-relay create vc .....                     | 332        |
| frame-relay define service .....                | 333        |
| frame-relay set fr-encaps-bgd .....             | 336        |
| frame-relay set lmi .....                       | 337        |
| frame-relay set payload-compress .....          | 339        |
| frame-relay set peer-addr .....                 | 340        |
| frame-relay show service .....                  | 341        |
| frame-relay show stats .....                    | 342        |
| frame-relay show stats summary .....            | 344        |
| <b>Chapter 25: garp Commands .....</b>          | <b>345</b> |
| Command Summary .....                           | 345        |
| garp set timers .....                           | 346        |
| garp show timers .....                          | 347        |
| <b>Chapter 26: gvrp Commands .....</b>          | <b>349</b> |
| Command Summary .....                           | 349        |
| gvrp show statistics .....                      | 350        |
| gvrp show status .....                          | 351        |
| gvrp show registration-mode .....               | 352        |
| gvrp show applicant-status .....                | 353        |
| gvrp clear statistics .....                     | 354        |
| gvrp enable dynamic-vlan-creation .....         | 355        |
| gvrp enable ports .....                         | 356        |
| gvrp set registration-mode forbidden .....      | 357        |
| gvrp set applicant-status non-participant ..... | 358        |
| gvrp start .....                                | 359        |

---

|   |                |
|---|----------------|
| <b>Chapter 27: igmp Commands.....</b>           | <b>361</b>     |
| Command Summary .....                           | 361            |
| igmp enable interface .....                     | 362            |
| igmp enable vlan .....                          | 364            |
| igmp join group .....                           | 365            |
| igmp set .....                                  | 366            |
| igmp set vlan .....                             | 368            |
| igmp show groups .....                          | 370            |
| igmp show interfaces .....                      | 371            |
| igmp show vlans.....                            | 372            |
| igmp start stop .....                           | 373            |
| igmp start-snooping.....                        | 374            |
| igmp trace.....                                 | 375            |
| igmp trace local-options.....                   | 377            |
| <br><b>Chapter 28: interface Commands .....</b> | <br><b>379</b> |
| Command Summary .....                           | 379            |
| interface add appletalk .....                   | 381            |
| interface add ip.....                           | 383            |
| interface add ipv6.....                         | 385            |
| interface add ipx.....                          | 387            |
| interface create appletalk .....                | 389            |
| interface create appletalk noseed .....         | 392            |
| interface create ip .....                       | 394            |
| interface create ipv6 .....                     | 399            |
| interface create ipx .....                      | 404            |
| interface show appletalk.....                   | 409            |
| interface show ip .....                         | 411            |
| interface show ipv6 .....                       | 413            |
| interface show ipx .....                        | 415            |
| <br><b>Chapter 29: ip Commands .....</b>        | <br><b>417</b> |
| Command Summary .....                           | 417            |
| ip add route.....                               | 419            |
| ip clear reverse-flows .....                    | 422            |
| ip disable .....                                | 423            |
| ip dos disable.....                             | 425            |
| ip enable .....                                 | 427            |
| ip helper-address .....                         | 430            |
| ip l3-hash.....                                 | 432            |
| ip set port forwarding-mode.....                | 434            |
| ip show connections .....                       | 436            |
| ip show hash-variant .....                      | 438            |
| ip show helper-address.....                     | 440            |
| ip show interfaces.....                         | 442            |
| ip show reverse-flows .....                     | 444            |
| ip show routes .....                            | 445            |

|  |            |
|--|------------|
| <b>Chapter 30: ipv6 Commands .....</b>                 | <b>449</b> |
| Command Summary .....                                  | 449        |
| ipv6 add route .....                                   | 450        |
| ipv6 set icmp-rate-limit .....                         | 453        |
| ipv6 disable icmp-redirect .....                       | 454        |
| ipv6 show interfaces .....                             | 455        |
| ipv6 show routes .....                                 | 457        |
| <b>Chapter 31: ip-policy Commands .....</b>            | <b>461</b> |
| Command Summary .....                                  | 461        |
| ip-policy apply .....                                  | 462        |
| ip-policy clear .....                                  | 464        |
| ip-policy deny .....                                   | 465        |
| ip-policy permit .....                                 | 467        |
| ip-policy set .....                                    | 470        |
| ip-policy show .....                                   | 472        |
| <b>Chapter 32: ip-redundancy (vrrp) Commands .....</b> | <b>475</b> |
| Command Summary .....                                  | 475        |
| ip-redundancy associate .....                          | 477        |
| ip-redundancy clear vrrp-stats .....                   | 479        |
| ip-redundancy create .....                             | 480        |
| ip-redundancy set .....                                | 481        |
| ip-redundancy show .....                               | 484        |
| ip-redundancy start vrrp .....                         | 487        |
| ip-redundancy trace .....                              | 488        |
| <b>Chapter 33: ip-router Commands .....</b>            | <b>489</b> |
| Command Summary .....                                  | 490        |
| ip-router authentication add key-chain .....           | 493        |
| ip-router authentication create key-chain .....        | 494        |
| ip-router find route .....                             | 495        |
| ip-router global add .....                             | 496        |
| ip-router global set .....                             | 497        |
| ip-router global set trace-level .....                 | 499        |
| ip-router global set trace-options .....               | 500        |
| ip-router global set trace-state .....                 | 501        |
| ip-router global use provided_config .....             | 502        |
| ip-router kernel trace .....                           | 503        |
| ip-router policy add filter .....                      | 504        |
| ip-router policy add optional-attributes-list .....    | 506        |
| ip-router policy aggr-gen destination .....            | 508        |
| ip-router policy create aggr-export-source .....       | 510        |
| ip-router policy create aggr-gen-dest .....            | 511        |
| ip-router policy create aggr-gen-source .....          | 512        |
| ip-router policy create aspath-export-source .....     | 514        |
| ip-router policy create bgp-export-destination .....   | 516        |
| ip-router policy create bgp-export-source .....        | 517        |
| ip-router policy create bgp-import-source .....        | 518        |
| ip-router policy create direct-export-source .....     | 520        |

---

|   |            |
|---|------------|
| ip-router policy create filter .....                      | 521        |
| ip-router policy create optional-attributes-list .....    | 523        |
| ip-router policy create ospfase-export-source .....       | 525        |
| ip-router policy create ospf-export-destination .....     | 526        |
| ip-router policy create ospf-export-source .....          | 527        |
| ip-router policy create ospf-import-source .....          | 528        |
| ip-router policy create ospfnssa-export-destination ..... | 529        |
| ip-router policy create redirect-import-source .....      | 530        |
| ip-router policy create rip-export-destination .....      | 531        |
| ip-router policy create rip-export-source .....           | 532        |
| ip-router policy create rip-import-source .....           | 533        |
| ip-router policy create static-export-source .....        | 535        |
| ip-router policy create tag-export-source .....           | 536        |
| ip-router policy export destination .....                 | 537        |
| ip-router policy import source .....                      | 540        |
| ip-router policy redistribute .....                       | 543        |
| ip-router policy summarize route .....                    | 545        |
| ip-router set .....                                       | 547        |
| ip-router set trace-options .....                         | 548        |
| ip-router show configuration file .....                   | 549        |
| ip-router show rib .....                                  | 550        |
| ip-router show route .....                                | 552        |
| ip-router show state .....                                | 555        |
| <br><b>Chapter 34: ipv6-router Commands .....</b>         | <b>557</b> |
| Command Summary .....                                     | 557        |
| ipv6-router find route .....                              | 559        |
| ipv6-router policy redistribute .....                     | 561        |
| ipv6-router show route .....                              | 562        |
| <br><b>Chapter 35: ipx Commands .....</b>                 | <b>565</b> |
| Command Summary .....                                     | 565        |
| ipx add route .....                                       | 567        |
| ipx add sap .....   | 568        |
| ipx find rip .....  | 569        |
| ipx find sap .....  | 570        |
| ipx l3-hash .....   | 572        |
| ipx set interface .....                                   | 574        |
| ipx set rip .....   | 575        |
| ipx set ripreq .....                                      | 576        |
| ipx set sap .....   | 577        |
| ipx set sapgns .....                                      | 578        |
| ipx set type20 propagation .....                          | 579        |
| ipx set port .....  | 580        |
| ipx show buffers .....                                    | 581        |
| ipx show hash-variant .....                               | 582        |
| ipx show interfaces .....                                 | 584        |
| ipx show rib destination .....                            | 586        |
| ipx show servers .....                                    | 587        |
| ipx show summary .....                                    | 588        |

|   |            |
|---|------------|
| ipx show routes.....                          | 589        |
| ipx show packets-per-iteration .....          | 590        |
| <b>Chapter 36: l2-tables Commands.....</b>    | <b>591</b> |
| Command Summary.....                          | 591        |
| l2-tables show all-flows .....                | 592        |
| l2-tables show all-macs .....                 | 594        |
| l2-tables show bridge-management.....         | 595        |
| l2-tables show igmp-mcast-registrations.....  | 596        |
| l2-tables show mac .....                      | 597        |
| l2-tables show mac-table-stats .....          | 598        |
| l2-tables show port-macs.....                 | 599        |
| l2-tables show vlan-igmp-status.....          | 601        |
| l2-tables show system-macs .....              | 603        |
| <b>Chapter 37: load-balance Commands.....</b> | <b>605</b> |
| Command Summary.....                          | 605        |
| load-balance add host-to-group .....          | 607        |
| load-balance add host-to-vip-range.....       | 609        |
| load-balance allow access-to-servers .....    | 611        |
| load-balance create group-name.....           | 613        |
| load-balance create vip-range-name.....       | 615        |
| load-balance set aging-for-src-maps .....     | 617        |
| load-balance set client-proxy-subnet.....     | 618        |
| load-balance set ftp-control-port .....       | 619        |
| load-balance set group-options.....           | 620        |
| load-balance set group-conn-thresh .....      | 622        |
| load-balance set hash-variant .....           | 623        |
| load-balance set mappings-age-timer.....      | 624        |
| load-balance set policy-for-group .....       | 625        |
| load-balance set server-status .....          | 627        |
| load-balance set server-options .....         | 629        |
| load-balance set vpn-dest-port .....          | 631        |
| load-balance show acv-options .....           | 632        |
| load-balance show hash-stats .....            | 633        |
| load-balance show source-mappings.....        | 635        |
| load-balance show statistics .....            | 637        |
| load-balance show virtual-hosts .....         | 639        |
| <b>Chapter 38: logout Command .....</b>       | <b>641</b> |
| <b>Chapter 39: mstp Commands.....</b>         | <b>643</b> |
| Command Summary.....                          | 643        |
| mstp start .....                              | 645        |
| mstp create msti.....                         | 646        |
| mstp disable edge-auto-detection .....        | 647        |
| mstp enable legacy-path-cost .....            | 648        |
| mstp enable per-port-hello-mode .....         | 650        |
| mstp enable port .....                        | 651        |
| mstp map vlan .....                           | 652        |

|  |            |
|--|------------|
| mstp set bridging forward-delay .....      | 653        |
| mstp set bridging hello-time .....         | 654        |
| mstp set bridging max-age .....            | 655        |
| mstp set bridging max-hops .....           | 656        |
| mstp set bridging priority .....           | 657        |
| mstp set configuration-id .....            | 658        |
| mstp set port .....                        | 659        |
| mstp set version .....                     | 661        |
| mstp show bpdu-stats msti port .....       | 662        |
| mstp show bridging .....                   | 664        |
| mstp show instances .....                  | 665        |
| mstp show map .....                        | 666        |
| mstp show stats msti .....                 | 667        |
| <b>Chapter 40: multicast Commands.....</b> | <b>669</b> |
| Command Summary .....                      | 669        |
| multicast show mfc .....                   | 670        |
| multicast show sg-counts .....             | 671        |
| multicast show vif .....                   | 672        |
| <b>Chapter 41: nat Commands.....</b>       | <b>673</b> |
| Command Summary .....                      | 673        |
| nat clear-err-stats .....                  | 675        |
| nat create dynamic .....                   | 676        |
| nat create static .....                    | 678        |
| nat flush-dynamic-binding .....            | 680        |
| nat set dns-name-extension-error .....     | 682        |
| nat set dns-session-timeout .....          | 683        |
| nat set dynamic-binding-timeout .....      | 684        |
| nat set ftp-control-port .....             | 685        |
| nat set ftp-session-timeout .....          | 687        |
| nat set interface .....                    | 688        |
| nat set secure-plus .....                  | 690        |
| nat show .....                             | 691        |
| <b>Chapter 42: ndisc Commands .....</b>    | <b>695</b> |
| Command Summary .....                      | 695        |
| ndisc set interface .....                  | 697        |
| ndisc show interface .....                 | 701        |
| ndisc add prefix .....                     | 703        |
| ndisc show prefix .....                    | 707        |
| ndisc add neighbor .....                   | 710        |
| ndisc clear neighbor .....                 | 712        |
| ndisc show neighbor .....                  | 714        |
| ndisc set dad-attempts .....               | 717        |
| ndisc show dad-attempts .....              | 719        |
| <b>Chapter 43: negate Command.....</b>     | <b>721</b> |

|  |            |
|--|------------|
| <b>Chapter 44: netflow Commands.....</b> | <b>723</b> |
| Command Summary.....                     | 723        |
| netflow clear statistics .....           | 724        |
| netflow enable .....                     | 725        |
| netflow set collector .....              | 726        |
| netflow set engine.....                  | 727        |
| netflow set flow-destination-port .....  | 728        |
| netflow set interval .....               | 729        |
| netflow set memory.....                  | 730        |
| netflow set ports .....                  | 731        |
| netflow show .....                       | 732        |
| <b>Chapter 45: no Command.....</b>       | <b>735</b> |
| <b>Chapter 46: ntp Commands.....</b>     | <b>737</b> |
| Command Summary.....                     | 737        |
| ntp set server.....                      | 738        |
| ntp show all .....                       | 740        |
| ntp synchronize server.....              | 741        |
| <b>Chapter 47: ospf Commands .....</b>   | <b>743</b> |
| Command Summary.....                     | 743        |
| ospf add interface .....                 | 745        |
| ospf add nbma-neighbor.....              | 746        |
| ospf add network   summary-range .....   | 747        |
| ospf add nssa-network.....               | 749        |
| ospf add pmp-neighbor.....               | 750        |
| ospf add stub-host.....                  | 751        |
| ospf add stub-network .....              | 752        |
| ospf add summary-filter .....            | 753        |
| ospf add virtual-link .....              | 755        |
| ospf create area.....                    | 756        |
| ospf log router-lsas .....               | 757        |
| ospf set advertise-subnet .....          | 758        |
| ospf set always-update-summary .....     | 759        |
| ospf set area.....                       | 760        |
| ospf set ase-defaults .....              | 762        |
| ospf set authentication-method.....      | 763        |
| ospf set hello-interval .....            | 764        |
| ospf set interface.....                  | 765        |
| ospf set nssa-defaults.....              | 768        |
| ospf set opaque-capability .....         | 769        |
| ospf set poll-interval .....             | 770        |
| ospf set priority.....                   | 771        |
| ospf set retransmit-interval.....        | 772        |
| ospf set rfc1583 on .....                | 773        |
| ospf set router-dead-interval.....       | 774        |
| ospf set transit-delay.....              | 775        |
| ospf set-trap .....                      | 776        |
| ospf set virtual-link.....               | 778        |



|  |            |
|--|------------|
| ospf show .....                              | 780        |
| ospf start stop .....                        | 783        |
| ospf trace .....                             | 784        |
| <b>Chapter 48: pim Commands.....</b>         | <b>787</b> |
| Command Summary .....                        | 787        |
| pim global .....                             | 789        |
| pim global set defaults .....                | 790        |
| pim global trace.....                        | 792        |
| pim global trace local-options.....          | 794        |
| pim show active-rps .....                    | 796        |
| pim show all .....                           | 797        |
| pim show bsr .....                           | 798        |
| pim show crp.....                            | 799        |
| pim show errors.....                         | 800        |
| pim show interface .....                     | 801        |
| pim show neighbor.....                       | 802        |
| pim show periodic-jp .....                   | 803        |
| pim show route.....                          | 804        |
| pim show rp-hash .....                       | 806        |
| pim show rp-set .....                        | 807        |
| pim show timers .....                        | 808        |
| pim sparse add crp-group.....                | 809        |
| pim sparse add interface.....                | 810        |
| pim sparse add static-rp.....                | 811        |
| pim sparse create component .....            | 812        |
| pim sparse set component .....               | 813        |
| pim sparse set interface .....               | 816        |
| <b>Chapter 49: ping Command .....</b>        | <b>819</b> |
| ping.....                                    | 819        |
| <b>Chapter 50: port Commands .....</b>       | <b>825</b> |
| Command Summary .....                        | 825        |
| port auto-negotiate .....                    | 827        |
| port bmon .....                              | 828        |
| port description .....                       | 831        |
| port disable.....                            | 832        |
| port enable 8021p.....                       | 833        |
| port flow-bridging.....                      | 834        |
| port enabled forced-return-flows .....       | 836        |
| port set.....                                | 837        |
| port show 8021p.....                         | 844        |
| port show autonegotiation.....               | 845        |
| port show autonegotiation-capabilities ..... | 846        |
| port show bmon.....                          | 848        |
| port show bridging-status.....               | 851        |
| port show description.....                   | 852        |
| port show hash-mode .....                    | 853        |
| port show MAU .....                          | 854        |

|   |            |
|---|------------|
| port show MAU-statistics.....                     | 855        |
| port show mc-vlan-encap .....                     | 856        |
| port show mirroring-status .....                  | 857        |
| port show port-status .....                       | 858        |
| port show pvst-info.....                          | 860        |
| port show serial-link-info .....                  | 862        |
| port show stp-info.....                           | 863        |
| port show vlan-info .....                         | 865        |
| <b>Chapter 51: port-list Commands.....</b>        | <b>867</b> |
| Command Summary.....                              | 867        |
| port-list compress .....                          | 868        |
| port-list expand.....                             | 870        |
| <b>Chapter 52: port mirroring Command .....</b>   | <b>873</b> |
| port mirroring .....                              | 873        |
| <b>Chapter 53: ppp Commands.....</b>              | <b>877</b> |
| Command Summary.....                              | 877        |
| ppp add-to-mlp .....                              | 879        |
| ppp apply service.....                            | 880        |
| ppp clear stats-counter.....                      | 881        |
| ppp create-mlp.....                               | 882        |
| ppp define service.....                           | 883        |
| ppp restart lcp-ncp.....                          | 886        |
| ppp set mlp-encaps-format .....                   | 887        |
| ppp set mlp-frag-size .....                       | 888        |
| ppp set mlp-fragq-depth .....                     | 889        |
| ppp set mlp-orderq-depth .....                    | 890        |
| ppp set payload-compress .....                    | 891        |
| ppp set payload-encrypt .....                     | 892        |
| ppp set peer-addr .....                           | 893        |
| ppp set ppp-encaps-bgd.....                       | 894        |
| ppp show mlp .....                                | 895        |
| ppp show service .....                            | 896        |
| ppp show stats .....                              | 897        |
| <b>Chapter 54: pvst Commands .....</b>            | <b>899</b> |
| Command Summary.....                              | 899        |
| pvst create spanningtree .....                    | 900        |
| pvst enable port spanning-tree.....               | 901        |
| pvst set bridging spanning-tree .....             | 902        |
| pvst set port .....                               | 904        |
| pvst show bridging-info spanning-tree.....        | 906        |
| pvst reset-rstp spanning-tree.....                | 907        |
| pvst set protocol-version rstp spanning-tree..... | 908        |
| pvst set no-special-encap.....                    | 909        |

|  |            |
|--|------------|
| <b>Chapter 55: qos Commands.....</b>       | <b>911</b> |
| Command Summary .....                      | 912        |
| qos apply priority-map .....               | 914        |
| qos create priority-map .....              | 915        |
| qos precedence ip .....                    | 917        |
| qos precedence ipx .....                   | 919        |
| qos priority-map off .....                 | 921        |
| qos wred input .....                       | 922        |
| qos set ip.....                            | 924        |
| qos set ipx.....                           | 927        |
| qos set l2.....                            | 930        |
| qos set queuing-policy .....               | 932        |
| qos set weighted-fair .....                | 933        |
| qos show ip.....                           | 934        |
| qos show ipx.....                          | 935        |
| qos show l2.....                           | 936        |
| qos show precedence.....                   | 938        |
| qos show priority-map .....                | 939        |
| qos show wred.....                         | 940        |
| qos show wfq .....                         | 941        |
| <b>Chapter 56: radius Commands .....</b>   | <b>943</b> |
| Command Summary .....                      | 943        |
| radius accounting command level.....       | 944        |
| radius accounting shell.....               | 945        |
| radius accounting snmp.....                | 946        |
| radius accounting system .....             | 947        |
| radius authentication .....                | 948        |
| radius enable .....                        | 949        |
| radius set .....                           | 950        |
| radius set server.....                     | 952        |
| radius show .....                          | 954        |
| <b>Chapter 57: rarpd Commands .....</b>    | <b>957</b> |
| Command Summary .....                      | 957        |
| rarpd add .....                            | 958        |
| rarpd set interface.....                   | 959        |
| rarpd show.....                            | 960        |
| <b>Chapter 58: rate-limit Command.....</b> | <b>961</b> |
| Command Summary .....                      | 962        |
| rate-limit aggregate acl.....              | 963        |
| rate-limit apply .....                     | 966        |
| rate-limit flow-aggregate.....             | 967        |
| rate-limit input acl.....                  | 970        |
| rate-limit port-level input .....          | 973        |
| rate-limit port-level slot .....           | 976        |
| rate-limit port-level output .....         | 977        |
| rate-limit show .....                      | 978        |
| rate-limit vlan port .....                 | 981        |

|   |             |
|---|-------------|
| <b>Chapter 59: rdisc Commands .....</b> | <b>985</b>  |
| Command Summary .....                   | 985         |
| rdisc add address .....                 | 986         |
| rdisc add interface .....               | 987         |
| rdisc set address .....                 | 988         |
| rdisc set interface .....               | 990         |
| rdisc show .....                        | 992         |
| rdisc start .....                       | 994         |
| <b>Chapter 60: reboot Command .....</b> | <b>995</b>  |
| <b>Chapter 61: rip Commands .....</b>   | <b>997</b>  |
| Command Summary .....                   | 997         |
| rip add .....                           | 999         |
| rip set auto-summary .....              | 1001        |
| rip set broadcast-state .....           | 1002        |
| rip set check-zero .....                | 1003        |
| rip set check-zero-metric .....         | 1004        |
| rip set default-metric .....            | 1005        |
| rip set interface .....                 | 1006        |
| rip set max-routes .....                | 1009        |
| rip set multipath .....                 | 1010        |
| rip set poison-reverse .....            | 1011        |
| rip set preference .....                | 1012        |
| rip show .....                          | 1013        |
| rip start .....                         | 1016        |
| rip stop .....                          | 1017        |
| rip trace .....                         | 1018        |
| <b>Chapter 62: ripng Commands .....</b> | <b>1021</b> |
| Command Summary .....                   | 1021        |
| ripng add interface .....               | 1023        |
| ripng set default-metric .....          | 1024        |
| ripng set expire-time .....             | 1025        |
| ripng set interface .....               | 1026        |
| ripng set poison-reverse .....          | 1028        |
| ripng set preference .....              | 1029        |
| ripng set update-time .....             | 1030        |
| ripng show .....                        | 1031        |
| ripng start .....                       | 1033        |
| ripng trace .....                       | 1034        |
| <b>Chapter 63: rmon Commands .....</b>  | <b>1037</b> |
| Command Summary .....                   | 1037        |
| rmon address-map .....                  | 1040        |
| rmon al-matrix-top-n .....              | 1042        |
| rmon alarm .....                        | 1044        |
| rmon apply cli-filters .....            | 1047        |
| rmon capture .....                      | 1049        |
| rmon channel .....                      | 1051        |

---

|                                       |      |
|---------------------------------------|------|
| rmon clear cli-filter .....           | 1053 |
| rmon enable .....                     | 1054 |
| rmon etherstats .....                 | 1055 |
| rmon event .....                      | 1056 |
| rmon filter .....                     | 1058 |
| rmon history .....                    | 1060 |
| rmon hl-host .....                    | 1062 |
| rmon hl-matrix .....                  | 1064 |
| rmon host .....                       | 1066 |
| rmon host-top-n .....                 | 1067 |
| rmon matrix .....                     | 1069 |
| rmon nl-matrix-top-n .....            | 1071 |
| rmon protocol-distribution .....      | 1073 |
| rmon set .....                        | 1074 |
| rmon set cli-filter .....             | 1077 |
| rmon set memory .....                 | 1080 |
| rmon set ports .....                  | 1082 |
| rmon set protocol-directory .....     | 1083 |
| rmon show address-map-logs .....      | 1085 |
| rmon show address-map-control .....   | 1087 |
| rmon show al-host .....               | 1088 |
| rmon show al-matrix .....             | 1090 |
| rmon show al-matrix-top-n .....       | 1092 |
| rmon show alarms .....                | 1094 |
| rmon show channels .....              | 1095 |
| rmon show cli-filters .....           | 1096 |
| rmon show etherstats .....            | 1098 |
| rmon show events .....                | 1100 |
| rmon show filters .....               | 1102 |
| rmon show history .....               | 1103 |
| rmon show host-top-n .....            | 1105 |
| rmon show hosts .....                 | 1107 |
| rmon show matrix .....                | 1110 |
| rmon show nl-host .....               | 1113 |
| rmon show nl-matrix .....             | 1115 |
| rmon show nl-matrix-top-n .....       | 1117 |
| rmon show packet-capture .....        | 1119 |
| rmon show probe-config .....          | 1120 |
| rmon show protocol-directory .....    | 1121 |
| rmon show protocol-distribution ..... | 1123 |
| rmon show status .....                | 1125 |
| rmon show user-history .....          | 1127 |
| rmon user-history-apply .....         | 1128 |
| rmon user-history-control .....       | 1129 |
| rmon user-history-objects .....       | 1130 |

|   |             |
|---|-------------|
| <b>Chapter 64: sam Commands .....</b>       | <b>1131</b> |
| Command Summary.....                        | 1131        |
| sam clear.....                              | 1132        |
| sam enable .....                            | 1133        |
| sam set activation-delay .....              | 1134        |
| sam set deactivation-delay .....            | 1135        |
| sam set rate-limit .....                    | 1136        |
| sam show history .....                      | 1137        |
| sam show statistics .....                   | 1139        |
| sam show status .....                       | 1140        |
| <b>Chapter 65: save Command.....</b>        | <b>1141</b> |
| <b>Chapter 66: search Command.....</b>      | <b>1143</b> |
| search.....                                 | 1143        |
| <b>Chapter 67: show Command .....</b>       | <b>1145</b> |
| <b>Chapter 68: smarttrunk Commands.....</b> | <b>1149</b> |
| Command Summary.....                        | 1149        |
| smarttrunk add ports.....                   | 1150        |
| smarttrunk clear load-distribution .....    | 1152        |
| smarttrunk create .....                     | 1153        |
| smarttrunk lacp actor-parameters .....      | 1155        |
| smarttrunk lacp aggregator.....             | 1157        |
| smarttrunk set load-policy.....             | 1158        |
| smarttrunk show .....                       | 1159        |
| <b>Chapter 69: snmp Commands .....</b>      | <b>1161</b> |
| Command Summary.....                        | 1161        |
| snmp disable trap.....                      | 1163        |
| snmp disable port-trap.....                 | 1164        |
| snmp set chassis-id .....                   | 1165        |
| snmp set community.....                     | 1166        |
| snmp set community-to-group .....           | 1168        |
| snmp set filter .....                       | 1169        |
| snmp set group .....                        | 1171        |
| snmp set if-alias.....                      | 1173        |
| snmp set mib.....                           | 1175        |
| snmp set notify .....                       | 1178        |
| snmp set retro-mib-ifspeed.....             | 1179        |
| snmp set target.....                        | 1180        |
| snmp set target-params.....                 | 1183        |
| snmp set trap-source .....                  | 1185        |
| snmp set user .....                         | 1186        |
| snmp set user-to-group .....                | 1188        |
| snmp set view .....                         | 1189        |
| snmp show.....                              | 1190        |
| snmp stop.....                              | 1201        |
| snmp test trap .....                        | 1202        |

|  |                 |
|--|-----------------|
| <b>Chapter 70: sonet Commands .....</b>          | <b>1203</b>     |
| Command Summary .....                            | 1203            |
| sonet set C2 .....                               | 1205            |
| sonet set circuit-id .....                       | 1207            |
| sonet set fcs-16-bit .....                       | 1208            |
| sonet set framing .....                          | 1209            |
| sonet set J0 .....                               | 1210            |
| sonet set loopback .....                         | 1212            |
| sonet set path-trace .....                       | 1213            |
| sonet set payload-scramble .....                 | 1214            |
| sonet set protected-by .....                     | 1215            |
| sonet set protection .....                       | 1216            |
| sonet set protection-switch .....                | 1218            |
| sonet set revertive .....                        | 1220            |
| sonet set S1S0 .....                             | 1222            |
| sonet set sd-ber .....                           | 1224            |
| sonet set sf-ber .....                           | 1225            |
| sonet set sts-stream-scramble .....              | 1226            |
| sonet set WTR-timer .....                        | 1227            |
| sonet show aps .....                             | 1228            |
| sonet show loopback .....                        | 1229            |
| sonet show medium .....                          | 1230            |
| sonet show pathtrace .....                       | 1231            |
| <br><b>Chapter 71: ssh Commands .....</b>        | <br><b>1233</b> |
| Command Summary .....                            | 1233            |
| ssh .....  | 1235            |
| ssh-client clear-known-hosts .....               | 1237            |
| ssh-client delete-host-key .....                 | 1238            |
| ssh-client import-host-keys .....                | 1239            |
| ssh-client set .....                             | 1241            |
| ssh-client set software-version-string .....     | 1244            |
| ssh-server enable .....                          | 1245            |
| ssh-server generate-host-key .....               | 1246            |
| ssh-server set auth-grace-timeout .....          | 1248            |
| ssh-server set encryption .....                  | 1249            |
| ssh-server set listen-port .....                 | 1251            |
| ssh-server set mac .....                         | 1252            |
| ssh-server set max-sessions .....                | 1254            |
| ssh-server set protocol-version .....            | 1255            |
| ssh-server set server-key-lifetime .....         | 1256            |
| ssh-server set software-version-string .....     | 1257            |
| ssh-server show public-host-key .....            | 1258            |
| <br><b>Chapter 72: statistics Commands .....</b> | <br><b>1261</b> |
| Command Summary .....                            | 1261            |
| statistics clear .....                           | 1263            |
| statistics show appletalk .....                  | 1265            |
| statistics show arp .....                        | 1266            |
| statistics show framer .....                     | 1268            |

|   |             |
|---|-------------|
| statistics show icmp.....                             | 1269        |
| statistics show icmp6.....                            | 1271        |
| statistics show ip.....                               | 1276        |
| statistics show ipv6.....                             | 1280        |
| statistics show ip-interface .....                    | 1285        |
| statistics show ipv6-interface .....                  | 1287        |
| statistics show ip-routing.....                       | 1290        |
| statistics show ipv6-routing.....                     | 1292        |
| statistics show ipx.....                              | 1294        |
| statistics show ipx-interface .....                   | 1298        |
| statistics show ipx-routing.....                      | 1300        |
| statistics show most-active .....                     | 1302        |
| statistics show multicast.....                        | 1304        |
| statistics show port-errors.....                      | 1306        |
| statistics show port-packets.....                     | 1310        |
| statistics show port-stats.....                       | 1311        |
| statistics show rarp .....                            | 1315        |
| statistics show summary-stats .....                   | 1316        |
| statistics show tcp.....                              | 1317        |
| statistics show udp.....                              | 1322        |
| statistics show vlan.....                             | 1324        |
| <b>Chapter 73: stp Commands .....</b>                 | <b>1325</b> |
| Command Summary.....                                  | 1325        |
| stp enable port .....                                 | 1326        |
| stp set bridging .....                                | 1327        |
| stp set port .....                                    | 1329        |
| stp show bridging-info .....                          | 1330        |
| stp reset-rstp .....                                  | 1331        |
| stp set protocol-version rstp .....                   | 1332        |
| stp filter-bpdu .....                                 | 1333        |
| <b>Chapter 74: system Commands.....</b>               | <b>1335</b> |
| Command Summary.....                                  | 1335        |
| system are-promimage upgrade .....                    | 1338        |
| system disable inputportlevel-rate-limiting slot..... | 1340        |
| system enable aggregate-rate-limiting .....           | 1341        |
| system failover master-cm .....                       | 1342        |
| system hotswap .....                                  | 1343        |
| system image add .....                                | 1345        |
| system image choose.....                              | 1347        |
| system image delete .....                             | 1348        |
| system image list .....                               | 1349        |
| system ipv6-fpga upgrade .....                        | 1350        |
| system kill ssh-session .....                         | 1352        |
| system kill telnet-session.....                       | 1353        |
| system l3-deep-buckets .....                          | 1355        |
| system promimage upgrade.....                         | 1357        |
| system set backup-cm-timeout.....                     | 1360        |
| system set bootprom.....                              | 1361        |



|   |             |
|---|-------------|
| system set console level .....                | 1363        |
| system set contact.....                       | 1364        |
| system set cpu-utilization-trap .....         | 1365        |
| system set date .....                         | 1366        |
| system set dns.....                           | 1367        |
| system set dst-changing .....                 | 1368        |
| system set dst-fixed.....                     | 1370        |
| system set dst-manual .....                   | 1372        |
| system set extended-debug.....                | 1373        |
| system set idle-timeout.....                  | 1374        |
| system set location .....                     | 1375        |
| system set login-banner.....                  | 1376        |
| system set malloc .....                       | 1378        |
| system set name .....                         | 1379        |
| system set password .....                     | 1380        |
| system set password-policy.....               | 1382        |
| system set poweron-selftest .....             | 1384        |
| system set show-config .....                  | 1385        |
| system set spooler-memory-limit.....          | 1386        |
| system set syslog .....                       | 1387        |
| system set syslog-levels .....                | 1392        |
| system set terminal.....                      | 1393        |
| system set tftpsource .....                   | 1394        |
| system set timezone .....                     | 1395        |
| system set user .....                         | 1397        |
| system show .....                             | 1398        |
| system show capacity.....                     | 1404        |
| system show syslog levels.....                | 1408        |
| <b>Chapter 75: tacacs-plus Commands .....</b> | <b>1413</b> |
| Command Summary .....                         | 1413        |
| tacacs-plus accounting command level.....     | 1415        |
| tacacs-plus accounting shell.....             | 1416        |
| tacacs-plus accounting snmp.....              | 1417        |
| tacacs-plus accounting system .....           | 1418        |
| tacacs-plus authentication .....              | 1419        |
| tacacs-plus enable .....                      | 1420        |
| tacacs-plus set .....                         | 1421        |
| tacacs-plus set server.....                   | 1423        |
| tacacs-plus show .....                        | 1425        |
| <b>Chapter 76: telnet Command .....</b>       | <b>1427</b> |
| <b>Chapter 77: traceroute Command .....</b>   | <b>1429</b> |
| traceroute.....                               | 1429        |

|  |                 |
|--|-----------------|
| <b>Chapter 78: vlan Commands .....</b>                 | <b>1433</b>     |
| Command Summary .....                                  | 1433            |
| vlan add ports .....                                   | 1434            |
| vlan create .....                                      | 1435            |
| vlan default-vlan ports.....                           | 1439            |
| vlan enable.....                                       | 1440            |
| vlan forbid ports .....                                | 1441            |
| vlan make .....  | 1442            |
| vlan multi-add .....                                   | 1444            |
| vlan multi-create.....                                 | 1445            |
| vlan show.....   | 1448            |
| vlan untagged ports .....                              | 1449            |
| <br><b>Chapter 79: web-cache Commands.....</b>         | <br><b>1451</b> |
| Command Summary .....                                  | 1451            |
| web-cache apply interface.....                         | 1452            |
| web-cache clear .....                                  | 1453            |
| web-cache create bypass-list .....                     | 1454            |
| web-cache create server-list .....                     | 1456            |
| web-cache permit deny hosts.....                       | 1457            |
| web-cache set .....                                    | 1459            |
| web-cache show .....                                   | 1462            |
| <br><b>Appendix A: RMON 2 Protocol Directory .....</b> | <br><b>1467</b> |

# About This Manual

This manual provides reference information for the commands in the Enterasys X-Pedition Command Line Interface (CLI). For product information not available in this manual, see the manuals listed in *Related Documentation* ([page xxxiv](#)).

Some features are not available with earlier firmware releases or specific hardware platforms. Review the Release Notes for your current firmware release or hardware platform to determine if a feature is supported.

## What's New (July 2004)

The content of this manual includes the addition of new and extended capabilities for the following:

### ACL

*acl apply interface* ([page 3](#))

*acl permit/deny ipv6* ([page 32](#))

*acl show* ([page 51](#))

### BGP

*bgp set bad-aspath* ([page 150](#))

*bgp set internal-set-pref* ([page 155](#))

*bgp set peer-group* ([page 157](#))

*bgp set peer-host* ([page 161](#))

*bgp show community* ([page 169](#))

*bgp show flap-statistics* ([page 171](#))

*bgp show routes* ([page 179](#))

## **DVMRP**

*dvmrp create tunnel* ([page 244](#))

*dvmrp enable interface* ([page 246](#))

*dvmrp enable tunnel* ([page 248](#))

*dvmrp set interface* ([page 249](#))

*dvmrp set neighbor-timeout* ([page 251](#))

*dvmrp set prunetime* ([page 252](#))

*dvmrp show* ([page 253](#))

*dvmrp start* ([page 255](#))

*dvmrp trace* ([page 256](#))

*dvmrp trace local-options* ([page 257](#))

The following commands have been removed:

- *dvmrp accept|noaccept*
- *dvmrp advertise|noadvertise*
- *dvmrp enable no-pruning*
- *dvmrp set protocol*
- *dvmrp show rules*

## **IGMP**

*igmp enable interface* ([page 362](#))

*igmp join group* ([page 365](#))

*igmp set* ([page 366](#))

*igmp show groups* ([page 370](#))

*igmp show interfaces* ([page 371](#))

*igmp start/stop* ([page 373](#))

*igmp trace* ([page 375](#))

*igmp trace local-options* ([page 377](#))

The following commands have been removed:

- `igmp set interface`
- `igmp set responsetime`
- `igmp show memberships`
- `igmp show timers`

## **Interface**

`interface add ipv6` ([page 385](#))

`interface create ipv6` ([page 399](#))

`interface show ipv6` ([page 413](#))

## **IP**

`ip l3-hash` ([page 432](#))

`ip show routes` ([page 445](#))

## **IPv6**

This is a new chapter.

## **IP Router**

`ip-router global set` ([page 497](#))

`ip-router global set trace-level` ([page 499](#))

`ip-router global set trace-options` ([page 500](#))

`ip-router global set trace-state` ([page 501](#))

`ip-router policy add optional-attributes-list` ([page 506](#))

`ip-router policy aggr-gen destination` ([page 508](#))

`ip-router policy create aggr-export-source` ([page 510](#))

`ip-router policy create aggr-gen-dest` ([page 511](#))

`ip-router policy create aggr-gen-source` ([page 512](#))

`ip-router policy create aspath-export-source` ([page 514](#))

*ip-router policy create bgp-export-destination* ([page 516](#))

*ip-router policy create bgp-export-source* ([page 517](#))

*ip-router policy create bgp-import-source* ([page 518](#))

*ip-router policy create direct-export-source* ([page 520](#))

*ip-router policy create filter* ([page 521](#))

*ip-router policy create optional-attributes-list* ([page 523](#))

*ip-router policy create ospfase-export-source* ([page 525](#))

*ip-router policy create ospf-export-destination* ([page 526](#))

*ip-router policy create ospf-export-source* ([page 527](#))

*ip-router policy create ospf-import-source* ([page 528](#))

*ip-router policy create ospfnssa-export-destination* ([page 529](#))

*ip-router policy create redirect-import-source* ([page 530](#))

*ip-router policy create rip-export-destination* ([page 531](#))

*ip-router policy create rip-export-source* ([page 532](#))

*ip-router policy create rip-import-source* ([page 533](#))

*ip-router policy create static-export-source* ([page 535](#))

*ip-router policy create tag-export-source* ([page 536](#))

*ip-router policy export destination* ([page 537](#))

*ip-router policy import source* ([page 540](#))

*ip-router policy redistribute* ([page 543](#))

## **IP Router V6**

This is a new chapter.

## **IPX**

*ipx l3-hash* ([page 572](#))

## **Load Balance**

*load-balance set group-options* ([page 620](#))

*load-balance set server-options* ([page 629](#))

## **MTRACE**

This command has been removed.

## **Multicast**

The following commands have been removed:

- *multicast show interface* (use **multicast show vif** instead)
- *multicast show mroutes* (use **dvmrp show mfc** instead)

## **ndisc**

This is a new chapter.

## **NetFlow**

*netflow set flow-destination-port* ([page 728](#))

*netflow set memory* ([page 730](#))

*netflow show* ([page 732](#))

The following commands have been removed:

- *netflow set memory-threshold*
- *netflow set priority*

## **OSPF**

*ospf add nssa-network* ([page 749](#))

*ospf add stub-network* ([page 752](#))

*ospf add summary-filter* ([page 753](#))

*ospf set advertise-subnet* ([page 758](#))

*ospf set always-update-summary* ([page 759](#))

*ospf set area* ([page 760](#))

*ospf set ase-defaults* ([page 762](#))  
*ospf set authentication-method* ([page 763](#))  
*ospf set hello-interval* ([page 764](#))  
*ospf set interface* ([page 765](#))  
*ospf set nssa-defaults* ([page 768](#))  
*ospf set opaque-capability* ([page 769](#))  
*ospf set poll-interval* ([page 770](#))  
*ospf set priority* ([page 771](#))  
*ospf set retransmit-interval* ([page 772](#))  
*ospf set rfc1583 on* ([page 773](#))  
*ospf set router-dead-interval* ([page 774](#))  
*ospf set transit-delay* ([page 775](#))  
*ospf set-trap* ([page 776](#))  
*ospf set virtual-link* ([page 778](#))  
*ospf show* ([page 780](#))  
*ospf trace* ([page 784](#))

The following commands have been removed:

- *ospf create-monitor*
- *ospf monitor*
- *ospf set export-interval*
- *ospf set export-limit*

## **PIM**

The following commands have been removed:

- *pim igmp*
- *pim show igmp-groups*
- *pim show igmp-interface*



**Ping**

*ping* ([page 819](#))

*Examples* ([page 823](#))

**Port**

*port set* ([page 837](#))

**RDISC**

*rdisc set address* ([page 988](#))

The **rdisc stop** command has been removed.

**Ripng**

This is a new chapter

**SNMP**

*snmp set mib* ([page 1175](#))

**Statistics**

*statistics show icmp6* ([page 1271](#))

*statistics show ipv6* ([page 1280](#))

*statistics show ipv6-interface* ([page 1287](#))

*statistics show ipv6-routing* ([page 1292](#))

**System**

*system ipv6-fpga upgrade* ([page 1350](#))

*system show* ([page 1398](#))

*system show syslog levels* ([page 1408](#))

**Traceroute**

*traceroute* ([page 1429](#))

**VLAN**

*vlan make* ([page 1442](#))

## Who Should Read This Manual?

Read this manual if you are a network administrator responsible for configuring or managing the X-Pedition router.

## How to Use This Manual

The CLI commands and facilities are organized alphabetically in this manual. To locate information about a command, go to the chapter for the command or for the facility that contains the command. For example, to find information about the **configure** command, go to *configure Command* (page 221). To find information about the **interface add** command, go to *interface Commands* (page 379), then locate the description of the **interface add** command within that chapter.

## Related Documentation

The X-Pedition documentation set includes the following items. Refer to these other documents to learn more about your product.

| For Information About...   | See the...   |
|--|--|
| Installing and setting up the X-Pedition router  | <i>Enterasys X-Pedition Getting Started Guide</i>  |
| How to use CLI (Command Line Interface) commands to configure and manage the X-Pedition router | <i>Enterasys X-Pedition User Reference Manual</i>  |
| SYSLOG messages and SNMP traps   | <i>Enterasys X-Pedition Error Reference Manual</i> |

## CLI Parameter Types

The following table describes all the parameter types you can use with the CLI.

| Data Type                       | Description   | Example                  |
|---------------------------------|---|--------------------------|
| conditional                     | A numerical conditional expression. Special symbols are used to describe a numerical condition: > (greater than), < (less than) and != (not equal to).  | <1024 or >2048 or !=4096 |
| hexadecimal                     | A hexadecimal number  | a7 or 0xa7               |
| hostname                        | Hostname of an IP host  | gauguin or john-pc       |
| hostname/IP                     | Hostname or IP address of a host  | nagasaki or 10.43.1.4    |
| keyword                         | A keyword described in the list of acceptable keywords in the online help   | on or off                |
| interface name<br>or IP address | Name of an interface or its IP address<br><br><b>Note:</b> Enterasys recommends that you use alphabetic characters when defining interface names—purely numeric interfaces will be interpreted as IP addresses.   | int1 or 10.1.4.33        |
| interface name<br>list          | A list of one or more interface names delimited by commas<br><br><b>Note:</b> Enterasys recommends that you use only alphabetic characters when defining interface names—purely numeric interfaces will be interpreted as IP addresses. The X-Pedition router will display interface names up to 32 characters in length. | int1 or int1,int2,int3   |
| IP address                      | An IP address of the form x.x.x.x. Some commands may explicitly require a unicast or multicast address.   | 10.1.2.3                 |

| Data Type                | Description  | Example                                   |
|--------------------------|--|---|
| IP address/mask          | <p>A pair of IP address and mask values. Depending on the command, the mask may be a network mask or filtering mask. The mask can be described using the traditional IP address syntax (255.0.0.0) or a CIDR syntax (/8).</p> <p><b>Note:</b> If the user does not specify a mask, the X-Pedition router will assign the natural network mask based on the class of the given IP address. For example, the router will assign a class A address 10.1.4.0 the 255.0.0.0 (or /8) network mask.</p> | 10.1.4.0/255.255.255.0 or 10.1.4.0/24     |
| IP address list          | A list of IP addresses separated by spaces but enclosed in quotes.   | <i>"10.1.4.4 10.1.5.5 10.1.6.6"</i>       |
| IPX network address      | An IPX network address in hexadecimal  |   |
| IPX network.node address | An IPX network and node address of the form <netaddr>.<macaddr> where <netaddr> is the network address of a host and <macaddr> is the node or MAC address of the IPX host. For some commands, if the node address is not given, the node address is assumed to be a wildcard.  | a1b2c3d4.0820a1:f3:38:11<br>or aa89f383   |
| IPX SAP server name      | An alphanumeric string representing a valid IPX SAP server name where the following characters are illegal:<br>"*./;<=>?[]\  | server1                                   |
| MAC address              | A MAC address specified in one of two forms: xx:xx:xx:xx:xx:xx or xxxxxx:xxxxxx  | 08:00:50:1a:2b:c3 or 080050:1a2bc3        |
| number                   | An integer number  | 100                                       |
| numerical range          | A number or a range of numbers   | 5 or 7-10                                 |
| port                     | A single port  | et.1.4, gi.2.1, hs.3.1.100, or se.4.2.200 |

| Data Type   | Description  | Example   |
|-------------|--|---|
| port list   | A list of one or more ports. To specify a range of ports within a module, describe the range in parenthesis. You can also specify non-consecutive ports by using commas to separate them. The wildcard character (*) can also be used to specify all modules or all ports within a module. | et.1.(3-8) or et.1.(1,3,5), hs.(1-2).1.100, or se.4.(1-3).200, gi.2.* |
| slot number | A list of one or more occupied slots in the X-Pedition router.   | 1 or 7  |
| string      | A character string. To include spaces in a string, specify the entire string in double quotes ("").  | abc or "abc def"  |
| URL         | A Uniform Resource Locator. The type of URL depends on the command where the URL is used. Currently, two URLs are supported:<br><br>TFTP: <i>tftp://host/pathname</i><br><br>RCP: <i>rcp://username@host/pathname</i>  | tftp://10.1.4.5/test/abc.txt<br>rcp://dave@rtr/test/abc.txt           |

## Command Syntax and Conventions

The CLI command syntax and conventions use the notation described in the following table.

| Convention                           | Description  |
|--------------------------------------|--|
| <b>xyz</b>                           | <b>Bold</b> indicates a keyword or mandatory parameter.  |
| < <i>variable</i> >                  | <> Angle brackets and <i>italics</i> indicate a variable, such as an IP address or interface name.                           |
| [ <b>x</b> ]                         | [ ] Square brackets indicate an optional parameter.  |
| [ <b>x</b>   <b>y</b>   <b>z</b> ]   | [   ] Square brackets with vertical bar indicate a choice of values.   |
| { <b>x</b>   <b>y</b>   <b>z</b> }   | {   } Braces with vertical bar indicate a choice of a required value.  |
| [ <b>x</b> { <b>y</b>   <b>z</b> } ] | [ {   } ] Combination of square brackets with braces and vertical bars indicates a required choice of an optional parameter. |

## Getting Help

For additional support related to the NATIVE CLI syntax or this document, contact Enterasys Networks using one of the following methods:

|  |  |
|--|--|
| World Wide Web   | <a href="http://www.enterasys.com/support">www.enterasys.com/support</a>   |
| Phone  | 603-332-9400<br>1-800-872-8440 (toll-free in U.S. and Canada)<br><br>For the Enterasys Networks Support toll-free number in your country: <a href="http://www.enterasys.com/support/gtac-all.html">www.enterasys.com/support/gtac-all.html</a> |
| Internet mail  | support@enterasys.com<br><br>To expedite your message, please type <b>[ROUTE]</b> in the subject line.   |
| To send comments or suggestions concerning this document to the Technical Writing Department: <b>TechWriting@enterasys.com</b><br><br>To expedite your message, please type <b>[techwriting]</b> in the subject line, and include the document Part Number in the email message. |  |

**Before contacting Enterasys Networks for technical support, have the following information ready:**

- Your Enterasys Networks service contract number
- A description of the failure
- A description of any action(s) already taken to resolve the problem (e.g., changing mode switches, rebooting the unit, etc.)
- The serial and revision numbers of all involved Enterasys Networks products in the network
- A description of your network environment (layout, cable type, etc.)
- Network load and frame size at the time of trouble (if known)
- The device history (i.e., have you returned the device before, is this a recurring problem, etc.)
- Any previous Return Material Authorization (RMA) numbers

# Chapter 1

## acl Commands

The **acl** commands allow you to create ACLs (Access Control Lists) and apply them to IPv4, IPv6, and IPX interfaces on the X-Pedition router. An ACL permits or denies switching of packets based on criteria such as the packet's source address and destination address, TCP or UDP port number, and so on. When you apply an ACL to an interface, you can specify whether the ACL affects incoming traffic or outgoing traffic. You also can enable a log of the ACL's use.

**Note:** Using ACLs for packet filtering directly impacts NetFlow performance. Specific performance will vary based on the number and complexity of the ACLs.

### Command Summary

[Table 1](#) lists the **acl** commands. The sections following the table describe the command syntax.

**Table 1. acl commands**

|   |
|---|
| <b>acl</b> <name> <b>apply interface</b> { <InterfaceName> all-ip all-ipv6 all-ipv6in4-tunnels }<br><b>input</b>   <b>output</b> [ <b>logging on</b>   <b>off</b> ] <b>deny-only</b>   <b>permit-only</b>   <b>on-syslog</b>   <b>deny-syslog</b>  <br><b>permit-syslog</b> ] [ <b>report-denied periodic</b>   <b>all</b> ] [ <b>policy local</b>   <b>external</b> ] [ <b>deny-trap</b> ] |
| <b>acl</b> <name> <b>apply interface-are</b> <InterfaceName> <b>input</b>   <b>output</b>   |
| <b>acl</b> <name> <b>apply port</b> <port list> <b>input</b>   <b>output</b> [ <b>logging on</b>   <b>off</b> ] <b>on-syslog</b>   <b>deny-syslog</b>  <br><b>permit-syslog</b> ] [ <b>report-denied periodic</b>   <b>all</b> ] [ <b>policy local</b>   <b>external</b> ] [ <b>deny-trap</b> ]   |
| <b>acl</b> <name> <b>apply service</b> <ServiceName> [ <b>logging on</b>   <b>off</b> ]  <b>on-syslog</b>   <b>deny-syslog</b>  <br><b>permit-syslog</b> ] [ <b>deny-trap</b> ]   |
| <b>acl</b> <name> <b>clearCounters</b> aclname  <b>all</b>   <b>interface</b>   <b>service</b>   <b>port</b>  |
| <b>acl logging set deny-trap</b><br>or...<br><b>acl</b> <number> <b>apply</b> [ <b>interface</b>   <b>port</b>   <b>service</b> ] <name> <b>logging deny-only deny-trap</b>   |

Table 1. acl commands (Continued)

|   |
|---|
| <b>acl logging set syslog-only</b>  |
| <b>acl logging set deny-report-frequency</b> [<number>]   |
| <b>acl</b> <name> <b>permit deny appletalk</b> [nbp-brrq] [nbp-fwdrq] [nbp-lookup]<br>[nbp-object <ObjectName>] [nbp-type <TypeName>] [nbp-zone <ZoneName>] |
| <b>acl</b> <name> <b>permit deny appletalk cable-range</b> <range>  |
| <b>acl</b> <name> <b>permit deny appletalk zone</b> <ZoneName>  |
| <b>acl</b> <name> <b>permit deny icmp</b> <SrcAddr/Mask> <DstAddr/Mask> [log]   |
| <b>acl</b> <name> <b>permit deny igmp</b> <SrcAddr/Mask> <DstIP/mask> [log]   |
| <b>acl</b> <name> <b>permit deny ip</b> <SrcAddr/Mask> <DstAddr/Mask> <SrcPort> <DstPort> <tos><br><tos-mask> [log]   |
| <b>acl</b> <name> [ <b>permit deny</b> ] <b>ipv6</b> <SrcIPv6Addr/PrefixLen> <DstIPv6Addr/PrefixLen><br><tclass> <nheader>                                  |
| <b>acl</b> <name> <b>permit deny ip-protocol</b> <proto-num> <SrcAddr/Mask> <DstAddr/Mask><br><tos> [log]   |
| <b>acl</b> <name> <b>permit deny ipx</b> <SrcAddr> <SrcSocket> <DstAddr> <DstSocket><br><SrcNetMask> <DstNetMask>   |
| <b>acl</b> <name> <b>permit deny ipxgns</b> <ServerAddr> <ServiceType> <ServiceName>  |
| <b>acl</b> <name> <b>permit deny ipxrip</b> <FromNetwork> <ToNetwork>   |
| <b>acl</b> <name> <b>permit deny ipxsap</b> <ServerAddr> <ServiceType> <ServiceName>  |
| <b>acl</b> <name> <b>permit deny ipxtype20</b>  |
| <b>acl</b> <name> <b>permit deny tcp</b> <SrcAddr/Mask> <DstAddr/Mask> <SrcPort> <DstPort><br><tos> <tos-mask> [established] [log]                          |
| <b>acl</b> <name> <b>permit deny udp</b> <SrcAddr/Mask> <DstAddr/Mask> <SrcPort> <DstPort><br><tos> <tos-mask> [log]  |
| <b>acl-policy enable external  policy-routing-external</b>  |
| <b>acl show</b> [aclname <string> all]   [interface <string> all-ip all-ipv6 all-ipv6in4-tunnels]  <br>[service]   [port <port list> all-ports]   [all]     |



# acl apply interface

## Purpose

Apply an ACL to an interface.

## Format

```
acl <name> apply interface { <InterfaceName>|all-ip|all-ipv6|all-ipv6in4-tunnels }  
input| output [logging on| off] deny-only| permit-only| on-syslog| deny-syslog| permit-syslog [report-denied periodic| all] [policy local| external] [deny-trap]
```

## Mode

Configure.

## Description

The **acl apply interface** command applies a previously defined ACL to an interface. When you apply an ACL to an interface, you implicitly enable access control on that interface. You can apply an ACL to filter out inbound traffic, outbound traffic, or both inbound and outbound traffic. Inbound traffic is packets coming into the interface while outbound traffic is packets going out of that interface.

You can use the **all-ip**, **all-ipv6**, or **all-ipv6in4-tunnels** options to apply an ACL to all the router's IPv4, IPv6 port-based, or IPv6-in-IPv4 tunnel interfaces at one time. However, if you then apply a different ACL to a specific interface, the ACL applied directly to the specific interface will replace any ACL applied to all IP interfaces, for that interface. If you subsequently remove or un-apply the specifically-applied ACL, the **all-ip/all-ipv6/all-ipv6in4-tunnels** ACL will automatically be applied to that interface again.

When you apply an ACL, you also can enable ACL Logging by using the **logging** keyword. When you enable ACL Logging on an interface, the X-Pedition router displays ACL Logging messages on the console. The ACL log provides information such as the interface name, the ACL name, whether the packet is forwarded or not, and the internal details of the packet.

You can also specify if the ACL is allowed to be modified or removed from the interface by an external agent (such as a policy manager application) by using the **policy** keyword. If you do not specify the **policy** keyword, an external agent is allowed to modify or remove the applied ACL. Note that the **acl-policy enable external** command must be in the configuration before an external agent can modify or remove an applied ACL.

**Note:** Logging, reporting, and modification by external agents are not supported for IPv6 ACLs.

## Parameters

|  |  |
|--|--|
| <b>&lt;name&gt;</b>  | Name of the ACL. The ACL must already be defined. To define an ACL, use one of the commands described in other sections in this chapter.   |
| <b>&lt;InterfaceName&gt; <br/>all-ip all-ipv6 <br/>all-ipv6in4-tunnels</b> | <p>Specifies the interface to which you are applying the ACL.</p> <p>You can apply it to a single interface, by entering the interface name. You can apply it to all IPv4 interfaces with the <b>all-ip</b> keyword, or to all IPv6 port-based interfaces with the <b>all-ipv6</b> keyword, or to all IPv6-in-IPv4 tunnel interfaces with the <b>all-ipv6in4-tunnels</b> keyword.</p> <p><b>Note:</b> Enterasys recommends that you use alphabetic characters when defining interface names—purely numeric interfaces will be interpreted as IP addresses. The X-Pedition router displays interface names up to 32 characters in length.</p> |
| <b>input</b>   | Applies the ACL to filter out inbound traffic.   |
| <b>output</b>  | <p>Applies the ACL to filter out outbound traffic.</p> <p><b>Note:</b> You cannot apply IPv6 ACLs to outbound traffic, only to inbound.</p>  |
| <b>logging &lt;keyword&gt;</b>   | <p>Enables or disables ACL logging for this interface.</p> <p><b>Note:</b> Logging is not supported for IPv6 ACLs.</p> <p>You can specify one of the following keywords:</p>   |
| <b>off</b>   | Disables all logging.  |
| <b>on</b>  | Enables logging of packets that are dropped or forwarded because of ACL. If logging is turned on when you apply the ACL to an interface, you will override the rule-based logging values. In order to enable rule-based logging, the log option must remain off.   |
| <b>deny-only</b>   | Enables logging of dropped packets only.   |
| <b>permit-only</b>   | Enables logging of forwarded packets only.   |
| <b>on-syslog</b>   | Enables logging of packets that are dropped or forwarded. Sends logging messages only to Syslog server.  |
| <b>deny-syslog</b>   | Enables logging of dropped packets only. Sends logging messages only to Syslog server.   |
| <b>permit-syslog</b>   | Enables logging of forwarded packets only. Sends logging messages only to Syslog server.   |

|                                   |   |
|-----------------------------------|---|
| <b>report-denied</b><br><keyword> | <p>Enables reporting of all denied traffic for this ACL. Without this option, only the first denied packet of a particular traffic stream is reported. Subsequent packets are dropped at the line module with no reporting. You can specify one of the following keywords:</p> <p><b>Note:</b> This option is currently available for IPv4 ACLs only.</p> |
| <b>periodic</b>                   | <p>The X-Pedition router will periodically report how many denied packets have been dropped by this ACL. The reporting period is configurable with the command 'acl logging set deny-report-frequency X'.</p>   |
| <b>all</b>                        | <p>All packets dropped by this ACL will be reported as they are received. This option may severely impact forwarding performance, and is not recommended for normal network operation.</p>  |
| <b>policy local external</b>      | <p>Allows or prevents an external agent from modifying or removing the applied ACL.</p> <p><b>Note:</b> This feature is not supported for IPv6 ACLs.</p> <p>You can specify one of the following keywords:</p>  |
| <b>local</b>                      | <p>External agent cannot modify or remove the applied ACL.</p>  |
| <b>external</b>                   | <p>External agent can modify or remove the applied ACL. This is the default.</p>  |
| <b>deny-trap</b>                  | <p>Send an SNMP trap when the applied ACL denies access. See also the <b>acl logging set deny-trap</b> command.</p> <p><b>Note:</b> This feature is not supported for IPv6 ACLs.</p>  |

## Restrictions

- You can apply only one ACL at a time (IPv4 or IPX) to inbound or outbound traffic on an interface. For example, if you define two ACLs, “ipacl1” and “ipacl2”, you cannot apply them both to inbound traffic. However, if you define one ACL for *inbound* traffic and one for *outbound* traffic, you can apply both ACLs. This does not limit the number of rules you may apply, it means only that you must include all rules in a single ACL.
- You can apply IPv4 ACLs to IPv4 interfaces only, IPv6 ACLs to IPv6 interfaces only, and IPX ACLs to IPX interfaces only.
- You can apply only one IPv6 ACL at a time on an IPv6 interface, and you can apply the ACL to inbound traffic only (with the **input** option). You cannot apply IPv6 ACLs to outbound traffic.
- You may not apply ACLs to interface EN0 of the control module.
- The **logging**, **policy**, and **report-denied** options cannot be used with IPv6 ACLs.

## Examples

To apply ACL “100” to interface *int4* to filter out inbound traffic:

```
xp(config)# acl 100 apply interface int4 input
```

To apply ACL “nonfs” to interface *int16* to filter out outbound traffic and enable logging:

```
xp(config)# acl nonfs apply interface int16 output logging on
```

To apply ACL “100” to interface *int10* to filter out inbound traffic and enable logging to the Syslog server:

```
xp(config)# acl 100 apply interface int10 input logging on-syslog
```

# acl apply interface-are

## Purpose

Applies an Appletalk/ARE (Advanced Routing Engine) ACL to an interface.

## Format

**acl** <name> **apply interface-are** <InterfaceName> **input|output**

## Mode

ARE-Configure.

## Description

The **acl apply interface-are command** works very similarly to the **acl apply interface** command, with the following exceptions:

- If an Appletalk/ARE ACL contains Names Binding Protocol (NBP) rules (such as nbp-brrq, nbp-fwdrq, nbp-lookup, nbp-object, nbp-type, or nbp-zone), you may only apply it to the *input* of an interface.
- Like other ACLs for the X-Pedition router, each direction (input and output) on an interface must have only one Appletalk/ARE ACL applied to it at a time. For example, although you can define two ARE ACLs, “areacl1” and “areacl2”, you cannot apply them both to the same interface. Unlike other ACLs, however, a single ARE ACL may be applied to *both* directions on one interface. In addition, a single ARE ACL may be applied to multiple interfaces.
- After applying an ARE ACL containing zone or cable-range rules, it may be necessary to reboot all network X-Pedition routers in order to see the new ACL. Alternatively, you may disable or disconnect the Routing Maintenance Protocol (RTMP) until all routes have been removed from each network X-Pedition routing table.

**Note:** No special action is required for ACLs containing only NBP rules.

- There are no logging options available for ARE ACLs at this time.

## Parameters

|                                    |   |
|------------------------------------|---|
| <code>&lt;name&gt;</code>          | Name of the ACL. The ACL must already be defined. To define an ACL, use one of the commands described in other sections in this chapter.  |
| <code>&lt;InterfaceName&gt;</code> | Name of the interface to which you are applying the ACL.<br><br><b>Note:</b> Enterasys recommends that you use alphabetic characters when defining interface names—purely numeric interfaces will be interpreted as IP addresses. The X-Pedition router displays interface names up to 32 characters in length. |
| <b>input</b>                       | Applies the ACL to filter out inbound traffic.  |
| <b>output</b>                      | Applies the ACL to filter out outbound traffic.   |

## Restrictions

- You may only use this command in ARE-Configure mode. For more about this mode, please see [Chapter 6, are Commands](#).
- You may apply only one ARE ACL to an interface at a time.
- You may not apply ACLs to interface EN0 of the control module.

## Examples

To apply ACL “ar10” to interface *int4* to filter out inbound traffic:

```
xp(are-config)# acl ar10 apply interface-are int4 input
```

To apply ACL “ar12” to interface *int16* to filter out outbound traffic:

```
xp(are-config)# acl ar12 apply interface-are int16 output
```

# acl apply port

## Purpose

Apply an ACL to one or more ports operating in Layer-4 bridging mode.

## Format

**acl** <name> **apply port** <port list> **input**|**output** [**logging on**|**off**] **on-syslog**|**deny-syslog**|**permit-syslog** [**report-denied periodic**|**all**] [**policy local**|**external**] [**deny-trap**]

## Mode

Configure.

## Description

The **acl apply port** applies a previously defined ACL to one or more ports. This command applies only to ports operating in Layer-4 bridging mode. The ACLs applied to a Layer-4 bridging port are only used with bridged traffic. Routed traffic is still subject to the ACLs attached to the interface.

IPv6 ACLs cannot be applied to ports.

## Parameters

|                          |  |
|--------------------------|--|
| <name>                   | Name of the ACL. The ACL must already be defined. To define an ACL, use one of the commands described in other sections in this chapter. |
| <port list>              | Specifies the port(s) in the Layer-4 bridging VLAN to which you are applying the ACL.  |
| <b>input</b>             | Applies the ACL to filter out inbound traffic.   |
| <b>output</b>            | Applies the ACL to filter out outbound traffic.  |
| <b>logging</b> <keyword> | Enables or disables ACL logging for this port. You can specify one of the following keywords:  |
| <b>on</b>                | Enables logging of packets that are dropped or forwarded because of ACL.   |
| <b>off</b>               | Disables all logging.  |
| <b>on-syslog</b>         | Enables logging of packets that are dropped or forwarded. Sends logging messages only to Syslog server.                                  |

|   |  |
|---|--|
| <b>deny-syslog</b>                      | Enables logging of dropped packets only. Sends logging messages only to Syslog server.   |
| <b>permit-syslog</b>                    | Enables logging of forwarded packets only. Sends logging messages only to Syslog server.   |
| <b>report-denied<br/>periodic   all</b> | Enables reporting of all denied traffic for this ACL. Without this option, only the first denied packet of a particular traffic stream is reported. Subsequent packets are dropped at the line module with no reporting. You can specify one of the following keywords:<br><br><b>Note:</b> The report-denied option is currently available for IP ACL's only. |
| <b>periodic</b>                         | The X-Pedition router will periodically report how many denied packets have been dropped by this ACL. The reporting period is configurable with the command: <b>acl logging set deny-report-frequency X</b>  |
| <b>all</b>                              | All packets dropped by this ACL will be reported as they are received. This option may severely impact forwarding performance, and is not recommended for normal network operation.  |
| <b>policy local external</b>            | Allows or prevents an external agent from modifying or removing the applied ACL. You can specify one of the following keywords:  |
| <b>local</b>                            | External agent cannot modify or remove the applied ACL.  |
| <b>external</b>                         | External agent can modify or remove the applied ACL. This is the default.  |
| <b>deny-trap</b>                        | Send an SNMP trap when the applied ACL denies access. See also the <b>acl logging set deny-trap</b> command.   |

## Restrictions

The line cards that contain the specified ports must support Layer 4 bridging. The X-Pedition software checks the line card(s) and displays an error message if new line card(s) are necessary.

IPv6 ACLs cannot be applied to ports.

## Examples

To apply ACL “l4” to slot 1, gigabit port 3 and slot 3, 10/100 port 6 for inbound traffic:

```
xp(config)# acl l4 apply port gi.1.2 et.3.6 input
```

To apply ACL “l4out” to slot 5, all ports for outbound traffic and enable logging:

```
xp(config)# acl l4out apply port et.5.* output logging on
```



To apply ACL “14” to slot 3, all ports for outbound traffic and enable logging to the Syslog server:

```
xp(config)# acl 14 apply port et.3.* output logging on-syslog
```

# acl apply service

## Purpose

Apply an ACL to a service on the X-Pedition router.

## Format

```
acl <name> apply service <ServiceName> [logging on|off|on-syslog|deny-syslog|permit-syslog]  
[deny-trap]
```

## Mode

Configure.

## Description

The **acl apply service** command applies a previously defined ACL to a service provided by the X-Pedition router. A service is typically a server or agent running on the router, for example, a Telnet server or SNMP agent. By applying an ACL to a service, you can control which host can access individual services on the router. This type of ACL is known as a Service ACL. It does not control packets going *through* the router. It only controls packets that are *destined* for the router, specifically, one of the services provided by the X-Pedition router. As a result, a Service ACL, by definition, is applied only to check for inbound traffic to the router. The destination host of a Service ACL is by definition the router. The destination port is the well-known port of the service.

When you apply an ACL, you also can enable ACL Logging by using the **logging** keyword. When you enable ACL Logging on an interface, the X-Pedition router displays ACL Logging messages on the console. The ACL log provides information such as the interface name, the ACL name, whether the packet is forwarded or not, and the internal details of the packet.

In addition, you may apply an ACL to a service on a per-interface basis, based on the destination address defined by the ACL.

## Parameters

|   |   |
|---|---|
| <code>&lt;name&gt;</code>                   | Name of the Service ACL. The ACL must already be defined. To define an ACL, use one of the commands described in other sections in this chapter.<br><br><b>Note:</b> Enterasys recommends that you use alphabetic characters when defining interface names—purely numeric interfaces will be interpreted as IP addresses. |
| <code>&lt;ServiceName&gt;</code>            | Name of the service on the X-Pedition router to which you are applying the ACL. Currently, the following services are supported:  |
| <b>http</b>                                 | HTTP web server   |
| <b>snmp</b>                                 | SNMP agent  |
| <b>telnet</b>                               | Telnet server   |
| <b>logging</b> <code>&lt;keyword&gt;</code> | Enables or disables ACL logging for this interface. You can specify one of the following keywords:  |
| <b>off</b>                                  | Disables logging.   |
| <b>on</b>                                   | Enables logging.  |
| <b>on-syslog</b>                            | Enables logging of packets that are dropped or forwarded. Sends logging messages only to Syslog server.   |
| <b>deny-syslog</b>                          | Enables logging of dropped packets only. Sends logging messages only to Syslog server.  |
| <b>permit-syslog</b>                        | Enables logging of forwarded packets only. Sends logging messages only to Syslog server.  |
| <b>deny-trap</b>                            | Send an SNMP trap when the applied ACL denies access. See also the <b>acl logging set deny-trap</b> command.  |

## Restrictions

You can apply only one ACL of each type (IPv4 or IPX) to a service at one time. For example, although you can define two ACLs, “ipacl1” and “ipacl2”, you cannot apply them both to the same service.

IPv6 ACLs cannot be applied to services.

## Examples

To permit access to the SNMP agent only from the host 10.4.3.33 (presumably an SNMP management station):

```
xp(config)# acl 100 permit udp 10.4.3.33  
xp(config)# acl 100 apply service snmp
```

The following commands permit access to the Telnet server from hosts on the subnet 10.4.7.0/24 with a privileged source port. In addition, with logging enabled, all incoming Telnet accesses are logged to the console.

```
xp(config)# acl 120 permit tcp 10.4.7.0/24 any <1024  
xp(config)# acl 120 apply service telnet logging on
```

The following commands permit access to the HTTP web server from subnet 10.12.4.0/24. Notice that even though the destination address and port are specified for this ACL (*10.12.7.44* and *any* port), they are ignored. This service ACL will match only packets destined for the X-Pedition router itself and the well-known port of the service (port 80 for HTTP).

```
xp(config)# acl 140 permit ip 10.12.4.0/24 any 10.12.7.44 any  
xp(config)# acl 120 apply service http
```

# acl clearCounters

## Purpose

Clears one or all ACL counters.

## Format

**acl clearCounters aclname** <string> | **all**| **interface**| **service**| **port**

## Mode

Enable.

## Description

The **acl clearCounters** commands allows the user to clear ACL counters. With ACL logging enabled, the router prints out a message about whether a packet is forwarded or dropped and counters keep track of these statistics. With this command, the user can clear these ACL counters.

## Parameters

|                           |  |
|---------------------------|--|
| <b>aclname</b> <string>   | Clears the counter based on the name of the ACL. Specify <b>all</b> to clear all ACLs.   |
| <b>all</b>                | Clears all ACL counters.   |
| <b>interface</b> <string> | Clears ACL counters attached to specific interfaces. Specify <b>all-ip</b> to clear the counters of ACLs applied to all IPv4 interfaces. |
| <b>service</b>            | Clears ACL counters that are applied to services.  |
| <b>port</b> <port list>   | Clears ACL counters on specific ports. Specify <b>all-ports</b> to clear counters on all ports.  |

## Restrictions

This feature does not apply to IPv6 ACLs.

## Examples

To clear the ACL counters for ACL ‘engacl’:

xp# **acl clearCounters aclname engacl**

## **acl logging set deny-trap**

### **Purpose**

Allows sending of SNMP traps when an acl denies traffic.

### **Format**

**acl logging set deny-trap**

or...

**acl <number> apply interface <name> logging deny-only deny-trap**

### **Mode**

Configure.

### **Description**

This command enables the router to send the polACLDenied traps to a configured snmp target. The trap is generated when an ACL denies access to traffic matching the specified "deny" pattern in the ACL.

### **Restrictions**

This feature does not apply to IPv6 ACLs.

# **acl logging set syslog-only**

## **Purpose**

Directs all acl reports only to the Syslog server.

## **Format**

**acl logging set syslog-only**

## **Mode**

Configure.

## **Description**

The **acl logging set syslog-only** commands allows the user to globally direct acl reporting to the Syslog server only (if defined). In order to view messages at the Syslog server, the Syslog level should be set to accept Informational Messages.

## **Restrictions**

This feature does not apply to IPv6 ACLs.

## **acl logging set deny-report-frequency**

### **Purpose**

Changes the reporting interval (in seconds) for all ACL's using the **report-denied periodic** option.

### **Format**

**acl logging set deny-report-frequency** [*<number>*]

### **Mode**

Configure.

### **Description**

The **acl logging set deny-report-frequency** command allows users to set how often the router will report denied traffic with an ACL.

### **Parameters**

---

|                       |   |
|-----------------------|---|
| <i>&lt;number&gt;</i> | The interval (15–3,600 seconds) at which to report denied traffic. By default, this interval is 15 seconds. |
|-----------------------|---|

---

### **Restrictions**

This feature does not apply to IPv6 ACLs.



# acl permit|deny appletalk nbp

## Purpose

Creates an Appletalk/ARE (Advanced Routing Engine) ACL with Name Binding Protocol (NBP) rules.

## Format

```
acl <name> permit|deny appletalk [nbp-brrq] [nbp-fwdrq] [nbp-lookup]
[nbp-object <ObjectName>] [nbp-type <TypeName>] [nbp-zone <ZoneName>]
```

## Mode

ARE-Configure.

## Description

The **acl permit appletalk** and **acl deny appletalk** commands creates and defines an ACL to allow or block specific types Appletalk/ARE traffic from entering or leaving the X-Pedition router. In this case, you use the commands to define Name Binding Protocol (NBP) rules. As with other ACLs for the X-Pedition router, you may use both deny and permit commands within the same NBP-ruled ACL.

## Parameters

|  |  |
|--|--|
| <b>&lt;name&gt;</b>                            | Name of this ACL. You may use a string of characters or a number.  |
| <b>nbp-brrq</b>                                | Name Binding Protocol Broadcast Request. Permit or deny all broadcast request packets.   |
| <b>nbp-fwdrq</b>                               | Name Binding Protocol Forward Request. Permit or deny all forward request packets.   |
| <b>nbp-lookup</b>                              | Name Binding Protocol Lookup Request. Permit or deny all lookup request packets.   |
| <b>nbp-object</b><br><b>&lt;ObjectName&gt;</b> | Permit or deny a specific machine. Specify the name of the machine (up to 32 characters). A single “~” can be used to request a match for 0 or more characters. If no machine is specified, the default “ <b>any</b> ” will be applied.              |
| <b>nbp-type</b><br><b>&lt;TypeName&gt;</b>     | Permit or deny a specific type of machine. Specify the name of the machine (up to 32 characters). A single “~” can be used to request a match for 0 or more characters. If no machine type is specified, the default “ <b>any</b> ” will be applied. |

---

|                               |  |
|-------------------------------|--|
| <b>nbp-zone</b><br><ZoneName> | Permit or deny requests from a specific zone. Specify the name of the zone. If no zone is specified, the default “ <b>any</b> ” will be applied. |
|-------------------------------|--|

---

## Restrictions

- You may only use this command in ARE-Configure mode. For more about this mode, please see [Chapter 6, are Commands](#).
- When you apply an Appletalk/ARE ACL to an interface, the X-Pedition router appends an *implicit deny rule* to that ACL. The implicit deny rule denies *all* traffic. If you intend to allow all traffic that doesn’t match your specified ACL rules to go through, you must *explicitly* define a rule to permit all traffic.
- A single ACL can contain rules for NBP, zone, or cable-range, due to the fact that these three Appletalk/ARE ACL rules act independently of one another. In effect, a single ACL containing all three types of rule will act as if it were three different ACLs.
- Users may not remove the last ACL rule for an ACL applied through the ACL editor to an interface unless they first remove the apply statement.

## Examples

To permit all broadcast requests for ACL ar310:

```
xp(are-config)# acl ar310 permit appletalk nbp-brrq
```

The *implicit deny rule* will automatically cause all forward requests to be dropped.

To permit both broadcast and forward requests:

```
xp(are-config)# acl ar310 permit appletalk nbp-brrq nbp-fwdrq
```

To deny recognition of all laser printers on any zone:

```
xp(are-config)# acl ar310 deny appletalk nbp-object ~ nbp-type laserprinter  
xp(are-config)# acl ar310 permit nbp-brrq nbp-fwdrq
```

To deny recognition of laser printer “printer 1”:

```
xp(are-config)# acl ar310 deny appletalk nbp-object printer1 nbp-type laserprinter  
xp(are-config)# acl ar310 permit nbp-brrq nbp-fwdrq
```

# acl permit|deny appletalk cable-range

## Purpose

Creates an Appletalk/ARE (Advanced Routing Engine) ACL containing cable range rules.

## Format

**acl** <name> **permit|deny appletalk cable-range** <range>

## Mode

ARE-Configure.

## Description

The **acl permit appletalk cable-range** and **acl deny appletalk cable-range** commands create and define an ACL to allow or block specific types Appletalk/ARE traffic from entering or leaving the X-Pedition router. In this case, you use the commands to define cable range rules. Unlike with other ACLs for the X-Pedition router, all cable range rules within an ACL must either permit or deny traffic; you may not mix the two commands.

## Parameters

|         |   |
|---------|---|
| <name>  | Name of this ACL. You may use a string of characters or a number.                   |
| <range> | Cable range for which to apply rule. Specify values between 1 and 65279, inclusive. |

## Restrictions

- You may only use this command in ARE-Configure mode. For more about this mode, please see [Chapter 6, are Commands](#).
- All cable range rules within a single ACL must either permit or deny traffic. For example, if you create a rule, “acl appleacl deny appletalk cable-range 1-100”, any additional cable range rules for ACL “appleacl” must also be of the type “deny.”
- When you apply an Appletalk/ARE ACL to an interface, the X-Pedition router appends an *implicit deny rule* to that ACL. The implicit deny rule denies *all* traffic. If you intend to allow all traffic that doesn’t match your specified ACL rules to go through, you must *explicitly* define a rule to permit all traffic. Thusly, if you define an ACL to “deny” cable range access, any cable range not listed within the ACL will be permitted. If you define an ACL to “permit” cable range access, any cable range not listed within the ACL will be blocked.

- A single ACL can contain rules for cable-range, NBP, and zone due to the fact that these three Appletalk/ARE ACL rules act independently of one another. In effect, a single ACL containing all three types of rule will act as if it were three different ACLs.
- Users may not remove the last ACL rule for an ACL applied through the ACL editor to an interface unless they first remove the apply statement.

# acl permit|deny appletalk zone

## Purpose

Creates an Appletalk/ARE (Advanced Routing Engine) ACL containing zone rules.

## Format

**acl** <name> **permit|deny appletalk zone** <ZoneName>

## Mode

ARE-Configure.

## Description

The **acl permit appletalk zone** and **acl deny appletalk zone** commands create and define an ACL to allow or block specific types Appletalk/ARE traffic from entering or leaving the X-Pedition router. In this case, you use the commands to define zone rules. Unlike with other ACLs for the X-Pedition router, all zone rules within an ACL must either permit or deny traffic; you may not mix the two commands.

**Note:** The X-Pedition router acts as either a *seed* or a *no-seed* router. If you set as a seed router, the X-Pedition router will assign zone information to the networks to which it is attached.

## Parameters

|            |   |
|------------|---|
| <name>     | Name of this ACL. You may use a string of characters or a number.   |
| <ZoneName> | The name of the zone for which to apply rule. Zone names may use a string of characters or numbers. (A zone refers a logical grouping of appletalk networks on a LAN or WAN.) |

## Restrictions

- You may use this command only in ARE-Configure mode. For more about this mode, please see [Chapter 6, are Commands](#).
- All zone rules within a single ACL must either permit or deny traffic. For example, if you create a rule, “acl zacl deny appletalk zone myzone,” any additional zone rules for ACL “zacl” must also be of the type “deny.”

- When you apply an Appletalk/ARE ACL to an interface, the X-Pedition router appends an *implicit deny rule* to that ACL. The implicit deny rule denies *all* traffic. If you intend to allow all traffic that doesn't match your specified ACL rules to go through, you must *explicitly* define a rule to permit all traffic. Thusly, if you define an ACL to "deny" zone access, any zone not listed within the ACL will be permitted. If you define an ACL to "permit" zone access, any zone not listed within the ACL will be blocked.
- A single ACL can contain rules for zone, NBP, and cable-range, due to the fact that these three Appletalk/ARE ACL rules act independently of one another. In effect, a single ACL containing all three types of rule will act as if it were three different ACLs.
- Users may not remove the last ACL rule for an ACL applied through the ACL editor to an interface unless they first remove the apply statement.

## Examples

If you wish to permit only those packets that emanate from zoneA (i.e., all other packets are ignored), enter the following:

```
acl 243 permit appletalk zone zoneA
```

If you wish to deny all packets from zoneB (i.e., all other packets are welcome), enter the following:

```
acl 245 deny appletalk zone zoneB
```

# acl permit|deny icmp

## Purpose

Create an ICMP ACL.

## Format

**acl** <name> **permit|deny icmp** <SrcAddr/Mask> <DstAddr/Mask> <tos>

## Mode

Configure.

## Description

The **acl permit icmp** and **acl deny icmp** commands define an ACL to allow or block ICMP traffic from entering or leaving the X-Pedition router. For each parameter describing a flow, you can specify a value or use the keyword **any** to indicate a *wildcard* (“don’t care”) condition. When you specify only some of the parameters, the remaining fields will require the **any** keyword. If you do not specify any value for any field, the X-Pedition router applies a wildcard condition to every field, giving the same effect as if you specify the **any** keyword.

## Parameters

|                |   |
|----------------|---|
| <name>         | Name of this ACL. You can use a string of characters or a number.   |
| <SrcAddr/Mask> | Source address and filtering mask of this flow. If the source address is a network or subnet address, you must supply the filtering mask. Generally, the filtering mask is the network mask of this network or subnet. If the source address is that of a host then no mask is required. By default, if a mask is not supplied, the source address is treated as that of a host. You can specify the mask using the traditional IP address format (“255.255.0.0”) or the CIDR format (“/16”). |

|                                   |  |
|-----------------------------------|--|
| <code>&lt;DstAddr/Mask&gt;</code> | The destination address and the filtering mask of this flow. The same requirements and restrictions for <code>&lt;SrcAddr/Mask&gt;</code> apply to <code>&lt;DstAddr/Mask&gt;</code> .   |
| <code>&lt;tos&gt;</code>          | IP TOS (Type of Service) value. You can specify a TOS value from 0 – 255.  |
| <b>log</b>                        | This optional parameter allows you to enable ACL logging for this specific ACL rule. If logging is turned on when you apply the ACL to an interface (e.g., with the <a href="#">acl apply interface on page 3</a> ), you will override the rule-based logging values. In order to enable rule-based logging, the log option must remain off. |

## Restrictions

- When you apply an ACL to an interface, the X-Pedition router appends an *implicit deny rule* to that ACL. The implicit deny rule denies *all* traffic. If you intend to allow all traffic that doesn't match your specified ACL rules to go through, you must *explicitly* define a rule to permit all traffic.
- This type of ACL cannot be applied to IPv6 interfaces.
- You may not apply ACLs to interface EN0 of the control module.
- Users may not remove the last ACL rule for an ACL applied through the ACL editor to an interface unless they first remove the apply statement.

## Examples

To deny ICMP traffic from the subnet 10.24.5.0 (with a 24 bit netmask) to any destination:

```
xp(config)# acl 310 deny icmp 10.24.5.0/24 any
```

To create an ACL to permit ICMP traffic from the host 10.12.28.44 to subnet 10.43.21.0:

```
xp(config)# acl 312 permit icmp 10.12.28.44 10.43.21.0/24
```



# acl permit|deny igmp

## Purpose

Create an IGMP ACL.

## Format

**acl** <name> **permit|deny igmp** <SrcAddr/Mask> <DstAddr/Mask> <tos>

## Mode

Configure.

## Description

The **acl permit igmp** and **acl deny igmp** commands define an ACL to allow or block IGMP traffic from entering or leaving the X-Pedition router. For each parameter describing a flow, you can specify a value or use the keyword **any** to indicate a *wildcard* (“don’t care”) condition. When you specify only some of the parameters, the remaining fields will require the **any** keyword. If you do not specify any value for any field, the X-Pedition router applies a wildcard condition to every field, giving the same effect as if you specify the **any** keyword.

## Parameters

|                |   |
|----------------|---|
| <name>         | Name of this ACL. You can use a string of characters or a number.   |
| <SrcAddr/Mask> | The source address and the filtering mask of this flow. If the source address is a network or subnet address, you must supply the filtering mask. Generally, the filtering mask is the network mask of this network or subnet. If the source address is that of a host then no mask is required. By default, if a mask is not supplied, the source address is treated as that of a host. You can specify the mask using the traditional IP address format (“255.255.0.0”) or the CIDR format (“/16”). |
| <DstAddr/Mask> | The destination address and the filtering mask of this flow. The same requirements and restrictions for <SrcAddr/Mask> apply to <DstAddr/Mask>.   |
| <tos>          | IP TOS (Type of Service) value. You can specify a TOS value from 0 – 255.   |
| <b>log</b>     | This optional parameter allows you to enable ACL logging for this specific ACL rule.  |

## Restrictions

- When you apply an ACL to an interface, the X-Pedition router appends an *implicit deny rule* to that ACL. The implicit deny rule denies *all* traffic. If you intend to allow all traffic that doesn't match your specified ACL rules to go through, you must *explicitly* define a rule to permit all traffic.
- This type of ACL cannot be applied to IPv6 interfaces.
- Users may not remove the last ACL rule for an ACL applied through the ACL editor to an interface unless they first remove the apply statement.

## Examples

To create an ACL to deny IGMP traffic from the subnet 10.1.5.0 (with a 24 bit netmask) to any destination:

```
xp(config)# acl 410 deny igmp 10.1.5.0/24 any
```

To create an ACL to permit IGMP traffic from the host 10.33.34.44 to subnet 10.11.21.0:

```
xp(config)# acl 714 permit igmp 10.33.34.44 10.11.21.0/24
```

# acl permit|deny ip

## Purpose

Create an IPv4 ACL.

## Format

```
acl <name> permit|deny ip <SrcAddr/Mask> <DstAddr/Mask> <SrcPort> <DstPort> [<tos>]  
<tos-mask> any [log]
```

## Mode

Configure.

## Description

The **acl permit ip** and **acl deny ip** commands define an Access Control List to allow or block IPv4 traffic from entering or leaving the router. Unlike the more specific variants of the acl commands for **tcp** and **udp**, the IPv4 version of the command includes IP-based protocols such as **tcp**, **udp**, **icmp** and **igmp**. For each parameter describing a flow, you can specify a value or use the keyword **any** to indicate a *wildcard* (“don’t care”) condition. When you specify only some of the parameters, the remaining fields will require the **any** keyword. If you do not specify any value for any field, the X-Pedition router applies a wildcard condition to every field, giving the same effect as if you specify the **any** keyword.

The exception to this rule is the optional parameter *<tos>* (type of service). *<tos>* is a value from 0 to 255.

To create a ACL for IPv6 interfaces, use the **acl permit|deny ipv6** command.

## Parameters

|                |   |
|----------------|---|
| <name>         | Name of this ACL. You can use a string of characters or a number. The string must be less than 100 characters.  |
| <SrcAddr/Mask> | The source address and the filtering mask of this flow. If the source address is a network or subnet address, you must supply the filtering mask. Generally, the filtering mask is the network mask of this network or subnet. If the source address is that of a host then no mask is required. By default, if a mask is not supplied, the source address is treated as that of a host. You can specify the mask using the traditional IP address format (“255.255.0.0”) or the CIDR format (“/16”).   |
| <DstAddr/Mask> | The destination address and the filtering mask of this flow. The same requirements and restrictions for <SrcAddr/Mask> apply to <DstAddr/Mask>.   |
| <SrcPort>      | <p>For TCP or UDP, the number of the source TCP or UDP port. This field applies only to TCP or UDP traffic. If the incoming packet is ICMP or another non-TCP or non-UDP packet and you specified a source or destination port, the X-Pedition router does not check the port value. The router checks only the source and destination IP addresses in the packet.</p> <p>You can specify a range of port numbers using operator symbols; for example, 10-20 (between 10 and 20 inclusive), &gt;1024 (greater than 1024), &lt;1024 (less than 1024), !=1024 (not equal to 1024). The port numbers of some popular services are already defined as keywords. For example, for Telnet, you can enter the port number 23 as well as the keyword <b>telnet</b>.</p> |
| <DstPort>      | For TCP or UDP, the number of the destination TCP or UDP port. This field applies only to incoming TCP or UDP traffic. The same requirements and restrictions for <SrcPort> apply to <DstPort>.   |
| <tos>          | IP TOS (Type of Service) value. You can specify a TOS value from 0 – 255.   |
| <tos-mask>     | Mask value used for the TOS byte. You can specify a mask value from 0– 255. Default is <b>30</b> . Specify <b>any</b> for any TOS value.  |
| <b>log</b>     | This optional parameter allows you to enable ACL logging for this specific ACL rule.  |

## Restrictions

- When you apply an ACL to an interface, the X-Pedition router appends an *implicit deny rule* to that ACL. The implicit deny rule denies *all* traffic. If you intend to allow all traffic that doesn't match your specified ACL rules to go through, you must *explicitly* define a rule to permit all traffic.

- Users may not remove the last ACL rule for an ACL applied through the ACL editor to an interface unless they first remove the apply statement.

## Examples

To create an ACL to permit IP traffic from the subnet 10.1.0.0 (with a 16 bit netmask) to any destination:

```
xp(config)# acl 100 permit ip 10.1.0.0/16 any
```

The following command creates an ACL to deny any incoming TCP or UDP traffic coming from a privileged port (less than 1024). If the incoming traffic is not TCP or UDP, then the X-Pedition router checks only the source and destination addresses, not the port number. Therefore, this ACL will deny all non-TCP and non-UDP traffic.

```
xp(config)# acl 120 deny ip any any 1-1024 any
```

To create an ACL to permit Telnet traffic (port 23) from the host 10.23.4.8 to the subnet 10.2.3.0:

```
xp(config)# acl 130 permit ip 10.23.4.8 10.2.3.0/24
```

The following command creates an ACL to permit all IP traffic. Since none of the ACL fields are specified, they are all assumed to be wildcards.

```
xp(config)# acl allip permit ip
```

The above command is equivalent to the following:

```
xp(config)# acl allip permit ip any any any any
```

# acl permit|deny ipv6

## Purpose

Create an IPv6 ACL.

## Format

```
acl <name> [permit|deny] ipv6 <SrcIPv6Addr/PrefixLen> <DstIPv6Addr/PrefixLen> <tc> <nheader> [any]
```

## Mode

Configure.

## Description

The **acl permit ipv6** and **acl deny ipv6** commands define an Access Control List to allow or block IPv6 traffic from entering the router. For each parameter describing a flow, you must specify either a value or use the keyword **any** to indicate a *wildcard* (“don’t care”) condition. If you specify values for only some of the parameters, the remaining fields will require the **any** keyword.

To create an ACL for an IPv4 interface, use the **acl permit|deny ip** command.

## Parameters

|                         |  |
|-------------------------|--|
| <name>                  | Name of this ACL. You can use a string of characters or a number. The string must be less than 100 characters.                                   |
| <SrcIPv6Addr/PrefixLen> | The source IPv6 address and prefix length on which to filter. If the prefix length is not specified, the default length of 64 will be used.      |
| <DstIPv6Addr/PrefixLen> | The destination IPv6 address and prefix length on which to filter. If the prefix length is not specified, the default length of 64 will be used. |
| <tc>                    | The value of the Traffic Class field in the IPv6 header of the incoming packet on which to filter. The value can range from 0 to 255.            |
| <nheader>               | The value of the Next Header field in the IPv6 header of the incoming packet on which to filter. The value can range from 0 to 255.              |

## Restrictions

- When you apply an ACL to an interface, the X-Pedition router appends an *implicit deny rule* to that ACL. The implicit deny rule denies *all* traffic. If you intend to allow all traffic that doesn't match your specified ACL rules to go through, you must *explicitly* define a rule to permit all traffic.
- Users may not remove the last ACL rule for an ACL applied through the ACL editor to an interface unless they first remove the apply statement.

## Examples

To create an ACL to permit IPv6 traffic from the source address 3ed7:1234:3456:78ae::/64 to any destination:

```
xp(config)# acl 100 permit ipv6 3ed7:1234:3456:78ae::/64 any any any
```

# acl permit|deny ip-protocol

## Purpose

Create an ACL for any IP protocol type.

## Format

```
acl <name> permit|deny ip-protocol <proto-num> <SrcAddr/Mask> <DstAddr/Mask> <tos>
[log]
```

## Mode

Configure.

## Description

The **acl permit ip-protocol** and **acl deny ip-protocol** commands define an Access Control List to allow or block IP traffic from entering or leaving the router for any protocol type. Unlike the more specific variants of the acl commands such as **ip**, **tcp** and **udp**, the **ip-protocol** version of the command allows the user to specify any valid IP protocol type. This command allows the user to specify an IP protocol other than the ones available with other **acl permit|deny** commands. For example, to specify an ACL for IP encapsulation in IP, one can use the IPinIP protocol type, 4, in the ACL. For each parameter describing a flow, you can specify a value or use the keyword **any** to indicate a *wildcard* (“don’t care”) condition. When you specify only some of the parameters, the remaining fields will require the **any** keyword. If you do not specify any value for any field, the X-Pedition router applies a wildcard condition to every field, giving the same effect as if you specify the **any** keyword.

## Parameters

|                |   |
|----------------|---|
| <name>         | Name of this ACL. You can use a string of characters or a number.   |
| <proto-num>    | IP protocol number of this flow.  |
| <SrcAddr/Mask> | The source address and the filtering mask of this flow. If the source address is a network or subnet address, you must supply the filtering mask. Generally, the filtering mask is the network mask of this network or subnet. If the source address is that of a host then no mask is required. By default, if a mask is not supplied, the source address is treated as that of a host. You can specify the mask using the traditional IP address format (“255.255.0.0”) or the CIDR format (“/16”). |



|                                   |  |
|-----------------------------------|--|
| <code>&lt;DstAddr/Mask&gt;</code> | The destination address and the filtering mask of this flow. The same requirements and restrictions for <code>&lt;SrcAddr/Mask&gt;</code> apply to <code>&lt;DstAddr/Mask&gt;</code> . |
| <code>&lt;tos&gt;</code>          | IP TOS (Type of Service) value. You can specify a TOS from 0 – 255.  |
| <b>log</b>                        | This optional parameter allows you to enable ACL logging for this specific ACL rule.   |

## Restrictions

- When you apply an ACL to an interface, the X-Pedition router appends an *implicit deny rule* to that ACL. The implicit deny rule denies *all* traffic. If you intend to allow all traffic that doesn't match your specified ACL rules to go through, you must *explicitly* define a rule to permit all traffic.
- This type of ACL cannot be applied to IPv6 interfaces.
- Users may not remove the last ACL rule for an ACL applied through the ACL editor to an interface unless they first remove the apply statement.

## Examples

To create an ACL to permit VRRP traffic (IP protocol type 112) from the subnet 10.14.0.0 (with a 16 bit netmask) to any destination:

```
xp(config)# acl 100 permit ip-protocol 112 10.14.0.0/16 any
```

The following command has the same function as **acl 120 deny igmp** since the protocol type for IGMP is 2.

```
xp(config)# acl 120 deny ip-protocol 2
```

# acl permit|deny ipx

## Purpose

Create an IPX ACL.

## Format

```
acl <name> permit|deny ipx <SrcAddr> <SrcSocket> <DstAddr> <DstSocket> <SrcNetMask> <DstNetMask>
```

## Mode

Configure.

## Description

The **acl permit ipx** and **acl deny ipx** commands define an ACL to allow or block IPX traffic from entering or leaving the X-Pedition router.

## Parameters

|             |  |
|-------------|--|
| <name>      | Name of this ACL. You can use a string of characters or a number.  |
| <SrcAddr>   | <p>The source IPX address in &lt;network&gt;.&lt;node&gt; format, where &lt;network&gt; is the network address and &lt;node&gt; is the MAC address. The X-Pedition router will interpret this number in hexadecimal format. You do not need to use a “0x” prefix. You can use the keyword <b>any</b> to specify a wildcard (“don’t care”) condition.</p> <p>To specify any network, enter <b>FFFFFFFF</b>.&lt;node&gt;; to specify any node, enter &lt;network&gt;.<b>FF:FF:FF:FF:FF:FF</b>.</p> |
| <SrcSocket> | Source IPX socket. The X-Pedition router will interpret this number in hexadecimal format. You do not need to use a “0x” prefix. You can use the keyword <b>any</b> to specify a wildcard (“don’t care”) condition.  |
| <DstAddr>   | The destination IPX address in <network>.<node> format. The syntax for the destination address is the same as the syntax for the source address <SrcAddr>. The X-Pedition router will interpret this number in hexadecimal format. You do not need to use a “0x” prefix. You can use the keyword <b>any</b> to specify a wildcard (“don’t care”) condition.  |

|              |   |
|--------------|---|
| <DstSocket>  | Destination IPX socket. The X-Pedition router will interpret this number in hexadecimal format. You do not need to use a “0x” prefix. You can use the keyword <b>any</b> to specify a wildcard (“don’t care”) condition.  |
| <SrcNetmask> | Source network mask. This field specifies a group of networks for which the ACL applies. This mask field is ANDed with the network portion of <SrcAddr> and the source network of the incoming packets to determine a hit. The X-Pedition router will interpret this number in hexadecimal format. You do not need to use a “0x” prefix.<br><br>This is an optional argument and if you omit the argument, the X-Pedition router uses the hexadecimal value FFFFFFFF.           |
| <DstNetmask> | Destination network mask. This field specifies a group of networks for which the ACL applies. This mask field is ANDed with the network portion of <DstAddr> and the destination network of the incoming packets to determine a hit. The X-Pedition router will interpret this number in hexadecimal format. You do not need to use a “0x” prefix.<br><br>This is an optional argument and if you omit the argument, the X-Pedition router uses the hexadecimal value FFFFFFFF. |

## Restrictions

- When you apply an ACL to an interface, the X-Pedition router appends an *implicit deny rule* to that ACL. The implicit deny rule denies *all* traffic. If you intend to allow all traffic that doesn’t match your specified ACL rules to go through, you must *explicitly* define a rule to permit all traffic.
- Users may not remove the last ACL rule for an ACL applied through the ACL editor to an interface unless they first remove the apply statement.

## Examples

The following command creates an ACL to permit IPX traffic from the host with IPX address AAAAAAAA.01:20:0A:F3:24:6D, any socket, to any other IPX address (network.node), any socket.

```
xp(config)# acl 100 permit ipx AAAAAAAA.01:20:0A:F3:24:6D any any any
```

The following command creates an ACL to deny IPX traffic from the host with IPX address F6D5E4.01:20:0A:F3:24:6D, with socket address 451, to any other IPX address (network.node), any socket.

```
xp(config)# acl 200 deny ipx F6D5E4.01:20:0A:F3:24:6D 451 any any
```

# acl permit|deny ipxgns

## Purpose

Create an IPX GNS (Get Nearest Server) ACL.

## Format

**acl** <name> **permit|deny ipxgns** <ServerAddr> <ServiceType> <ServiceName>

## Mode

Configure.

## Description

The **acl permit ipxgns** and **acl deny ipxgns** commands define an ACL to allow or block replying to GNS requests.

## Parameters

|               |   |
|---------------|---|
| <name>        | Name of this ACL. You can use a string of characters or a number.   |
| <ServerAddr>  | The SAP server's IPX address in <network>.<node> format, where <network> is the network address and <node> is the MAC address. You can use the keyword <b>any</b> to specify a wildcard ("don't care") condition. |
| <ServiceType> | The SAP service type. Express the service type in hexadecimal. You do not need to use a "0x" prefix. You can use the keyword <b>any</b> to specify a wildcard ("don't care") condition.                           |
| <ServiceName> | The SAP service name. This is an optional argument and if you omit the argument, the X-Pedition router applies a wildcard condition to the field.   |

## Restrictions

- When you apply an ACL to an interface, the X-Pedition router appends an *implicit deny rule* to that ACL. The implicit deny rule denies **all** traffic. If you intend to allow all traffic that doesn't match your specified ACL rules to go through, you must *explicitly* define a rule to permit all traffic. You can only apply the **acl permit ipxgns** and **acl deny ipxgns** commands to output.
- Users may not remove the last ACL rule for an ACL applied through the ACL editor to an interface unless they first remove the apply statement.

## Examples

To create a GNS ACL to permit the X-Pedition router to reply with the server “FILESERVER”, whose IPX address is F6D5E4.01:20:0A:F3:24:5D, to get nearest server requests:

```
xp(config)# acl 100 permit ipxgns F6D5E4.01:20:0A:F3:24:5D 0004 FILESERVER
```

To create a GNS ACL to prevent the X-Pedition router from replying with the server “ARCHIVESERVER”, whose IPX address is F6D5E4.01:20:0A:F3:24:5C, to a get nearest server request:

```
xp(config)# acl 200 deny ipxgns F6D5E4.01:20:0A:F3:24:5C 0009 ARCHIVESERVER
```

# acl permit|deny ipxrip

## Purpose

Create an IPX RIP (Route Information Protocol) ACL.

## Format

**acl** <name> **permit|deny ipxrip** <FromNetwork> <ToNetwork>

## Mode

Configure.

## Description

The **acl permit ipxrip** and **acl deny ipxrip** commands define an ACL which allows or blocks IPX RIP traffic from entering or leaving the X-Pedition router.

## Parameters

|               |   |
|---------------|---|
| <name>        | Name of this ACL. You can use a string of characters or a number.   |
| <FromNetwork> | The “from” IPX network address. You can use the <b>any</b> keyword to specify a wildcard condition. If you use <b>any</b> , the X-Pedition router uses the value 0 for <FromNetwork> and FFFFFFFE for <ToNetwork>.  |
| <ToNetwork>   | <p>The “to” IPX network address. This is an optional parameter. If you omit this parameter, the value that the X-Pedition router assumes depends on whether you specified <b>any</b> for &lt;FromNetwork&gt;.</p> <ul style="list-style-type: none"><li>• If you omit the &lt;ToNetwork&gt; value and you used the value <b>any</b> for &lt;FromNetwork&gt;, the X-Pedition router sets the &lt;ToNetwork&gt; to FFFFFFFE.</li><li>• If you omit the &lt;ToNetwork&gt; value but do not use the value <b>any</b> for &lt;FromNetwork&gt;, the X-Pedition router sets &lt;ToNetwork&gt; to the same value you specified for &lt;FromNetwork&gt;.</li></ul> |

## Restrictions

- Please note that the rules within an ACL must belong to the same protocol family.

- When you apply an ACL to an interface, the X-Pedition router appends an *implicit deny rule* to that ACL. The implicit deny rule denies ***all*** traffic. If you intend to allow all traffic that doesn't match your specified ACL rules to go through, you must *explicitly* define a rule to permit all traffic.
- Users may not remove the last ACL rule for an ACL applied through the ACL editor to an interface unless they first remove the apply statement.

## Examples

To create an ACL to permit IPX RIP traffic from networks AA000001 to AFFFFFFF:

```
xp(config)# acl 100 permit ipxrip AA000001 AFFFFFFF
```

# acl permit|deny ipxsap

## Purpose

Create an IPX SAP (Service Advertisement Protocol) ACL.

## Format

**acl** <name> **permit|deny ipxsap** <ServerAddr> <ServiceType> <ServiceName>

## Mode

Configure.

## Description

The **acl permit ipxsap** and **acl deny ipxsap** commands define an ACL to allow or block IPX SAP traffic from entering or leaving the X-Pedition router.

## Parameters

|               |  |
|---------------|--|
| <name>        | Name of this ACL. You can use a string of characters or a number.  |
| <ServerAddr>  | The SAP server's IPX address in <network>.<node> format, where <network> is the network address and <node> is the MAC address. You can use the keyword <b>any</b> to specify a wildcard ("don't care") condition.<br><br>To specify any network, enter <b>FFFFFFFF.&lt;node&gt;</b> ; to specify any node, enter <network>. <b>FF:FF:FF:FF:FF:FF</b> . |
| <ServiceType> | The SAP service type. Express the service type in hexadecimal. You do not need to use a "0x" prefix. You can use the keyword <b>any</b> to specify a wildcard ("don't care") condition.  |
| <ServiceName> | The SAP service name. This is an optional argument and if you omit the argument, the X-Pedition router applies a wildcard condition to the field.  |

## Restrictions

- Please note that the rules within an ACL must belong to the same protocol family.



- When you apply an ACL to an interface, the X-Pedition router appends an *implicit deny rule* to that ACL. The implicit deny rule denies *all* traffic. If you intend to allow all traffic that doesn't match your specified ACL rules to go through, you must *explicitly* define a rule to permit all traffic.
- Users may not remove the last ACL rule for an ACL applied through the ACL editor to an interface unless they first remove the apply statement.

## Examples

To create a SAP ACL to permit SAP information related to the server "FILESERVER" whose IPX address is F6D5E4.01:20:0A:F3:24:5D:

```
xp(config)# acl 100 permit ipxsap F6D5E4.01:20:0A:F3:24:5D 0004 FILESERVER
```

To create a SAP ACL to deny SAP information related to the server "ARCHIVESERVER" whose IPX address is F6D5E4.01:20:0A:F3:24:5C:

```
xp(config)# acl 200 deny ipxsap F6D5E4.01:20:0A:F3:24:5C 0009 ARCHIVESERVER
```

## acl permit|deny ipxtype20

### Purpose

Create an IPX type 20 ACL.

### Format

**acl** <name> **permit|deny ipxtype20**

### Mode

Configure.

### Description

The **acl permit ipxtype20** and **acl deny ipxtype20** commands define an ACL to allow or block IPX type 20 packets from entering or leaving the X-Pedition router.

### Parameters

---

|        |   |
|--------|---|
| <name> | Name of this ACL. You may use a string of characters or a number. |
|--------|---|

---

### Restrictions

- Please note that the rules within an ACL must belong to the same protocol family.
- When you apply an ACL to an interface, the X-Pedition router appends an *implicit deny rule* to that ACL. The implicit deny rule denies *all* traffic. If you intend to allow all traffic that doesn't match your specified ACL rules to go through, you must *explicitly* define a rule to permit all traffic.
- Users may not remove the last ACL rule for an ACL applied through the ACL editor to an interface unless they first remove the apply statement.

### Examples

To create an ACL to deny IPX type 20 packets:

```
xp(config)# acl 100 deny ipxtype20
```

# acl permit|deny tcp

## Purpose

Create a TCP ACL.

## Format

```
acl <name> permit|deny tcp <SrcAddr/Mask> <DstAddr/Mask> <SrcPort> <DstPort> <tos>
<tos-mask> [established] [log]
```

## Mode

Configure.

## Description

The **acl permit tcp** and **acl deny tcp** commands define an ACL to allow or block TCP traffic from entering or leaving the X-Pedition router. For each parameter describing a flow, you can specify a value or use the keyword **any** to indicate a *wildcard* (“don’t care”) condition. When you specify only some of the parameters, the remaining fields will require the **any** keyword. If you do not specify any value for any field, the X-Pedition router applies a wildcard condition to every field, giving the same effect as if you specify the **any** keyword.

The exception to this rule is the optional parameter *<tos>* (type of service). *<tos>* is a value from 0 to 255.

## Parameters

|                             |  |
|-----------------------------|--|
| <i>&lt;name&gt;</i>         | Is the name of this ACL. You can use a string of characters or a number.   |
| <i>&lt;SrcAddr/Mask&gt;</i> | Is the source address and the filtering mask of this flow. If the source address is a network or subnet address, you must supply the filtering mask. Generally, the filtering mask is the network mask of this network or subnet. If the source address is that of a host then no mask is required. By default, if a mask is not supplied, the source address is treated as that of a host. You can specify the mask using the traditional IP address format (“255.255.0.0”) or the CIDR format (“/16”). |
| <i>&lt;DstAddr/Mask&gt;</i> | Is the destination address and the filtering mask of this flow. The same requirements and restrictions for <i>&lt;SrcAddr/Mask&gt;</i> apply to <i>&lt;DstAddr/Mask&gt;</i> .  |

|                               |  |
|-------------------------------|--|
| <code>&lt;SrcPort&gt;</code>  | For TCP or UDP, is the number of the source TCP or UDP port. <i>This field applies only to incoming TCP or UDP traffic.</i> You can specify a range of port numbers using operator symbols; for example, 10-20 (between 10 and 20 inclusive), >1024 (greater than 1024), <1024 (less than 1024), !=1024 (not equal to 1024). The port numbers of some popular services are already defined as keywords. For example, for Telnet, you can enter the port number 23 as well as the keyword <b>telnet</b> . |
| <code>&lt;DstPort&gt;</code>  | For TCP or UDP, is the number of the destination TCP or UDP port. <i>This field applies only to incoming TCP or UDP traffic.</i> The same requirements and restrictions for <code>&lt;SrcPort&gt;</code> apply to <code>&lt;DstPort&gt;</code> .   |
| <code>&lt;tos&gt;</code>      | Is the IP TOS (Type of Service) value. You can specify a TOS value from 0 – 255.   |
| <code>&lt;tos-mask&gt;</code> | Mask value used for the TOS byte. You can specify a mask value from 0– 255. Default is <b>30</b> . Specify <b>any</b> for any TOS value.   |
| <b>established</b>            | Allows TCP responses from external hosts, provided the connection was established internally.  |
| <b>log</b>                    | This optional parameter allows you to enable ACL logging for this specific ACL rule.   |

## Restrictions

- When you apply an ACL to an interface, the X-Pedition router appends an *implicit deny rule* to that ACL. The implicit deny rule denies **all** traffic. If you intend to allow all traffic that doesn't match your specified ACL rules to go through, you must *explicitly* define a rule to permit all traffic.
- This type of ACL cannot be applied to IPv6 interfaces.
- Users may not remove the last ACL rule for an ACL applied through the ACL editor to an interface unless they first remove the apply statement.

## Examples

To create an ACL to permit TCP traffic from the subnet 10.21.33.0 (with a 24 bit netmask) to any destination:

```
xp(config)# acl 100 permit tcp 10.21.33.0/255.255.255.0 any
```

To create an ACL to deny any incoming HTTP traffic:

```
xp(config)# acl noweb deny tcp any any http any
```

To create an ACL to permit FTP traffic (both command and data ports) from subnet 10.31.34.0 to 10.31.60.0:

```
xp(config)# acl ftp100 permit tcp 10.31.34.0/24 10.31.60.0/24 20-21 any
```

# acl permit|deny udp

## Purpose

Create a UDP ACL.

## Format

```
acl <name> permit|deny udp <SrcAddr/Mask> <DstAddr/Mask> <SrcPort> <DstPort> <tos>  
<tos-mask> [log]
```

## Mode

Configure.

## Description

The **acl permit udp** and **acl deny udp** commands define an ACL to allow or block UDP traffic from entering or leaving the X-Pedition router. For each parameter describing a flow, you can specify a value or use the keyword **any** to indicate a *wildcard* (“don’t care”) condition. When you specify only some of the parameters, the remaining fields will require the **any** keyword. If you do not specify any value for any field, the X-Pedition router applies a wildcard condition to every field, giving the same effect as if you specify the **any** keyword.

The exception to this rule is the optional parameter *<tos>* (type of service). *<tos>* is a value from 0 to 255.

## Parameters

|                |   |
|----------------|---|
| <name>         | Name of this ACL. You can use a string of characters or a number.   |
| <SrcAddr/Mask> | The source address and the filtering mask of this flow. If the source address is a network or subnet address, you must supply the filtering mask. Generally, the filtering mask is the network mask of this network or subnet. If the source address is that of a host then no mask is required. By default, if a mask is not supplied, the source address is treated as that of a host. You can specify the mask using the traditional IP address format (“255.255.0.0”) or the CIDR format (“/16”). |
| <DstAddr/Mask> | The destination address and the filtering mask of this flow. The same requirements and restrictions for <SrcAddr/Mask> apply to <DstAddr/Mask>.   |

|            |   |
|------------|---|
| <SrcPort>  | For TCP or UDP, the number of the source TCP or UDP port. <i>This field applies only to incoming TCP or UDP traffic.</i> You can specify a range of port numbers using operator symbols; for example, 10-20 (between 10 and 20 inclusive), >1024 (greater than 1024), <1024 (less than 1024), !=1024 (not equal to 1024). The port numbers of some popular services are already defined as keywords. For example, for Telnet, you can enter the port number 23 as well as the keyword <b>telnet</b> . |
| <DstPort>  | For TCP or UDP, the number of the destination TCP or UDP port. <i>This field applies only to incoming TCP or UDP traffic.</i> The same requirements and restrictions for <SrcPort> apply to <DstPort>.  |
| <tos>      | IP TOS (Type of Service) value. You can specify a TOS value from 0 – 255.   |
| <tos-mask> | Mask value used for the TOS byte. You can specify a mask value from 0– 255. Default is <b>30</b> . Specify <b>any</b> for any TOS value.  |
| <b>log</b> | This optional parameter allows you to enable ACL logging for this specific ACL rule.  |

## Restrictions

- When you apply an ACL to an interface, the X-Pedition router appends an *implicit deny rule* to that ACL. The implicit deny rule denies *all* traffic. If you intend to allow all traffic that doesn't match your specified ACL rules to go through, you must *explicitly* define a rule to permit all traffic.
- This type of ACL cannot be applied to IPv6 interfaces.
- Users may not remove the last ACL rule for an ACL applied through the ACL editor to an interface unless they first remove the apply statement.

## Examples

The following example creates an ACL to permit UDP traffic from the subnet 10.1.3.0 (with a 24 bit netmask) to any destination.

```
xp(config)# acl 100 permit udp 10.1.3.0/24 any
```

This example creates an ACL to deny any incoming TFTP traffic.

```
xp(config)# acl notftp deny udp any any tftp any
```

Creates an ACL to permit UDP based NFS traffic from subnet 10.12.0.0 to subnet 10.7.0.0.

```
xp(config)# acl udpnfs permit udp 10.12.0.0/16 10.7.0.0/16 any nfs
```

# acl-policy enable external

## Purpose

Allow an external server to create and delete ACLs.

## Format

**acl-policy enable external| policy-routing-external**

## Mode

Configure.

## Description

The **acl-policy enable** command allows ACLs to be configured by an external agent, such as the Policy Manager. If this command is in the active configuration, an external server can create, modify, and delete ACLs on the X-Pedition router. If this command is not in the active configuration, then ACLs can only be created, modified, and deleted using the CLI.

## Parameters

|                                |  |
|--------------------------------|--|
| <b>external</b>                | Enables ACLs to be configured by an external agent such as the Policy Manager.           |
| <b>policy-routing-external</b> | Enables policy routing to be configured by an external agent such as the Policy Manager. |

## Restrictions

The only action allowed by the **acl-policy enable external** command is to allow an external server to create, modify, and delete ACLs. Once entered, this command must be negated in order to prohibit an external server from creating, altering, or deleting ACLs. An external server can only modify ACLs that it created, or ACLs that were created using the CLI with the “external” flag. It cannot modify an ACL that was created using the CLI with the “local” flag.

This feature does not apply to IPv6 interfaces.



# acl show

## Purpose

Displays one or more ACLs.

## Format

```
acl show [aclname <string>|all] | [interface <string>|all-ip|all-ipv6|all-ipv6in4-tunnels] |
[service] | [port <port list>|all-ports] | [all]
```

## Mode

Enable.

## Description

The **acl show** command allows you to display the ACLs currently configured. Using the parameters associated with this command allows you to sort and display the ACLs by the name, interface, port, or service type.

You may also use the **acl show** command to display rules for Appletalk/ARE ACLs. Under this command, the Appletalk ACL is displayed in three separate sections. Each section provides information on configured zone, cable-range, and NBP rules, respectively. An *implicit deny* or *permit* rule is appended to the end of the ACL in all three sections. The third section, displaying Name Binding Protocol (NBP) rules, contains six fields:

1. **Forward:** Displays all permit and deny traffic.
2. **Count:** The number of times the ACL has been used to permit or deny traffic.
3. **Object, Type, and Zone:** The requested object, type, and zone names to be filtered. These parameters display as **object: type@zone**.
4. **Packet Type:** The type of NBP packet currently being filtered (broadcast request or forward request).

## Parameters

|                       |  |
|-----------------------|--|
| <b>aclname</b>        | Use this parameter to display ACLs by name.                          |
| <b>&lt;string&gt;</b> | The name of the ACL.   |
| <b>all</b>            | Specify <b>all</b> to display all ACLs.                              |
| <b>interface</b>      | Use this parameter to display ACLs attached to a specific interface. |
| <b>&lt;string&gt;</b> | The name of the interface.   |

|                            |   |
|----------------------------|---|
| <b>all-ip</b>              | Specify to display ACLs attached to all IPv4 interfaces.                |
| <b>all-ipv6</b>            | Specify to display ACLs attached to all IPv6 port-based interfaces.     |
| <b>all-ipv6in4-tunnels</b> | Specify to display ACLs attached to all IPv6-in-IPv4 tunnel interfaces. |
| <b>service</b>             | Use this parameter to display ACLs applied to services.                 |
| <b>port</b>                | Use this parameter to display ACLs applied to a specified port(s).      |
| <i>&lt;port list&gt;</i>   | The list of port(s) or SmartTRUNK(s).                                   |
| <b>all-ports</b>           | Specify <b>all</b> to display ACLs applied to all ports.                |
| <b>all</b>                 | Use this parameter to display all ACLs.                                 |

## Restrictions

You may sort Appletalk/ARE ACLs by **aclname** and **interface** only.

You may display IPv6 ACLs by **aclname** and **interface** only.

# Chapter 2

## acl-edit Commands

The **acl-edit** command activates the ACL Editor mode. The ACL Editor provides a user-friendly interface for maintaining and manipulating rules in an ACL. Using the editor, you can add, delete or re-order ACL rules. In addition, if the modified ACL is currently applied to an interface, the ACL is automatically “re-applied” to the interface and takes effect immediately. To edit an ACL, you enter the **acl-edit** command in Configure mode. The command must also specify the name of the ACL you want to edit. Only one ACL can be edited at one time.

**Note:** You may also use the ACL Editor to maintain and manipulate Appletalk/ARE (Advanced Routing Engine) ACL rules. In order to do this, however, you must be in **ARE-Configure** mode. For more information on this mode, please see [Chapter 6, are Commands](#).

### Command Summary

[Table 2](#) lists the commands available with the ACL Editor. The sections following the table describe the command syntax.

**Table 2. acl-edit Commands**

|  |
|--|
| <b>acl-edit</b> <aclname>                |
| <b>acl</b> permit deny                   |
| <b>delete</b> <rule#>                    |
| <b>exit</b>                              |
| <b>move</b> <rule#> <b>after</b> <rule#> |
| <b>save</b>                              |
| <b>show</b>                              |

# acl-edit

## Purpose

Enter ACL Editor to edit the specified ACL.

## Format

**acl-edit** <aclname>

## Mode

Configure.

## Description

The **acl-edit** command enters the ACL Editor to edit an ACL specified by the user. Once inside the ACL editor, the user can then add, delete or re-order ACL rules for that ACL. If the ACL happens to be applied to an interface, changes made to that ACL will automatically take effect when the changes are committed to the running system.

## Parameters

---

|           |                          |
|-----------|--------------------------|
| <aclname> | Name of the ACL to edit. |
|-----------|--------------------------|

---

## Restrictions

- Inside the ACL Editor, you can only add rules for the ACL you specified in the **acl-edit** command. You cannot add rules for other ACLs. Basically, each ACL editing session works only on one ACL at a time. For example, if you start with *acl-edit 110*, you cannot add rules for ACL *121*.
- Users may not remove the last ACL rule for an ACL applied through the ACL editor to an interface unless they first remove the **apply** statement.

## Example

To edit ACL 111:

```
xp(config)# acl-edit 111
xp(acl-edit)> ?
acl          - Configure L3 Access Control List
delete       - Delete an ACL rule
exit         - Exit current mode
help         - Describe online help facility
move         - Move an ACL rule
save         - Save changes made to this ACL
show         - Show contents of this ACL
xp(acl-edit)>
```

# acl permit| deny

## Purpose

Create an ACL rule to permit or deny traffic.

## Format

**acl** <name> **permit|deny**

## Mode

ACL Editor.

## Description

The **acl permit| deny** commands are equivalent to the same commands in the Configuration mode. You can use these commands to create rules for the ACL that you are editing. Just like the **acl** commands in Configuration mode, new rules are appended to the end of the rules. You can use the **move** command to re-order the rules.

## Restrictions

You can only add rules for the ACL you specified in the **acl-edit** command. You cannot add rules for other ACLs. For example, if you start with *acl-edit 110*, you cannot add rules for ACL *121*.

## Example

To add a new rule (deny all UDP traffic) to ACL 111:

```
xp(config)# acl-edit 111
xp(acl-edit)> show
  1*: acl 111 permit tcp 10.1.15.0/24 10.1.11.0/24 2000-2002 any
  2*: acl 111 permit tcp 10.1.15.0/24 10.1.11.0/24 2003-2005 any
xp(acl-edit)> acl 111 deny udp
xp(acl-edit)> show
  1*: acl 111 permit tcp 10.1.15.0/24 10.1.11.0/24 2000-2002 any
  2*: acl 111 permit tcp 10.1.15.0/24 10.1.11.0/24 2003-2005 any
  3*: acl 111 deny udp
xp(acl-edit)>
```

# delete

## Purpose

Deletes one or more rules from an ACL.

## Format

**delete** <rule#>

## Mode

ACL Editor.

## Description

The **delete** command allows the administrator to delete one or more specific rules from an ACL. When in the ACL Editor, each rule is displayed with its rule number. Users can delete rules from an ACL by specifying rule numbers with the delete command.

## Parameters

---

|         |  |
|---------|--|
| <rule#> | The number of the ACL rule(s) to delete. |
|---------|--|

---

## Restrictions

- If the ACL is referenced by any other command in the configuration, the ACL Editor will allow users to delete all but one ACL rule. Users can delete the last ACL rule only from the ACL once the reference to the ACL by another command is removed from the configuration.
- Users may not remove the last ACL rule for an ACL applied through the ACL editor to an interface unless they first remove the apply statement.

## Example

To delete ACL rule number 2 from the ACL:

```
xp(config)# acl-edit 111
xp(acl-edit)> show
1*: acl 111 permit tcp 10.1.15.0/24 10.1.11.0/24 2000-2002 any
2*: acl 111 permit tcp 10.1.15.0/24 10.1.11.0/24 2003-2005 any
3*: acl 111 deny udp
xp(acl-edit)> delete 2
xp(acl-edit)> show
1*: acl 111 permit tcp 10.1.15.0/24 10.1.11.0/24 2000-2002 any
2*: acl 111 deny udp
xp(acl-edit)>
```

To delete ACL rules 1-3 and 6 from the ACL:

```
xp(config)# acl-edit 222
xp(acl-edit)> show
1*: acl 222 permit tcp 10.1.15.0/24 10.1.11.0/24 2000-2002 any
2*: acl 222 permit tcp 10.1.15.0/24 10.1.11.0/24 2003-2005 any
3*: acl 222 permit tcp 10.1.15.0/24 10.1.11.0/24 2006-2010 any
4*: acl 222 permit tcp 10.1.16.0/24 10.1.11.0/24 2000-2002 any
5*: acl 222 permit tcp 10.1.16.0/24 10.1.11.0/24 2003-2005 any
6*: acl 222 deny udp
xp(acl-edit)> delete 1-3,6
xp(acl-edit)> show
1*: acl 222 permit tcp 10.1.16.0/24 10.1.11.0/24 2000-2002 any
2*: acl 222 permit tcp 10.1.16.0/24 10.1.11.0/24 2003-2005 any
xp(acl-edit)>
```



# exit

## Purpose

Exit ACL Editor.

## Format

**exit**

## Mode

ACL Editor.

## Description

The **exit** command allows the user to exit the ACL Editor. Before exiting, if changes are made to this ACL, the system will prompt the user to see if the changes should be committed to the running system or discarded. If the user commits the changes then changes made to this ACL will take effect immediately. If the ACL is applied to an interface, the ACL is automatically re-applied to the interface. Packets going through this interface will be matched against the new rules in this ACL. If the user chooses not to commit the changes, the changes will be discarded. The next time the user edits this ACL, changes from the previous edit session will be lost.

## Parameters

None.

## Restrictions

None.

## Example

To exit the ACL editor:

```
xp(config)# acl-edit 111
xp(acl-edit)> show
 1*: acl 111 permit tcp 10.1.15.0/24 10.1.11.0/24 2000-2002 any
 2*: acl 111 permit tcp 10.1.15.0/24 10.1.11.0/24 2003-2005 any
 3*: acl 111 deny udp
xp(acl-edit)> delete 3
xp(acl-edit)> show
 1*: acl 111 permit tcp 10.1.15.0/24 10.1.11.0/24 2000-2002 any
 2*: acl 111 permit tcp 10.1.15.0/24 10.1.11.0/24 2003-2005 any
xp(acl-edit)> exit
Do you want to commit your ACL changes (yes: commit, no: discard) [yes]? no
xp(config)#
```

## move

### Purpose

Re-order ACL rules by moving a rule to another position.

### Format

**move** <src-rule#> **after** <dst-rule#>

### Mode

ACL Editor.

### Description

The **move** command provides the user with the ability to re-order rules within an ACL. When new rules are entered in the ACL Editor, they are appended to the end of the rules. One can move these rules to the desired location by using the move command. The move command can also be used on existing ACL rules created in Configuration mode instead of the ACL Editor.

### Parameters

|             |  |
|-------------|--|
| <src-rule#> | Rule number of the rule you want to move.                                |
| <dst-rule#> | Rule number of the rule after which you want the source rule to move to. |

### Restrictions

None.

## Example

To move rule #2 to the end of the list:

```
xp(config)# acl-edit 111
xp(acl-edit)> show
 1*: acl 111 permit tcp 10.1.15.0/24 10.1.11.0/24 2000-2002 any
 2*: acl 111 permit tcp 10.1.15.0/24 10.1.11.0/24 2003-2005 any
 3*: acl 111 deny udp
xp(acl-edit)> move 2 after 3
xp(acl-edit)> show
 1*: acl 111 permit tcp 10.1.15.0/24 10.1.11.0/24 2000-2002 any
 2*: acl 111 deny udp
 3*: acl 111 permit tcp 10.1.15.0/24 10.1.11.0/24 2003-2005 any
xp(acl-edit)>
```

## save

### Purpose

Save any changes made by the ACL Editor.

### Format

**save**

### Mode

ACL Editor.

### Description

The **save** command saves any non-committed changes made by the ACL Editor. If changes are made to this ACL, the changes will be saved and will take effect immediately. If the ACL is applied to an interface, the ACL is automatically re-applied to the interface. Packets going through this interface will be matched against the new rules in this ACL. The **save** command also contains an implicit exit command. Regardless of whether changes were made by the ACL Editor or not, upon completion of the **save** command, the user exits the ACL Editor and returns to Configuration mode. Consequently, one should issue the **save** command after all the changes are made.

### Parameters

None.

### Restrictions

None.

## Example

To save and commit the changes made by the ACL Editor.

```
xp(config)# acl-edit 111
xp(acl-edit)> show
 1*: acl 111 permit tcp 10.1.15.0/24 10.1.11.0/24 2000-2002 any
 2*: acl 111 permit tcp 10.1.15.0/24 10.1.11.0/24 2003-2005 any
 3*: acl 111 deny udp
xp(acl-edit)> delete 2
xp(acl-edit)> show
 1*: acl 111 permit tcp 10.1.15.0/24 10.1.11.0/24 2000-2002 any
 2*: acl 111 deny udp
xp(acl-edit)> save
2003-04-29 14:38:33 %ACL-A-MODIFIED, ACL (111) modified.
xp(config)#
```

# show

## Purpose

Displays the contents of the ACL in the current editing session.

## Format

**show**

## Mode

ACL Editor.

## Description

The **show** command displays the contents of the ACL currently being edited.

## Parameters

None.

## Restrictions

None.

## Example

To display the contents of the ACL currently being edited:

```
xp(config)# acl-edit 111
xp(acl-edit)> show
 1*: acl 111 permit tcp 10.1.15.0/24 10.1.11.0/24 2000-2002 any
 2*: acl 111 permit tcp 10.1.15.0/24 10.1.11.0/24 2003-2005 any
 3*: acl 111 deny udp
xp(acl-edit)>
```





# Chapter 3

## aging Commands

The **aging** commands control aging of learned MAC address entries in the X-Pedition router's Layer-2 lookup tables or Layer-3 and Layer-4 flows. Using the **aging** commands, you can show Layer-2 or Layer-3 and Layer-4 aging information, set or disable Layer-2 aging on specific ports, set or disable aging of Layer-3 and Layer-4 flows, or set or disable NAT or LSNAT flows.

**Note:** Interfaces configured with PVCs do not support LSNAT.

### Command Summary

[Table 3](#) lists the **I2** and **I3** aging commands. The sections following the table describe the command syntax.

**Table 3. aging Commands**

|  |
|--|
| <b>aging I2 disable</b> <port-list> all-ports                          |
| <b>aging I2 set aging-timeout</b> <seconds> port <port-list> all-ports |
| <b>aging I2 show status</b>  |
| <b>aging I3 set timeout</b> <seconds> disable                          |
| <b>aging I3 set nat-flow-timeout</b> <minutes> disable                 |
| <b>aging I3 show status</b>  |

# aging l2 disable

## Purpose

Disable aging of MAC addresses.

## Format

**aging l2 disable** <port-list>|**all-ports**

## Mode

Configure.

## Description

By default, the X-Pedition router ages learned MAC addresses in the Layer-2 lookup tables. Each port has its own Layer-2 lookup table. When a learned entry ages out, the router removes the aged out entry. You can disable this behavior by disabling aging on all ports or on specific ports.

## Parameters

|                                  |  |
|----------------------------------|--|
| <port-list> <br><b>all-ports</b> | The port(s) on which you want to disable aging. You can specify a single port or a comma-separated list of ports. If you use the <b>all-ports</b> keyword, aging is disabled on all ports. |
|----------------------------------|--|

## Restrictions

Unknown.

## Examples

To disable aging on slot 1, port 3:

```
xp(config)# aging l2 disable et.1.3
```

To disable aging on slot 4, port 2, and slots 1 through 3, ports 4, 6, 7, and 8:

```
xp(config)# aging l2 disable et.4.2,et.(1-3).(4,6-8)
```

To disable aging on all ports:

```
xp(config)# aging l2 disable all-ports
```

# aging l2 set aging-timeout

## Purpose

Set the aging time for learned MAC entries.

## Format

**aging l2 set** <port-list>|**all-ports** **aging-timeout** <seconds>

## Mode

Configure.

## Description

The **aging l2 set aging-timeout** command sets the aging time for learned MAC entries. When the aging time expires for a MAC address, the X-Pedition router removes the MAC address from the specified port(s). The aging time is specified in seconds.

## Parameters

|                                  |   |
|----------------------------------|---|
| <port-list> <br><b>all-ports</b> | The port(s) on which you want to set the aging time. You can specify a single port or a comma-separated list of ports. If you use the <b>all-ports</b> keyword, the aging time is set on all ports.         |
| <seconds>                        | The number of seconds the X-Pedition router allows a learned MAC address to remain in the L2 lookup table (for the specified port). You can specify from 15 to 1000000 seconds. The default is 300 seconds. |

## Restrictions

None.

## Example

To set the aging time to 15 seconds on all ports:

```
xp(config)# aging l2 set all-ports aging-timeout 15
```

# **aging l2 show status**

## **Purpose**

Show the L2 aging status for X-Pedition ports.

## **Format**

**aging l2 show status**

## **Mode**

User.

## **Description**

The **aging l2 show status** command shows whether L2 aging is enabled or disabled on X-Pedition ports. For ports on which L2 aging is enabled, this command also shows the aging time.

## **Parameters**

None.

## **Restrictions**

None.

# aging l3 set timeout

## Purpose

Set the aging time for a Layer-3 or Layer-4 flow.

## Format

**aging l3 set timeout** <seconds>|**disable**

## Mode

Configure.

## Description

The **aging l3 set timeout** command sets the aging time for a Layer-3 or Layer-4 flow. The aging time is specified in seconds.

## Parameters

|                |  |
|----------------|--|
| <seconds>      | The number of seconds the X-Pedition router allows for a Layer-3 or Layer-4 flow. You can specify a value from 4 to 3600 seconds. For example, in an ISP environment (where thousands of flows are possible), you could change this value to 180-300 (3-5 minutes) to help in keeping with longer-term flows. The default is 30 seconds. |
| <b>disable</b> | Disables Layer-3 and Layer-4 aging.  |

## Restrictions

None.

## Example

To set the Layer-3 or Layer-4 flow aging time to 300 seconds (5 minutes):

```
xp(config)# aging l3 set timeout 60
```

# aging l3 set nat-flow-timeout

## Purpose

Set the aging time for NAT and LSNAT flows.

## Format

**aging l3 set nat-flow-timeout** <minutes>|disable

## Mode

Configure.

## Description

The **aging l3 set nat-flow-timeout** command sets the aging time for Network Address Translation (NAT) and Load Sharing NAT flows. The aging time is specified in minutes.

## Parameters

|           |   |
|-----------|---|
| <minutes> | The number of minutes the X-Pedition router allows for NAT and LSNAT flows. You can specify from 2 to 1440 minutes. The default is 2 minutes. |
| disable   | Disables NAT and LSNAT flow aging.  |

## Restrictions

Interfaces configured with PVCs do not support LSNAT.

## Example

To set the NAT aging time to 5 minutes:

```
xp(config)# aging l3 set nat-flow-timeout 5
```

## aging l3 show status

### Purpose

Show the L3 aging status for X-Pedition ports.

### Format

**aging l3 show status**

### Mode

User.

### Description

The **aging l3 show status** command shows whether Layer-3 or Layer-4 aging is enabled or disabled on X-Pedition ports. For ports on which Layer-3 or Layer-4 aging is enabled, this command also shows the aging time.

### Parameters

None.

### Restrictions

None.

### Example

To show whether Layer-3 or Layer-4 aging is enabled and display the aging time for enabled ports:

```
xp# aging l3 show status  
L3 Aging: Timeout 30 seconds
```



# Chapter 4

## appletalk Commands

The **appletalk** commands allow the user to manipulate the AppleTalk Protocol for an Advanced Routing Engine (ARE) module. Before using any of the commands in this chapter, you must first execute the command **are enable protocol appletalk module** *<module-number>* from the Configuration mode. For more information on the **are enable protocol appletalk** command, see [Chapter 6, are Commands](#).

### Command Summary

[Table 4](#) lists the **appletalk** commands. The sections following the table describe the command syntax.

**Table 4. appletalk Commands**

|  |
|--|
| <b>appletalk aarp clear address</b> <i>&lt;Net.Node&gt;</i>  all   |
| <b>appletalk aarp show address</b> <i>&lt;Net.Node&gt;</i>  all  |
| <b>appletalk ping</b> <i>&lt;address&gt;</i> [ <b>packets</b> <i>&lt;num&gt;</i> ] [ <b>size</b> <i>&lt;packet-size&gt;</i> ] [ <b>wait</b> <i>&lt;seconds&gt;</i> ] |
| <b>appletalk qos internal-queue-priority</b> <i>&lt;priority&gt;</i>   |
| <b>appletalk show aarp-globals</b>   |
| <b>appletalk show interfaces</b> <i>&lt;InterfaceName&gt;</i>  all   |
| <b>appletalk show routes interface</b> <i>&lt;InterfaceName&gt;</i>  all   |
| <b>appletalk show rtmp-jitter</b>  -status -update-interval -valid-interval  |
| <b>appletalk show zip-query-interval</b>   |
| <b>appletalk show zone interface</b> <i>&lt;InterfaceName&gt;</i>  all   |
| <b>appletalk show zone network</b> <i>&lt;range&gt;</i>  all   |

# appletalk aarp clear

## Purpose

Removes the specified AppleTalk Address Resolution Protocol (AARP) entries.

## Format

**appletalk aarp clear address** <Net.Node>|**all**

## Mode

Enable.

## Description

The **appletalk aarp clear** command allows the user to remove specific AppleTalk AARP entries from the AppleTalk AARP tables. This command will not remove permanent AARP entries (such as those created with the **appletalk add aarp** command).

## Parameters

---

|                           |   |
|---------------------------|---|
| <b>address</b> <Net.Node> | Specifies AppleTalk AARP entry to remove. Specifying <b>all</b> will remove all AppleTalk AARP entries. |
|---------------------------|---|

---

## Restrictions

None.

## Example

To remove AppleTalk AARP entry 1.2:

|   |
|---|
| xp# <b>appletalk aarp clear address 1.2</b> |
|---|

# appletalk aarp show

## Purpose

Displays the specified AppleTalk Address Resolution Protocol (AARP) entries.

## Format

**appletalk aarp show address** *<Net.Node>* | **all**

## Mode

Enable.

## Parameters

---

|  |   |
|--|---|
| <b>address</b> <i>&lt;Net.Node&gt;</i> | Specifies AppleTalk AARP entry to display. Specifying <b>all</b> will display all AppleTalk AARP entries. |
|--|---|

---

## Restrictions

None.

# appletalk ping

## Purpose

Tests connection for the specified AppleTalk address.

## Format

**appletalk ping** <address> [**packets** <num>] [**size** <packet-size>] [**wait** <seconds>]

## Mode

Enable.

## Description

The **appletalk ping** command allows the user to test the connection between the router and a specific AppleTalk address.

## Parameters

|                           |  |
|---------------------------|--|
| <address>                 | Specifies AppleTalk address you want to ping.  |
| <b>packets</b> <num>      | Specifies total number of packets to send. The default is 1.                                       |
| <b>size</b> <packet-size> | Specifies the size of each packet. This number must lie between 0 and 585. The default size is 20. |
| <b>wait</b> <seconds>     | Specifies the number of seconds to wait for all ping responses to arrive. The default is 1.        |

## Restrictions

None.

## Example

To ping AppleTalk address 1.2:

```
xp# appletalk ping 1.2
```

To ping the same AppleTalk address 5 times with packets 100 bytes in length, with a wait time of 3 seconds before displaying the ping response:

|   |
|---|
| <code>xp# appletalk ping 1.2 packets 5 size 100 wait 3</code> |
|---|

# appletalk qos internal-queue-priority

## Purpose

This command allows users to prioritize AppleTalk traffic.

## Format

**appletalk qos internal-queue-priority** <priority>

## Mode

ARE Configure.

## Description

Sets the internal queue priority for all forwarded AppleTalk traffic.

## Parameter

|            |   |
|------------|---|
| <priority> | Possible priorities are <b>low-priority</b> , <b>med-priority</b> , <b>high-priority</b> , and <b>control-priority</b> . The default priority level for AppleTalk traffic is low. |
|------------|---|

## Restrictions

None.

## Example

To set the priority for all forwarded AppleTalk traffic to medium, enter the following:

```
xp(config)# appletalk qos internal-queue-priority med-priority
```

# **appletalk show aarp-globals**

## **Purpose**

Displays all AppleTalk AARP settings.

## **Format**

**appletalk show aarp-globals**

## **Mode**

Enable.

## **Parameters**

None.

## **Restrictions**

None.

# appletalk show interfaces

## Purpose

Displays AppleTalk interfaces defined on the system.

## Format

**appletalk show interfaces** *<InterfaceName>*|**all**

## Mode

Enable.

## Parameters

|                              |  |
|------------------------------|--|
| <i>&lt;InterfaceName&gt;</i> | Specifies an interface to display.     |
| <b>all</b>                   | Displays all interfaces on the system. |

**Note:** Enterasys recommends that you use alphabetic characters when defining interface names, since purely numeric interfaces will be interpreted as IP addresses. The X-Pedition router will display interface names up to 32 characters in length.

## Restrictions

None.



# appletalk show routes

## Purpose

Displays AppleTalk routing table for system interface(s).

## Format

**appletalk show routes interface** <InterfaceName>|**all**

## Mode

Enable.

## Description

The **appletalk show routes** command shows the user the AppleTalk routing table for all interfaces, or a specified interface. If you choose the **all** parameter, the entire routing table will be shown. If you choose to display a specific interface, the commands will show the entire routing table *minus* any routes filtered for that interface.

## Parameters

|                 |   |
|-----------------|---|
| <InterfaceName> | Specifies an interface for which to display routing table. If a specific interface is entered, the routing table will not include routes which are filtered for that interface. |
| <b>all</b>      | Displays all interfaces on the system.  |

**Note:** Enterasys recommends that you use alphabetic characters when defining interface names, since purely numeric interfaces will be interpreted as IP addresses. The X-Pedition router will display interface names up to 32 characters in length.

## Restrictions

None.

## Example

To display the routing table for interface “app3”:

```
xp# appletalk show routes interface app3
```

# appletalk show rtmp

## Purpose

Displays various Routing Table Maintenance Protocol (RTMP) statistics.

## Format

**appletalk show rtmp-jitter|-status|-update-interval|-valid-interval**

## Mode

Enable.

## Description

The **appletalk show rtmp** command shows the user statistics for the RTMP, including functions defined by the **appletalk rtmp** command.

## Parameters

|                        |  |
|------------------------|--|
| <b>jitter</b>          | Displays RTMP jitter statistics.   |
| <b>status</b>          | Displays the RTMP status for each interface. This status shows whether RTMP and split-horizon are enabled or disabled. |
| <b>update-interval</b> | Displays, in seconds, the currently set interval between the sending of RTMP updates.                                  |
| <b>valid-interval</b>  | Displays, in seconds, the currently set interval during which an RTMP route is considered valid.                       |

## Restrictions

None.

# **appletalk show zip-query-interval**

## **Purpose**

Displays the currently set number of seconds between Zone Information Protocol (ZIP) queries.

## **Format**

**appletalk show zip-query-interval**

## **Mode**

Enable.

## **Description**

The **appletalk show zip-query-interval** command shows the user the currently set interval between ZIP queries, as defined by the **appletalk zip query-interval** command.

## **Parameters**

None.

## **Restrictions**

None.

# appletalk show zone interface

## Purpose

Displays all zones for specified interface(s).

## Format

**appletalk show zone interface** *<InterfaceName>***|all**

## Mode

Enable.

## Description

The **appletalk show zone interface** command shows the user all zones for specified interfaces on the router. Zones derived from other routers on the network will not be displayed.

## Parameters

|                              |  |
|------------------------------|--|
| <i>&lt;InterfaceName&gt;</i> | Specifies the interface for which you would like to see zone statistics. |
| <b>all</b>                   | Displays zones for all interfaces on the router.                         |

**Note:** Enterasys recommends that you use alphabetic characters when defining interface names—purely numeric interfaces will be interpreted as IP addresses. The X-Pedition router will display interface names up to 32 characters in length.

## Restrictions

None.

## Examples

To display zones for interface “app7”:

```
xp# appletalk show zone interface app7
```

To display zones for all interfaces:

```
xp# appletalk show zones interface all
```

# appletalk show zone network

## Purpose

Displays all zones for specified cable range(s).

## Format

**appletalk show zone network** *<range>*|**all**

## Mode

Enable.

## Description

The **appletalk show zone network** command shows the user all zones for specified cable ranges on the router. If the keyword **all** is specified, command will display all known zones on the entire network.

## Parameters

|                      |  |
|----------------------|--|
| <i>&lt;range&gt;</i> | Specifies the cable range for which you would like to see zone statistics. Valid numbers include 1 to 65279. |
| <b>all</b>           | Displays zones from the entire network.  |

## Restrictions

None.

## Examples

To display zones for range 10-100:

```
xp# appletalk show zone network 10-100
```

To display zones from the entire network:

```
xp# appletalk show zones network all
```



# Chapter 5

## appletalk Configuration Commands

The **appletalk** configuration commands allow the user to configure the AppleTalk Protocol for an Advanced Routing Engine (ARE) module. Before using any of the commands in this chapter, you must first execute the command **are enable protocol appletalk module** *<module-number>* from the Configuration mode. Then you must enter the ARE-Configuration mode. These commands can be used *only* from the ARE-Configuration mode. For more information on the **are enable protocol appletalk** command and ARE-Configuration mode, see [Chapter 6, are Commands](#).

### Command Summary

[Table 5](#) lists the appletalk configuration commands. The sections following the table describe the command syntax.

**Table 5. appletalk Configuration Commands**

|  |
|--|
| <b>appletalk add aarp exit-port</b> <i>&lt;port&gt;</i> <b>address</b> <i>&lt;Net.Node&gt;</i> <b>macaddr</b> <i>&lt;MACAddr&gt;</i>   |
| <b>appletalk add route interface</b> <i>&lt;InterfaceName&gt;</i> <b>cable-range</b> <i>&lt;range&gt;</i> <b>gateway</b> <i>&lt;Net.Node&gt;</i> <b>distance</b> <i>&lt;hops&gt;</i> |
| <b>appletalk aarp interval</b> <i>&lt;seconds&gt;</i>  |
| <b>appletalk aarp timeout</b> <i>&lt;seconds&gt;</i>   |
| <b>appletalk checksum disable</b>  |
| <b>appletalk rtmp jitter</b> <i>&lt;percent&gt;</i>  |
| <b>appletalk rtmp update-disable interface</b> <i>&lt;InterfaceName&gt;</i> <b>all</b>   |
| <b>appletalk rtmp update-interval</b> <i>&lt;seconds&gt;</i>   |

**Table 5. appletalk Configuration Commands (Continued)**

|  |
|--|
| <b>appletalk rtmp valid-interval</b> <seconds> |
| <b>appletalk split-horizon disable</b>         |
| <b>appletalk zip query-interval</b> <seconds>  |



# appletalk add aarp

## Purpose

Creates a permanent AppleTalk Address Resolution Protocol (ARP) entry.

## Format

**appletalk add aarp exit port** *<port>* **address** *<Net.Node>* **macaddr** *<MACAddr>*

## Mode

ARE-Configure.

## Description

The **appletalk add aarp** command allows the user to create a permanent AppleTalk ARP entry.

## Parameters

|  |  |
|--|--|
| <b>exit-port</b> <i>&lt;port&gt;</i>     | Specifies port for which to send any packet destined for the following address.  |
| <b>address</b> <i>&lt;Net.Node&gt;</i>   | Specifies AppleTalk address to associate with the following MAC address.   |
| <b>macaddr</b><br><i>&lt;MACAddr&gt;</i> | Specifies MAC address to associate with the previous AppleTalk address. MAC address should be entered in the following format:<br>xx:xx:xx:xx:xx:xx. |

## Restrictions

You must be in ARE-Configure mode before using this command.

# appletalk add route

## Purpose

Adds a static route to the routing table.

## Format

**appletalk add route interface** *<InterfaceName>* **cable-range** *<range>* **gateway** *<Net.Node>*  
**distance** *<hops>*

## Mode

ARE-Configure.

## Description

The **appletalk add route** command allows the user to add a static route to the routing table.

## Parameters

|  |   |
|--|---|
| <b>interface</b><br><i>&lt;InterfaceName&gt;</i> | Specifies the interface through which packets will be routed.   |
| <b>cable-range</b> <i>&lt;range&gt;</i>          | Specifies range of network numbers which can be reached through this route. Valid numbers include 1 to 65279. |
| <b>gateway</b> <i>&lt;Net.Node&gt;</i>           | Specifies the address of the next router a packet destined for the cable range will encounter.                |
| <b>distance</b> <i>&lt;hops&gt;</i>              | Specifies how many routers a packet must encounter before reaching its final destination.                     |

**Note:** Enterasys recommends that you use alphabetic characters when defining interface names, since purely numeric interfaces will be interpreted as IP addresses. The X-Pedition router will display interface names up to 32 characters in length.

## Restrictions

You must be in ARE-Configure mode before using this command.

## Example

To add a route on interface “if1”:

```
xp(are-config)# appletalk add route interface if1 cable-range 3-4 gateway 5.6 distance 2
```

This command determines that an AppleTalk packet destined for network “3-4” will exit through this interface. The AppleTalk address for the next router to be encountered is “5.6,” and there are “2” hops (routers) between this router and the destination.

# appletalk aarp interval

## Purpose

Sets the interval between AppleTalk AARP requests.

## Format

**appletalk aarp interval** *<seconds>*

## Mode

ARE-Configure.

## Description

The **appletalk aarp interval** command creates an interval between AARP requests while the system is attempting to determine a hardware address.

## Parameters

|                        |  |
|------------------------|--|
| <i>&lt;seconds&gt;</i> | Specifies number of seconds at which you want to set the interval. |
|------------------------|--|

## Restrictions

You must be in ARE-Configure mode before using this command.

# appletalk aarp timeout

## Purpose

Determines the age-out time of the AppleTalk AARP table.

## Format

**appletalk aarp timeout** *<seconds>*

## Mode

ARE-Configure.

## Parameters

---

|                        |  |
|------------------------|--|
| <i>&lt;seconds&gt;</i> | Specifies number of seconds at which you want to set the age-out time. |
|------------------------|--|

---

## Restrictions

You must be in ARE-Configure mode before using this command.

# **appletalk checksum disable**

## **Purpose**

Disables checksum calculation for out-going packets.

## **Format**

**appletalk checksum disable**

## **Mode**

ARE-Configure.

## **Parameters**

None.

## **Restrictions**

You must be in ARE-Configure mode before using this command.

# appletalk rtmp jitter

## Purpose

Staggers Routing Table Maintenance Protocol (RTMP) routing updates.

## Format

**appletalk rtmp jitter** *<percent>*

## Mode

ARE-Configure.

## Description

The **appletalk rtmp jitter** command staggers routing updates by altering the RTMP update interval in order to avoid syncing with other routers on the same link.

## Parameters

|                        |   |
|------------------------|---|
| <i>&lt;percent&gt;</i> | Specifies the percentage to alter the RTMP update interval. For example, if the current RTMP update interval is 10, and you set the “jitter” to 10%, the update interval will be altered to occur between 9 and 11 seconds. |
|------------------------|---|

## Restrictions

You must be in ARE-Configure mode before using this command.

## Example

To alter the RTMP update interval by 15%:

```
xp(are-config)# appletalk rtmp jitter 15
```

# appletalk rtmp update-disable

## Purpose

Disables RTMP updates.

## Format

**appletalk rtmp update-disable interface** <InterfaceName>|**all**

## Mode

ARE-Configure.

## Description

The **appletalk rtmp update-disable** command prevents RTMP updates from being sent out on the indicated interface(s).

## Parameters

|                 |   |
|-----------------|---|
| <InterfaceName> | Specifies the interface for which you want to disable RTMP updates. |
| <b>all</b>      | Disables updates on all available interfaces.                       |

**Note:** Enterasys recommends that you use alphabetic characters when defining interface names, since purely numeric interfaces will be interpreted as IP addresses. The X-Pedition router will display interface names up to 32 characters in length.

## Restrictions

You must be in ARE-Configure mode before using this command.

## Example

To disable RTMP updates on interface “app5”:

```
xp(are-config)# appletalk rtmp update-disable interface app5
```



# appletalk rtmp update-interval

## Purpose

Determines the number of seconds between RTMP updates.

## Format

**appletalk rtmp update-interval** *<seconds>*

## Mode

ARE-Configure.

## Description

The **appletalk rtmp update-interval** command sets the number of seconds between RTMP updates on an interface.

## Parameters

---

|                        |  |
|------------------------|--|
| <i>&lt;seconds&gt;</i> | Specifies number of seconds at which to set RTMP update interval. The default is 10. |
|------------------------|--|

---

## Restrictions

You must be in ARE-Configure mode before using this command.

# appletalk rtmp valid-interval

## Purpose

Determines number of seconds a route is considered valid.

## Format

**appletalk rtmp valid-interval** *<seconds>*

## Mode

ARE-Configure.

## Description

The **appletalk rtmp valid-interval** command sets the number of seconds for which a route is considered valid. A route is considered invalid after the valid-interval expires twice. A route is deleted after the valid-interval expires three times. The valid timer is reset every time an RTMP packet is received which validates the route.

## Parameters

---

|                        |  |
|------------------------|--|
| <i>&lt;seconds&gt;</i> | Specifies number of seconds for which you want to set the valid-interval timer. The default is 20. |
|------------------------|--|

---

## Restrictions

You must be in ARE-Configure mode before using this command.

# **appletalk split-horizon disable**

## **Purpose**

Disables RTMP from using split-horizon methodology.

## **Format**

**appletalk split-horizon disable**

## **Mode**

ARE-Configure.

## **Description**

The **appletalk split-horizon disable** command prevents the Route Maintenance Protocol (RTMP) from using the split-horizon methodology. This methodology is enabled by default.

## **Parameters**

None.

## **Restrictions**

You must be in ARE-Configure mode before using this command.

# appletalk zip query-interval

## Purpose

Determines interval between Zone Information Protocol (ZIP) queries.

## Format

**appletalk zip query-interval** *<seconds>*

## Mode

ARE-Configure.

## Description

The **appletalk zip query-interval** command sets the interval between zip queries. These queries occur when the router discovers a routing table entry without an associated zone. It sends a zip query to collect appropriate zones for the entry.

## Parameters

---

|                        |  |
|------------------------|--|
| <i>&lt;seconds&gt;</i> | Specifies number of seconds for which you want to set the query interval timer. The default is 10. |
|------------------------|--|

---

## Restrictions

You must be in ARE-Configure mode before using this command.

# Chapter 6

## are Commands

The **are** commands allow you to manipulate the Advanced Routing Engine (ARE) module, the full-featured AppleTalk Phase II router available for the X-Pedition router. These commands apply to the ARE module globally, and will function regardless of protocol designation.

### Command Summary

[Table 6](#) lists the **are** commands. The sections following the table describe the command syntax.

**Table 6. are Commands**

|   |
|---|
| <b>are enable protocol appletalk module</b> <i>&lt;module-number&gt;</i>  |
| <b>are-config</b> <i>&lt;module-number&gt;</i>  |
| <b>system are-promimage upgrade</b> <i>&lt;module-number&gt;</i> <i>&lt;tftp-server&gt;</i> <i>&lt;filename&gt;</i> |

# are enable protocol appletalk

## Purpose

Enables AppleTalk protocol on an ARE module.

## Format

**are enable protocol appletalk module** *<module-number>*

## Mode

Configure.

## Description

The **are enable protocol appletalk** command allows the user to enable AppleTalk protocol on a specified ARE module. This command is required before the user attempts to configure any protocol-specific commands on a module.

## Parameters

---

|   |  |
|---|--|
| <b>module</b><br><i>&lt;module-number&gt;</i> | Specifies ARE module for which to enable the protocol. |
|---|--|

---

## Restrictions

None.

## Example

The following examples demonstrate how to enable AppleTalk protocol on module 5:

```
xp(config)# show
Running system configuration:
!
! Last modified from Console on 2001-12-06 12:21:43
!
1 : vlan create blue appletalk id 100
2 : vlan create green appletalk id 200
3 : vlan create red appletalk id 300
4 : vlan add ports et.1.1 to blue
5 : vlan add ports et.1.2 to green
6 : vlan add ports et.1.3 to red
!
7 : are enable protocol appletalk module 5
!
8 : interface create appletalk Apple20000 vlan blue noseed
9 : interface create appletalk Apple21000 vlan green cable-range 21000-21010 zone Teachers
   address 21001.1
10 : interface create appletalk Apple22000 vlan red cable-range 22000-22010 zone Admins
    address 22001.1
11 : interface add appletalk Apple21000 zone Biology
12 : interface add appletalk Apple21000 zone Journalism
```

```
xp(config)# show

1 : vlan create blue appletalk id 100
2 : vlan create black appletalk id 400
3 : vlan create yellow appletalk id 500
4 : vlan add ports et.1.1 to blue
5 : vlan add ports et.1.2 to black
6 : vlan add ports et.1.3 to yellow
!
7 : are enable protocol appletalk module 5
!
8 : interface create appletalk Apple20000 vlan blue cable-range 20000-20010 zone Students
   address 20000.1
9 : interface create appletalk Apple30000 vlan black cable-range 30000-30010 zone Geology
   address 30000.1
10 : interface create appletalk Apple40000 vlan yellow cable-range 40000-40010 zone English
    address 40000.1
11 : interface add appletalk Apple30000 zone Chemistry
12 : interface add appletalk Apple30000 zone Physics
```

# are-config

## Purpose

Places CLI session in ARE-Configure mode.

## Format

**are config** <module-number>

## Mode

Configure.

## Description

The **are configure** command places the CLI session in ARE-Configure mode. All configuration settings for a specific ARE module or modules must be made from this mode.

**Note:** When you negate an interface configured with an ARP command, the X-Pedition router automatically reassigns the command to a non-existing interface in the same configuration.

## Parameters

---

|                 |  |
|-----------------|--|
| <module-number> | Specifies ARE module for which to enter ARE-Configure mode. If no module is specified, interface will return a list of all active modules available for configuration. |
|-----------------|--|

---

## Restrictions

User must be in Configure mode.

## Example

To enter ARE-Configure mode on module 5:

```
xp(config)# are config 5
```



# system are-promimage upgrade

## Purpose

Upgrades boot PROM image on a specified ARE module.

## Format

**system are-promimage upgrade** *<module-number>* *<tftp-server>* *<filename>*

## Mode

Enable.

## Description

The **system are-promimage upgrade** command allows you to upgrade a specific ARE module's boot PROM image with the image located on the TFTP server.

**Note:** To take advantage of this upgrade, you must reboot the ARE module.

## Parameters

|                              |  |
|------------------------------|--|
| <i>&lt;module-number&gt;</i> | Specifies ARE module for which to upgrade Boot PROM image. |
| <i>&lt;tftp-server&gt;</i>   | Specifies the TFTP server on which the image is located.   |
| <i>&lt;filename&gt;</i>      | Specifies image file name.                                 |

## Restrictions

None.

## Example

To upgrade the PROM for ARE module 5 with the file "prom\_image\_file":

```
xp(config)# system are-promimage upgrade 5 tftp://host1/public/prom_image_file
```



# Chapter 7

## arp Commands

The **arp** commands enable you to add, display, and clear ARP entries on the X-Pedition router.

### Command Summary

[Table 7](#) lists the arp commands. The sections following the table describe the command syntax.

**Table 7. arp Commands**

|   |
|---|
| <b>arp add</b> <host> <b>mac-addr</b> <MAC-addr> [vlan   <b>exit-port</b> <port>] <b>keep-time</b> <seconds>                            |
| <b>arp clear</b> <host> all [ <b>interface</b> <string>  <b>unresolved</b>  all] [ <b>port</b> <port>]                                  |
| <b>arp set drop-unresolved</b> disabled  enabled  |
| <b>arp set interface</b> <name> all <b>keep-time</b> <number>   |
| <b>arp set max-unresolved</b> <num>   |
| <b>arp set unresolve-threshold</b> <num>  |
| <b>apr set unresolve-timer</b> <num>  |
| <b>arp show</b> <IPaddr> all [ <b>undecoded</b> ] [ <b>unresolved</b> ] [ <b>interface</b> <string>  <b>all</b> ] [ <b>port</b> <port>] |

# arp add

## Purpose

Add an ARP entry.

## Format

**arp add** <host> **mac-addr** <MAC-addr> [**vlan** | **exit-port** <port>] **keep-time** <seconds>

## Mode

Enable and Configure.

## Description

The **arp add** command lets you manually add ARP entries to the ARP table. Typically, the X-Pedition router creates ARP entries dynamically. Using the **arp add** command, you can create an ARP entry to last a specific amount of time or as a permanent ARP entry. This command exists in both Enable and Configure mode with a slight variation. The **keep-time** option is valid only in Enable mode and allows you to create an ARP entry that will last for a specific amount of time. The Configure mode version of the **arp add** command does not use the **keep-time** option and the ARP entries created will be permanent and will not have an expiration time.

If you specify an **exit port**, packets destined for the IP address will always transmit out the given exit port. If you specify the **vlan** option, the ARP entry will be associated to a VLAN rather than a specific exit port and traffic destined for the given IP address will always flood out of the entire VLAN/interface that provides a route to it. If you specify neither option, packets will transmit on all ports of the interface until the host receives an ARP request. The X-Pedition router will then update the exit port with the port on which the ARP request was received, so that subsequent packets will transmit on only one port.

## Parameters

|                               |   |
|-------------------------------|---|
| <host>                        | Hostname or IP address of this ARP entry.   |
| <b>mac-addr</b><br><MAC-addr> | MAC address of the host.  |
| vlan                          | Traffic to this host should be flooded out the VLAN/interface it belongs to.                  |
| <b>exit-port</b> <port>       | The port for which you are adding the entry. Specify the port to which the host is connected. |

---

**keep-time** <seconds> The number of seconds this ARP entry should remain in the ARP table. A value of 0 means this is a permanent ARP entry.

**Note:** This option is valid only for the Enable mode **arp add** command.

---

## Restrictions

- If you enter the **arp add** command while in the Configure mode, you can add only permanent ARP entries.
- The X-Pedition router clears all expired and unresolved ARP entries once every 5 minutes. Therefore, expired ARPs may be kept up to 5 minutes longer than the keep-time.

## Examples

To create an ARP entry for the IP address 10.8.1.2 at port et.4.7 for 15 seconds:

```
xp# arp add 10.8.1.2 mac-addr 08:00:20:a2:f3:49 exit-port et.4.7 keep-time 15
```

To create a permanent ARP entry for the host *nfs2* at port et.3.1:

```
xp(config)# arp add nfs2 mac-addr 080020:13a09f exit-port et.3.1
```

To create a permanent ARP entry for IP address 10.8.1.25 that will always flood the traffic out the subnet:

```
xp(config)# arp add 10.8.1.25 mac-addr 080020:a2f360 vlan
```

# arp clear

## Purpose

Remove an ARP entry from the ARP table.

## Format

**arp clear** <host>|**all** [**interface** <string>| **all**] [**port** <port>] **unresolved**

## Mode

Enable.

## Description

The **arp clear** command lets you manually remove entries from the ARP table. The command can remove both dynamic and permanent entries.

## Parameters

|                    |   |
|--------------------|---|
| <host>             | Hostname or IP address of the ARP entry to remove.  |
| <b>all</b>         | Remove all ARP entries, thus clearing the entire ARP table.   |
| <b>interface</b>   | Specify this optional parameter to clear only entries in the ARP table that corresponds to a specific interface.<br><br><string>      Specifies the interface name.<br><br><b>all</b> Specifies all interfaces.<br><br><b>Note:</b> Enterasys recommends that you use alphabetic characters when defining interface names, since purely numeric interfaces will be interpreted as IP addresses. The X-Pedition router will display interface names up to 32 characters in length. |
| <b>port</b> <port> | Specify this optional parameter to clear only entries in the ARP table that corresponds to a specific exit port.  |
| <b>unresolved</b>  | Specify this optional parameter to clear only currently unresolved entries.   |

## Examples

To remove the ARP entry for the host 10.8.1.2 from the ARP table:.

xp# **arp clear 10.8.1.2**

To clear the entire ARP table.

```
xp# arp clear all
```

If the Startup configuration file contains **arp add** commands, the Control Module re-adds the ARP entries even if you have cleared them using the **arp clear** command. To permanently remove an ARP entry, use the **negate** command or **no** command to remove the entry. The following **no** command removes the ARP entry for nfs2:

```
xp# no arp add nfs2 macaddr 080020:13a09f exit-port et.3.1
```

# arp set drop-unresolved

## Purpose

Specify how to handle traffic that cannot be resolved by the Address Resolution Protocol (ARP).

## Format

**arp set drop-unresolved disabled| enabled**

## Mode

Configure.

## Description

When the X-Pedition router receives an IP packet with an unknown nexthop MAC address, the router attempts to resolve it by broadcasting an ARP request on the destination subnet. If the host replies to the ARP, the router forwards the packet to the host. However, if the router does not receive a reply, it will send one ARP request for each of the next four data packets it receives. If the ARP is not resolved when the sixth packet arrives, the router will (by default) drop the sixth and all subsequent packets *in software* for 20 seconds and transmit ICMP destination unreachable messages back to the sender(s) for each new packet received. The router will then remove the unresolved ARP entry and the resolution process will resume.

When the **arp set drop-unresolved** command is enabled, any unresolved ARP that has not started sending ICMP destination unreachable messages will have its sixth and all subsequent packets dropped *in hardware* through the addition of a Layer-3 drop flow—*no ICMP message will be sent*.

Furthermore, the router will cycle periodically through the list of all unresolved ARPs and re-send ARP requests in an attempt to resolve their nexthop MAC addresses. To configure the frequency of the resolution attempts and the maximum number of ARP requests sent with each attempt, use the **arp set unresolve-timer** and **arp set unresolve-threshold** commands. The behavior you configure will last until the Layer-3 drop ages out or until the router clears all expired and unresolved ARP entries (every 5 minutes). The router will then re-start the resolution process.

## Parameters

|                 |  |
|-----------------|--|
| <b>disabled</b> | Specifies that all unresolved ARP traffic will be handled by <i>software</i> , and that ICMP destination unreachable <i>messages will be sent</i> if the IP address cannot be resolved. This is the default behavior.  |
| <b>enabled</b>  | Specifies that all unresolved ARP traffic will be dropped by the <i>hardware</i> with ICMP destination unreachable <i>messages suppressed</i> . The X-Pedition router will then attempt to resolve the ARP periodically, according to the unresolve-threshold and the unresolve-timer. |



## Restrictions

None.

## Example

To drop IP packets with unresolved nexthop MAC addresses in *hardware* and *suppress* ICMP destination unreachable messages after ARP fails to resolve the IP address:

```
xp# arp set drop-unresolved enabled
```

# arp set interface

## Purpose

Set the lifetime (in seconds) of un-accessed ARP entries.

## Format

**arp set interface** <name>|**all** **keep-time** <number>

## Mode

Configure.

## Description

The **arp set interface** command lets users specify the amount of time (in seconds) to keep un-accessed ARP entries. ARP entries not accessed during the defined keep-time value are deleted the next time the system checks for un-accessed entries (by default, once every 5 minutes). As a result, an ARP entry may not be deleted immediately after the keep-time passes.

## Parameters

|                                     |   |
|-------------------------------------|---|
| <b>interface</b> <name>  <b>all</b> | Name of the interface(s) for which you will define the lifespan. Use <b>all</b> to specify all interfaces.  |
| <b>Note:</b>                        | Enterasys recommends that you use alphabetic characters when defining interface names, since purely numeric interfaces will be interpreted as IP addresses. The X-Pedition router will display interface names up to 32 characters in length. |
| <b>keep-time</b> <number>           | Number of seconds determining lifespan of ARP interfaces. The default value is 1200 seconds (20 minutes).   |

## Restrictions

The X-Pedition router clears all expired and unresolved ARP entries once every 5 minutes. Therefore, expired ARPs may be kept up to 5 minutes longer than the keep-time.

# arp set max-unresolved

## Purpose

Allow users to limit the number of unresolved ARP entries created by the X-Pedition router.

## Format

**arp set max-unresolved** <num>

## Mode

Configure.

## Description

The **arp set max-unresolved** command lets you specify the maximum number of unresolved ARP entries the X-Pedition router may create. When the number of unresolved ARP entries exceeds this limit, the older ARP entries are removed to make room for the new ones.

The router may stop sending ICMP host unreachable messages and transmit more ARP requests if the number of unresolved ARPs exceeds the specified limit and entries are constantly removed and relearned. However, if the maximum is set too high, the router may exhaust available system memory and suffer degraded performance. Under normal network conditions, the number of unresolved ARPs is only a small fraction of the total number of ARP entries created, but network events such as a route change or an STP topology change can temporarily increase the number of unresolved ARP entries. Since the frequency of these events varies from network to network, there is no global solution. Users are encouraged to experiment on their own. If you are unsure of where to set the max-threshold, Enterasys recommends leaving the number at 1000 (the default).

## Parameters

|       |  |
|-------|--|
| <num> | Maximum number of unresolved ARP entries an X-Pedition router can keep. Requires a number greater than or equal to 500. Default is 1000. |
|-------|--|

## Restrictions

None.

## Example

To limit the number of unresolved ARP entries to under 500:

```
xp# arp set max-unresolved 500
```

# arp set unresolve-threshold

## Purpose

This command allows users to limit the number of unresolved ARPs the X-Pedition router will periodically attempt to resolve if **arp set drop-unresolved** is enabled.

## Format

**arp set unresolve-threshold** <num>

## Mode

Configure.

## Description

The **arp set unresolve-threshold** command lets you specify the maximum number of ARP requests sent in each periodic resolution attempt. When **arp set drop-unresolved** is enabled, the X-Pedition router will periodically cycle through the list of all unresolved ARPs and send ARP requests in an attempt to resolve their nexthop MAC addresses. This command controls the number of ARP entries the router attempts to resolve. Also see [arp set drop-unresolved on page 114](#).

## Parameters

|       |   |
|-------|---|
| <num> | The maximum number of ARP requests sent in each periodic resolution attempt. Requires a number greater than or equal to 1. The default is 50. |
|-------|---|

## Restrictions

This command has no effect unless **arp set drop-unresolved enabled** command is configured.

## Example

To increase the maximum number of ARP requests sent during each attempt to 100:

```
xp# arp set unresolve-threshold 100
```

# arp set unresolve-timer

## Purpose

Allows users to specify the frequency of the periodic resolution attempts when the **arp set drop-unresolved** command is enabled.

## Format

**arp set unresolve-timer** <num>

## Mode

Configure.

## Description

The **arp set unresolve-timer** command lets you specify the frequency of the periodic resolution attempts. When the **arp set drop-unresolved** command is enabled, the X-Pedition router will periodically cycle through the list of all unresolved ARPs and re-send ARP requests in an attempt to resolve their nexthop MAC addresses. This command controls how often to make these resolution attempts. Refer to [arp set drop-unresolved on page 114](#) for details.

## Parameters

|       |   |
|-------|---|
| <num> | The interval (in seconds) between each periodic resolution attempt. Requires a number greater than or equal to 10. The default is 10. |
|-------|---|

## Restrictions

This command has no effect unless the **arp set drop-unresolved enabled** command is configured.

## Example

To increase the interval between each subsequent resolution attempt to 30 seconds:

```
xp# arp set unresolve-timer 30
```

# arp show

## Purpose

Display the ARP table.

## Format

**arp show** <IPaddr>|**all** [**undecoded**] [**unresolved**] [**interface** <string>| **all**] [**port** <port>]

## Mode

Enable.

## Description

The **arp show** command displays the entire ARP table.

## Parameters

|                    |   |
|--------------------|---|
| <IPaddr>           | Shows the ARP entry for the specified IP address.   |
| <b>all</b>         | Shows all entries in the ARP table.   |
| <b>undecoded</b>   | Specify this optional parameter to show MAC addresses in hexadecimal format.  |
| <b>unresolved</b>  | Specify this optional parameter to show only MAC addresses in the ARP table that have yet to be mapped to an network layer address.   |
| <b>interface</b>   | Specify this optional parameter to show only addresses in the ARP table that is associated with the specific interface.<br><br><string> Specifies the interface name.<br><br><b>all</b> Specifies all interfaces.<br><br><b>Note:</b> Enterasys recommends that you use alphabetic characters when defining interface names, since purely numeric interfaces will be interpreted as IP addresses. The X-Pedition router will display interface names up to 32 characters in length. |
| <b>port</b> <port> | Specify this optional parameter to show only addresses in the ARP table that corresponds to a specific exit port.   |





# Chapter 8

## atm Commands

### Command Summary

[Table 8](#) lists the **atm** commands. The sections following [Table 8](#) describe the command syntax for each command.

**Note:** Interfaces configured with PVCs do not support LSNAT or VRRP.

**Table 8. atm commands**

|  |
|--|
| <b>atm apply service</b> <string> <b>port</b> <port list>  |
| <b>atm create vcl port</b> <port list> [ <b>vbr</b> ]  |
| <b>atm define service</b> <string> [ <b>srv-cat</b> <b>ubr</b>   <b>cbr</b>   <b>rt-vbr</b>   <b>nrt-vbr</b> ] [ <b>pcr</b> ]   [ <b>pcr-kbits</b> ] [ <b>scr</b> ]   [ <b>scr-kbits</b> ] [ <b>mbs</b> ] [ <b>encaps</b> <b>llc-mux</b>   <b>vc-mux</b> ] [ <b>oam</b> <b>on</b>   <b>off</b> ] [ <b>oam-f5-type</b> <b>current-segment</b>   <b>end-to-end</b> ] |
| <b>atm set peer-addr port</b> <port> <b>ip-address</b> <ipaddr>  <b>ipx-address</b> <netaddr>.<macaddr>  |
| <b>atm set port</b> <port list> <b>cell-mapping</b> <b>direct</b>   <b>plcp</b>  |
| <b>atm set port</b> <port list> <b>pdh-cell-scramble</b> <b>on</b>   <b>off</b>  |
| <b>atm set port</b> <port list> <b>vpi-bits</b> <num>  |
| <b>atm set vcl port</b> <port> <b>forced-bridged</b>   |
| <b>atm show</b> [ <b>vpl port</b> <port list>  <b>all</b> [ <b>summary</b> ]]   [ <b>vcl port</b> <port list>  <b>all</b> [ <b>summary</b> ]] [ <b>service</b> <string>  <b>all</b> ]   [ <b>port-settings</b> <port list>/ <b>all-ports</b> ]   [ <b>stats port</b> <port list>]  |

# atm apply service

## Purpose

Apply a service profile.

## Format

**atm apply service** <string> **port** <port list>

## Mode

Configure.

## Description

The **atm apply service** command applies a service profile to a virtual channel (VC), virtual path (VP), and/or atm port. Service profiles define certain preset values for traffic and QoS parameters. Each service profile has its own unique set of traffic and QoS guarantees in handling transmission of ATM cells.

The concept of inheritance is important when applying service profile definitions. Since a service profile definition can be applied to a VC, VP, or on a port, the actual connection can inherit the service profile definition from any one of the three. The VC will inherit the service profile definition that is directly applied on it. If no service profile was applied to the VC, the connection will inherit the service profile applied to the VP. If no service profile definition was applied to the VP, then the connection will inherit the service profile applied to the ATM port. If no service profile was applied to the port, then the default service profile UBR is applied.

The following service classes are supported: CBR (constant bit rate), rt-VBR (real-time variable bit rate), nrt-VBR (non real-time variable bit rate), and UBR (unspecified bit rate). ABR (available bit rate) is not currently supported.

## Parameters

---

|          |  |
|----------|--|
| <string> | Is the character string of a previously-defined service. You define a service using the <b>atm define service</b> command (see <a href="#">page 128</a> ). |
|----------|--|

---

|                          |   |
|--------------------------|---|
| <b>&lt;port list&gt;</b> | Is the port name, in the format: <b>media.slot.port.vpi.vci</b> |
| <b>media</b>             | Is the media type. This is <b>at</b> for an ATM port.           |
| <b>slot</b>              | Is the slot number where the module is installed.               |
| <b>port</b>              | Is the number of the port through which data is passing.        |
| <b>vpi</b>               | Is the Virtual Path Identifier. This parameter is optional.     |
| <b>vci</b>               | Is the Virtual Channel Identifier. This parameter is optional.  |

## Examples

To apply the pre-defined service profile 'CBR1' to virtual channel at.5.1.1.100:

```
xp(config)# atm apply service CBR1 port at.5.1.1.100
```

To apply the pre-defined service profile 'CBR1' to virtual path at.5.1.1:

```
xp(config)# atm apply service CBR1 port at.5.1.1
```

To apply the pre-defined service profile 'CBR1' to port at.5.1:

```
xp(config)# atm apply service CBR1 port at.5.1
```

# atm create vcl port

## Purpose

Create a virtual channel.

## Format

**atm create vcl port** <port list> [**vbr**]

## Mode

Configure.

## Description

The **atm create vcl** command creates a virtual channel on an ATM port. Virtual channels are point to point cell-switched connections used for ATM cell traffic. Virtual channels are defined by specifying a VCI (Virtual Channel Identifier) and VPI (Virtual Path Identifier) pair.

The range of available VCI and VPI are set by the **atm set port vpi-bits** command.

**Note:** Be careful when specifying VCI numbers 0 through 31. Those VPI/VCI pairs are used by some protocols for signaling purposes.

## Parameters

|              |   |
|--------------|---|
| <port list>  | Is the port name, in the format: <b>media.slot.port.vpi.vci</b>   |
| <b>media</b> | Is the media type. This is <b>at</b> for an ATM port.   |
| <b>slot</b>  | Is the slot number where the module is installed.   |
| <b>port</b>  | Is the number of the port through which data is passing.  |
| <b>vpi</b>   | Is the Virtual Path Identifier.   |
| <b>vci</b>   | Specifies the Virtual Channel Identifier. This number identifies a particular VC. The combination of VPI and VCI is known as the VPI/VCI pair, and identifies the VC. |
| <b>Note:</b> | Do not specify VCI numbers 0 through 31. Some protocols use these VPI/VCI pairs for signaling purposes.   |

|            |   |
|------------|---|
| <b>vbr</b> | <p>Opens the VC with a default VBR service. All VCs to which you will apply a VBR service must be created with this option for traffic shaping to behave properly. If you specify the <b>vbr</b> option, you may apply only VBR services to the VC. If you do not specify the <b>vbr</b> option, you may apply only UBR and CBR services to the VC.</p> <p><b>Note:</b> Traffic on ATM Virtual Circuits configured with a Variable Bit Rate (nrt-vbr or rt-vbr) traffic descriptor will not obey the configured traffic descriptor's parameters. ATM policing mechanisms will drop nonconforming ATM cells.</p> |
|------------|---|

## Restrictions

None.

## Examples

To create a virtual channel on slot 5, port 1, VPI 1, and VCI 100:

```
xp(config)# atm create vcl port at.5.1.1.100
```

To create many virtual channels simultaneously:

```
xp(config)# atm create vcl port at.5.1.(1,3-5,7).(100,555-600,700)
```

The following commands create an ATM virtual channel on an ATM port and associate the port with an IPX interface. This allows IPX routing between two IPX interfaces. As with any IPX interface, IPX routing using RIP (the default) will begin when you configure an IPX interface.

```
xp(config)# atm create vcl port at.3.1.1.100
xp(config)# interface create ipx finance address 01234567 peer-address 01234567.00:00:1d:a9:8c:a1
port at.3.1.1.100
xp(config)# interface create ipx marketing address 01234569 port et.1.1
```

## atm define service

### Purpose

Define a service profile.

### Format

```
atm define service <string> [srv-cat ubr| cbr| rt-vbr| nrt-vbr] [pcr] | [pcr-kbits] [scr] |  
[scr-kbits] [mbs] [encaps llc-mux| vc-mux] [oam on| off] [oam-f5-type current-segment |  
end-to-end]
```

### Mode

Configure.

### Description

The **atm define** command defines a set of traffic parameters, which you can apply to a virtual channel (VC). Quality of Service (QoS) parameters define the delays, dependability, and peak limits for a VC. Class of Service defines the bandwidth guarantees. When a VC is established, a service profile definition created by this command can then be applied to the connection.

### Parameters

---

|          |  |
|----------|--|
| <string> | Is a character string. The maximum length is 32 bytes. |
|----------|--|

---

|                  |  |
|------------------|--|
| <b>srv-cat</b>   | Is the service category (UBR is the default):  |
| <b>cbr</b>       | Constant Bit Rate. This service category provides a guaranteed constant bandwidth specified by the Peak Cell Rate (PCR). This service requires only the PCR value. The Sustainable Cell Rate (SCR) and Maximum Burst Size (MBS) values are ignored. This service category is intended for applications that require constant cell rate guarantees such as uncompressed voice or video transmission.  |
| <b>ubr</b>       | Unspecified Bit Rate. This service category is strictly best effort and runs at the available bandwidth. Users may limit the bandwidth by specifying a PCR value. The SCR and MBS are ignored. This service class is intended for applications that do not require specific traffic guarantees. UBR is the default.  |
| <b>nrt-vbr</b>   | Non Real-Time Variable Bit Rate. This service category provides a guaranteed constant bandwidth (specified by the SCR), but also provides for peak bandwidth requirements (specified by the PCR). This service category requires the PCR, SCR, and MBS options and is intended for applications that can accommodate bursty traffic with no need for real-time guarantees.   |
| <b>rt-vbr</b>    | Real-Time Variable Bit Rate. This service category provides a guaranteed constant bandwidth (specified by the SCR), but also provides for peak bandwidth requirements (specified by the PCR). This service category requires the PCR, SCR, and MBS options and is intended for applications that can accommodate bursty real-time traffic such as compressed voice or video.   |
| <b>pcr</b>       | Peak Cell Rate. This rate specifies the maximum cell transmission rate, expressed in cells/sec. The default is 353207 cells/sec for ATM OC-3. This parameter is valid for CBR, rtVBR, nrtVBR, and UBR service categories. This parameter is optional for UBR.  |
| <b>pcr-kbits</b> | Is the Peak Cell Rate, and specifies the maximum cell transmission rate, expressed in kbits/sec. The default is 149759 kbits/sec (353207 cells/sec) for ATM OC-3. This is the same as PCR, but is expressed in kbits/sec, and therefore may be a more convenient form. However, since the natural unit for ATM is cells/sec, there may be a difference in the actual rate because the kbit/sec value may not be an integral number of cells. This parameter is valid for CBR, rtVBR, nrtVBR, and UBR service categories. |
| <b>scr</b>       | Sustainable Cell Rate. This rate specifies the average cell rate, expressed in cells/sec. The default is 0 cells/sec. This parameter is valid only for rtVBR and nrtVBR service categories.  |
| <b>scr-kbits</b> | Sustainable Cell Rate expressed in kbits/sec. The default is 0 kbits/sec. This is the same as SCR, but is expressed in kbits/sec, and therefore may be a more convenient form. However, since the natural unit for ATM is cells/sec, there may be a difference in the actual rate because the kbit/sec value may not be an integral number of cells. This parameter is valid only for rtVBR and nrtVBR service categories.   |

|                    |  |
|--------------------|--|
| <b>mbs</b>         | Is the Maximum Burst Size in cells. MBS specifies how many cells (2 to 255) can be transmitted at the Peak Cell Rate. The default is 0 cells. This parameter is valid only for rtVBR and nrtVBR service categories.  |
| <b>encaps</b>      | Is the encapsulation scheme to transport multi protocol data over the AAL5 layer. Either llc-mux (logical link control based on multiplexing) or vc-mux (virtual channel-based multiplexing). The default is llc-mux.  |
| <b>oam</b>         | OAM (Operation, Administration, and Management) loopback cells are used to provide loopback capabilities and confirm whether a VC connection is up. Only F5 OAM segments and end-to-end are supported, which provides loopback capabilities on a VC connection level. This parameter turns OAM ON or OFF on the PVC. The default is off. OAM OFF means that the X-Pedition router responds to F5 OAM requests, but will not generate F5 OAM responses. |
| <b>oam-f5-type</b> | Used to specify the path of the OAM cells. Select either current-segment or end-to-end. The default is current-segment.  |

## Restrictions

**scr** can not exceed **pcr**. No parameters may exceed the link rate for the type of **phy**.

## Example

To define a 10Mbps service:

```
xp(config)# atm define service CBR-example srv-cat cbr pcr_kbits 10000
```



# atm set peer-addr

## Purpose

Maps peer address to virtual channels.

## Format

**atm set peer-addr port** <port> **ip-address** <ipaddr>| **ipx-address** <netaddr>.<macaddr>

## Mode

Configure.

## Description

The **atm set peer-addr** command allows you to map a peer address for an ATM port to a specific virtual channel. This allows you to associate a specific virtual channel and its interface to a specific peer address.

## Parameters

|  |  |
|--|--|
| <b>port</b> <port>                     | Specifies a single port, including virtual channel, in the format: <b>media.slot.port.vpi.vci</b> .<br><br><b>media</b> Is the media type. This is always <b>at</b> for an ATM port.<br><b>slot</b> Is the slot number where the module is installed.<br><b>port</b> Is the number of the port through which data is passing.<br><b>vpi</b> Is the Virtual Path Identifier.<br><b>vci</b> Is the Virtual Channel Identifier. |
| <b>ip-address</b> <ipaddr>             | Specifies an IP address for the peer. Specify a unicast IP address and netmask value in the following format: <b>a.b.c.d/e</b> . This IP address will be mapped to the VC.   |
| <b>ipx-address</b> <netaddr>.<macaddr> | Specifies an IPX address for the peer. Specify an IPX network and node address in the following format: <b>a1b2c3d4.aa:bb:cc:dd:ee:ff</b> . If a <macaddr> is not specified, then a wildcard address is used. This IPX address will be mapped to the VC.   |

## Restrictions

None.

## Example

To map the peer address 10.0.0.100/24 to the virtual channel at.4.1.0.100:

```
xp (config)# atm set peer-addr ports at.4.1.0.100 ip-address 10.0.0.100/24
```

# atm set port cell-mapping

## Purpose

Sets the format used to map ATM cells.

## Format

**atm set port** <port list> **cell-mapping** direct| plcp

## Mode

Configure.

## Description

The **atm set port cell-mapping** command specifies the format for mapping ATM cells into PDH (plesiochronous digital hierarchy) T3 and E3 frames. The ATM cells that each frame carries does not fit exactly into the PDH frame, therefore mapping of the data is necessary to ensure efficient transmission.

## Parameters

|               |  |
|---------------|--|
| <port list>   | Specifies the ATM port(s). Specify <b>all-ports</b> to select all ports. |
| <b>direct</b> | Specifies ATM direct mapping. Default.                                   |
| <b>plcp</b>   | Specifies physical layer convergence protocol mapping.                   |

## Restrictions

Cell mapping is valid only for T3 and E3 PHY interfaces.

## Example

To set cell-mapping to plcp for ATM port at.9.1:

```
xp(config)# atm set port at.9.1 cell-mapping plcp
```

# atm set port pdh-cell-scramble

## Purpose

Enables cell scrambling for ATM ports.

## Format

**atm set port** *<port list>* **pdh-cell-scramble on| off**

## Mode

Configure.

## Description

The **atm set port pdh-cell-scramble** command allows you to enable payload scrambling for PDH (plesiochronous digital hierarchy) PHY interfaces for the ATM line card, such as T1, T3, E1, and E3. Scrambling a payload is important in optimizing the transmission density of the data stream. Since all transmission use the same source clock for timing, scrambling the payload using a random number generator converts the data stream to a more random sequence. This ensures optimal transmission density of the data stream.

## Parameters

|                                      |  |
|--------------------------------------|--|
| <b>port</b> <i>&lt;port list&gt;</i> | Specifies the port, in the format: <b>media.slot.port</b> . Specify <b>all-ports</b> to enable cell scrambling on all ports. |
| <b>media</b>                         | Specifies the media type. This is at for ATM ports.  |
| <b>slot</b>                          | Specifies the slot number where the module is installed.   |
| <b>port</b>                          | Specifies the port number.   |
| <b>on</b>                            | Enables cell scrambling.   |
| <b>off</b>                           | Disables cell scrambling.  |

## Restrictions

This command is valid only for PDH PHY interfaces. SONET frames are scrambled using the SONET commands.

## Example

To enable cell scrambling for ATM port at.9.1:

```
xp(config)# atm set port pdh-cell-scramble on
```

# atm set port vpi-bits

## Purpose

Sets the bit allocation for VPI on an ATM port.

## Format

**atm set port** <port list> **vpi-bits** <num>

## Mode

Configure.

## Description

The **atm set port vpi-bits** command allows you to set the number of bits allocated for VPI on an ATM port. There are 12 bits available for each VPI/VCI pair. The number of bits allocated define the amount of VPI and VCI values available. The following equations define the number of virtual paths and virtual channels:

# of virtual paths =  $2^n$ ; where  $n$  is the number of bits allocated for VPI and  $n$  is a value from 1 to 4

# of virtual channels =  $2^{12-n}$ ; where  $n$  is the number of bits allocated for VCI

Since there are only 12 bits available for each VPI/VCI pair, the more bits you allocate for VPI, the less bits remain for VCI. This is a shared number of bits. With the bit allocation command, you set the number of bits allocated for VPI. In turn, this sets the remaining number of bits as the number of bits allocated for VCI. The maximum value for  $n$  is 4.

**Note:** Be careful when specifying VCI numbers 0 through 31. Those VPI/VCI pairs are used by some protocols for signaling purposes.

**Note:** The maximum value for  $n$  is 4.

## Parameters

|                         |   |
|-------------------------|---|
| <b>port</b> <port list> | This parameter identifies the ATM port. Specify this parameter in the format: <b>media.slot.port</b> . Specify <b>all-ports</b> to set bit allocation on all ports. |
| <b>media</b>            | Specifies the media type. This is <b>at</b> for ATM ports.  |
| <b>slot</b>             | Specifies the slot number where the module is installed.  |
| <b>port</b>             | Specifies the port number.  |

---

|                       |  |
|-----------------------|--|
| <b>vpi-bits</b> <num> | This parameter sets the number of bits for VPI. Specify any number between 1 and 4 (default is 1). |
|-----------------------|--|

---

## Restrictions

None.

## Example

To allocate 3 bits for VPI on port at.9.1:

```
xp(config)# atm set port at.9.1 vpi-bits 3
```

## atm set vcl

### Purpose

Sets the VCL operation mode.

### Format

**atm set vcl port** <port> **forced-bridged**

### Mode

Configure.

### Description

The **atm set vcl** command enables forced bridging on a per-VC basis. Forced-bridging forces the VC to encapsulate all ingress/egress traffic into a Layer-2 frame. This formats all traffic on a VC as bridged traffic, better suited for inter-operability with other routers.

### Parameters

|                       |              |  |
|-----------------------|--------------|--|
| <port>                |              | Specifies a single port, including the virtual channel, in the format:<br><b>media.slot.port.vpi.vci</b>   |
|                       | <b>media</b> | The media type. This is always <b>at</b> for an ATM port.  |
|                       | <b>slot</b>  | The slot number where the module is installed.   |
|                       | <b>port</b>  | The number of the port through which data is passing.  |
|                       | <b>vpi</b>   | The Virtual Path Identifier.   |
|                       | <b>vci</b>   | The Virtual Channel Identifier.  |
| <b>forced-bridged</b> |              | Enables encapsulation of all traffic as Layer-2 bridged traffic. This parameter can be used for inter-operability between the Enterasys X-Pedition router and other vendor products. |

### Restrictions

None.

### Example

To encapsulate all traffic as bridged traffic on at.4.1.0.100:

```
xp(config)# atm set vcl port at.4.1.0.100 forced-bridged
```



# atm show

## Purpose

Display information specific to an ATM port.

## Format

**atm show** [**vpl port** <port list>| **all** [summary]] | [**vcl port** <port list>| **all** [summary]]  
 [**service** <string>| **all**] | [**port-settings** <port list>| **all-ports**] | [**stats port** <port list>]

## Mode

Enable.

## Parameters

|   |  |
|---|--|
| <b>vpl port</b> <port list> <br><b>all</b> [summary]  | Shows VPL configurations on a port.  |
|   | Specify <b>at.slot.port</b> to display all VPL configurations on the port.   |
|   | Specify <b>at.slot.port.vpl</b> to display only the specified VPL configuration on the port.   |
|   | Specify <b>all</b> to display verbose VPL configurations on all ports.   |
|   | Specify <b>summary</b> to display summarized VPL configuration in tabular form.  |
| <b>vcl port</b> <port list> <br><b>all</b> [summary]  | Shows VCL configurations on a port.  |
|   | Specify <b>at.slot.port</b> to display all VCLs configurations on the port.  |
|   | Specify <b>at.slot.port.vpl</b> to display all VCL configurations for a specified VPL.   |
|   | Specify <b>at.slot.port.vpl.vcl</b> to display only the specified VCL configuration on the port.   |
|   | Specify <b>all</b> to display verbose VCL configurations on all ports.   |
|   | Specify <b>summary</b> to display summarized VCL configuration in tabular form.  |
| <b>service</b> <string>  <b>all</b>                   | Shows the profile for a defined service. Specify <b>all</b> to show all ATM service profiles.  |
| <b>port-settings</b><br><port list>  <b>all-ports</b> | Shows the characteristics of an ATM port that were set by the port set command. Specify the port using the following format: <b>at.slot.port</b> . |
|   | Specify <b>all-ports</b> to show characteristics of all ATM ports.   |

---

|                               |  |
|-------------------------------|--|
| <b>stats port</b> <port list> | Specify <b>at.slot.port.vpl</b> to display traffic statistics for all VCLs within a specified VPL. |
|                               | Specify <b>at.slot.port.vpl.vcl</b> to display traffic statistics for the specified VCL only.      |

---

## Restrictions

None.

## Examples

To display information about the VPL configurations on ATM port 1:

```
xp(atm-show)# vpl port at.9.1

VPL Table Contents for Slot 9, Port 1:
Virtual Path Identifier:      1
Administrative Status:       Up
Operational Status:          Up
Last State Change:           1581
Service Definition:          default-OC3
    Service Class:            UBR
    Peak Bit Rate:            Best Effort
    Sustained Bit Rate:       0 Kbits/sec (0 cps)
    Maximum Burst Size:       0 cells
    Encapsulation Type:       LLC Multiplexing
    F5-OAM:                   Responses Only
    F5-OAM-Type:              Current Segment
```

- **Virtual Path Identifier**      Identifies a particular VP.
- **Administrative Status**      Shows whether the VP is a viable network element.  
    **Up** indicates a viable network element.  
    **Down** indicates a non-viable network element.
- **Operational Status**          Shows whether the VP is passing traffic.  
    **Up** indicates traffic.  
    **Down** indicates no traffic.
- **Last State Change**          Shows the last time the VP went up or down. Time is in seconds relative to system boot-up.
- **Service Definition**          Shows the name of the defined service and its traffic parameters.

To display information about all the defined service profiles for UBR:

```
xp# atm show service all

default-OC3
  Service Class:      UBR
  Peak Bit Rate:     Best Effort
  Sustained Bit Rate: 0 Kbits/sec (0 cps)
  Maximum Burst Size: 0 cells
  Encapsulation Type: LLC Multiplexing
  F5-OAM:             Responses Only
  F5-OAM-Type:       Current Segment
```

- **Service Class**                      Shows the type of service class.  
**UBR** indicates Unspecified Bit Rate.  
**CBR** indicates Constant Bit Rate.  
**RT-VBR** indicates Real-time Variable Bit Rate.  
**NRT-VBR** indicates Non Real-time Variable Bit Rate.
- **Peak Bit Rate**                      Shows the maximum bit transmission rate.
- **Sustained Bit Rate**                Shows the average bit transmission rate (in Kilobits per second).
- **Maximum Burst Size**               Shows how many cells can be transmitted at the Peak Bit Rate.
- **Encapsulation Type**               Shows the encapsulation scheme to transport multi protocol data over the AAL5 layer.  
**LLC Multiplexing** indicates logical link control encapsulation (**default**).  
**VC Multiplexing** indicates VC-based multiplexing encapsulation.
- **F5-OAM**                               Shows how OAM (Operation, Administration, and Management) loopback cells provide loopback capabilities and confirm whether a VC connection is up. F5 OAM segments and end-to-end are supported, which provides loopback capabilities on a VC connection level.  
**Responses Only** indicates that the port will respond but doesn't generate OAM cells.  
**Requests & Responses** indicates that the port will respond and generate OAM cells.
- **F5-OAM-Type**                        Shows F5-OAM-Type setting.

To display port-setting information about ATM port 1:

```
xp(atm-show)# port-settings at.9.1
Port information for Slot 9, Port 1:
  Port Type:          T3 ATM coaxial cable
  Xmt Clock Source:   Local
  Scramble Mode:      Payload
  Line Coding:        B3ZS
  Cell Mapping:       Direct
  Framing             Cbit-Parity
  VC Mode:            1 bit of VPI, 11 bits of VCI
  Service Definition: default-OC3
  Service Class:      UBR
  Peak Bit Rate:      Best Effort
  Sustained Bit Rate: 0 Kbits/sec (0 cps)
  Maximum Burst Size: 0 cells
  Encapsulation Type: LLC Multiplexing
  F5-OAM:             Requests & Responses
  F5-OAM-Type:        Current Segment
```

- Port Type                      Shows the type of PHY interface for the port.
- Xmt Clock Source              Shows the timing source for the port.  
**Local** indicates the on board clock oscillator as the timing source.  
**Loop** indicates the receiver input as the timing source.
- Scramble Mode                Shows the scramble/descramble mode for the port.  
**None** indicates no scrambling.  
**Payload** indicates scrambling of the payload only.  
**Frame** indicates scrambling of the stream only.  
**Both** indicates scrambling of payload and stream.
- Line Coding                  Shows the particular DS1/T1 and DS3/T3 coding convention.
- Cell Mapping                Shows the format used to map ATM cells.  
**Direct** indicates direct cell mapping.  
**Plcp** indicates physical layer convergence protocol mapping.
- Framing                      Shows the type of framing scheme.  
**cbit-parity** is used for T3 framing.  
**m23** is used for T3 framing.  
**esf** indicates extended super frame and is used for T1 framing.  
**g832** is used for E3 framing.  
**g751** is used for E3 framing.
- VC Mode                      Shows the bit allocation for VPI and VCI.
- Service Definition            Shows the name of the defined service on the port and its traffic parameters.

# Chapter 9

## bgp Commands

The bgp commands let you display and set parameters for the Border Gateway Protocol (BGP).

### Notes:

- BGP management traps are not supported in this release.
- The X-Pedition router does not currently follow “Breaking Ties (Phase2),” Section 9.1.2.1 (p. 37-38) of RFC 1771. Instead, the router follows “Breaking Ties (Phase2),” Section 9.1.2.2 (p. 49-50) of Draft-ietf-ier-bgp-4-17.

## Command Summary

[Table 9](#) lists the bgp commands. The sections following the table describe the command syntax.

**Table 9. bgp Commands**

|   |
|---|
| <b>bgp add network</b> <ipaddr-mask>  <b>all group</b> <number-or-string> |
| <b>bgp add peer-host</b> <ipaddr> <b>group</b> <number-or-string>         |
| <b>bgp clear peer-host</b> <ipaddr>                                       |
| <b>bgp create peer-group</b> <number-or-string>                           |
| <b>bgp set bad-path</b> [ <b>discard</b>   <b>ignore</b> ]                |
| <b>bgp set DampenFlap</b> <option>  |
| <b>bgp set default-metric</b> <num>                                       |
| <b>bgp set cluster-id</b> <ipaddr>  |
| <b>bgp set internal-set-pref</b> <num>                                    |

Table 9. bgp Commands (Continued)

|  |
|--|
| <b>bgp set multipath off</b>   |
| <b>bgp set peer-group</b> <number-or-string>   |
| <b>bgp set peer-host</b> <ipaddr>  |
| <b>bgp set preference</b> <num>  |
| <b>bgp show aspaths</b> <aspath> all [to-terminal to-file]   |
| <b>bgp show cidr-only</b> <ip-addr-mask> default all [to-terminal to-file]   |
| <b>bgp show community</b> <standard-community-string>  <extended-community-string> <br>no-export no-advertise no-export-subconfed]] [to-terminal to-file]  |
| <b>bgp show flap-statistics</b> [<ip-addr-mask> damped suppressed history]   |
| <b>bgp show peer-as</b> <number> [to-terminal to-file]   |
| <b>bgp show peer-group-type</b> external internal routing [to-terminal to-file]  |
| <b>bgp show peer-host</b> <ipAddr> received-routes all-received-routes  advertised-routes<br>[to-terminal to-file]   |
| <b>bgp show regexp</b> to-terminal to-file   |
| <b>bgp show routes</b> <ip-addr-mask> default all [to-terminal to-file]  |
| <b>bgp show summary</b> [to-terminal to-file]  |
| <b>bgp show sync-tree</b>  |
| <b>bgp start stop</b>  |
| <b>bgp trace packets</b> [detail  send  receive  group <number-or-string>  peer-host <ipaddr>] <br>open [detail  send  receive  group <number-or-string>  peer-host <ipaddr>] <br>update [detail  send  receive  group <number-or-string>  peer-host <ipaddr>] <br>keep-alive [detail  send  receive  group <number-or-string>  peer-host <ipaddr>] <br>aspath [group <number-or-string>  peer-host <ipaddr>] local-options [all  general  state <br>normal  policy  task  timer  route  group <number-or-string>  peer-host <ipaddr>] |

# bgp add network

## Purpose

Adds a network to a BGP peer group.

## Format

**bgp add network** <ip-addr-mask>|**all** **group** <number-or-string>

## Mode

Configure.

## Description

The **bgp add network** command lets you add a BGP peer network, thus allowing peer connections from any addresses in the specified range of network and mask pairs.

## Parameters

|  |  |
|--|--|
| <b>network</b><br><ip-addr-mask>  <b>all</b> | Specifies a network from which peer connections are allowed. Specify an IP address and Mask value. Example: 1.2.3.4/255.255.0.0 or 1.2.3.4/16. Specify <b>all</b> to add all networks. |
| <b>group</b><br><number-or-string>           | Specifies the group ID associated with this network range.   |

## Restrictions

None.

# bgp add peer-host

## Purpose

Add a BGP peer by adding a peer host.

## Format

**bgp add peer-host** <ipaddr> **group** <number-or-string>

## Mode

Configure.

## Description

The **bgp add peer-host** command adds a peer-host to a BGP group.

## Parameters

|                                 |   |
|---------------------------------|---|
| <b>peer-host</b> <ipaddr>       | Specifies the peer host's IP address.                               |
| <b>group</b> <number-or-string> | Specifies the group ID of the group to which the peer host belongs. |

## Restrictions

When adding multiple peer hosts to a peer group, you may not connect more than one peer group to the same AS.



# **bgp clear peer-host**

## **Purpose**

Disconnect and re-establish a peer connection.

## **Format**

**bgp clear peer-host** *<ipaddr>*

## **Mode**

Enable.

## **Description**

The **bgp clear peer-host** command sends a notification packet to the selected peer host, causing the peer session to close and re-establish.

## **Parameters**

---

|  |                                       |
|--|---------------------------------------|
| <b>peer-host</b> <i>&lt;ipaddr&gt;</i> | Specifies the peer host's IP address. |
|--|---------------------------------------|

---

## **Restrictions**

None.

## bgp create peer-group

### Purpose

Create a BGP group based on a type and autonomous system number. You may create any number of groups, but each group must have a unique combination of type and autonomous system.

### Format

```
bgp create peer-group <number-or-string> type external|internal|routing  
[autonomous-system <number>][proto any|rip|ospf|static]  
[interface <interface-name-or-ipaddr> |all]
```

### Mode

Configure.

### Description

The **bgp create peer-group** command creates an entity into which peers are added. Peers are added to this group with the commands **bgp add peer-host** or **bgp add network**. Once a group is created, group-wide parameters may be applied with the **bgp set peer-group** command.

### Parameters

---

|   |   |
|---|---|
| <b>peer-group</b><br><number-or-string> | Is a group ID, which can be a number or a character string. |
|---|---|

---

|  |   |
|--|---|
| <b>type</b>  | Type of BGP group to add. Specify one of the following: <ul style="list-style-type: none"> <li><b>external</b> Use for external BGP peers. Full policy checking is applied to all incoming and outgoing advertisements. All peers in this group must be directly reachable through a local interface (i.e., they must be L2 adjacent).</li> <li><b>internal</b> Use for IBGP peers only, where no IGP is used. This group expects all peers to be Layer-2 adjacent so that next hops received in updates can be used directly for forwarding.</li> <li><b>routing</b> An IBGP type that uses the routes of an interior protocol to resolve forwarding addresses (this implementation comes closest to the IBGP implementation of other router vendors). This type determines the immediate next hops for routes by using the next hop received with a route from a peer as a forwarding address, and using this to look up an immediate next hop in an IGP's routes. Such groups support distant peers, but need to be informed of the IGP whose routes they are using to determine immediate next hops.</li> </ul> |
| <b>autonomous-system</b>                                 | Specifies the autonomous system of the peer group. Specify a number from 1 – 65534.   |
| <b>proto</b>   | Used for group-type routing only. Specifies the interior protocol to use to resolve BGP next hops. Specify one of the following: <ul style="list-style-type: none"> <li><b>any</b> Use any IGP to resolve BGP next hops.</li> <li><b>rip</b> Use RIP to resolve BGP next hops.</li> <li><b>ospf</b> Use OSPF to resolve BGP next hops.</li> <li><b>static</b> Use static to resolve BGP next hops.</li> </ul>   |
| <b>interface</b> <interface-name-or-ipAddr>   <b>all</b> | Interfaces whose routes are carried via the IGP for which third-party next hops may be used instead. Use only with parameter type ROUTING. Specify the interface or use <b>all</b> to use all interfaces.   |

**Note:** Enterasys recommends that you use alphabetic characters when defining interface names—purely numeric interfaces will be interpreted as IP addresses. The X-Pedition router will display interface names up to 32 characters in length.

## Restrictions

None.

## bgp set bad-aspath

### Purpose

Specifies the handling of routes with bad aspaths.

### Format

**bgp set bad-aspath** [**discard** | **ignore**]

### Mode

Configure.

### Description

The **bgp set bad-aspath** command specifies whether bad aspaths should be discarded or ignored. The default action is to reset the BGP peering session.

### Parameters

|                |   |
|----------------|---|
| <b>discard</b> | Specifies to discard routes with bad aspaths. |
| <b>ignore</b>  | Specifies to ignore routes with bad aspaths.  |

### Restrictions

None.

# bgp set cluster-id

## Purpose

Specifies the route reflection cluster ID for BGP.

## Format

**bgp set cluster-id** *<ipAddr>*

## Mode

Configure.

## Description

The **bgp set cluster-id** command specifies the route reflection cluster ID for BGP. The cluster ID defaults to the same as the router-id. If a router is to be a route reflector, then a single cluster ID should be selected and configured on all route reflectors in the cluster. If there is only one route reflector in the cluster, the cluster ID setting may be omitted, as the default will suffice.

## Parameters

|   |             |
|---|-------------|
| <b>cluster-id</b> <i>&lt;ipAddr&gt;</i> | Cluster ID. |
|---|-------------|

## Restrictions

The only constraints on the choice of cluster ID are (a) IDs of clusters within an AS must be unique within that AS, and (b) the cluster ID must not be 0.0.0.0. Choosing the cluster ID to be the router ID of one router in the cluster will always fulfill these criteria.

# bgp set dampenflap

## Purpose

Configures parameters for Weighted Route Dampening.

## Format

```
bgp set dampenflap [state enable|disable][suppress-above <num>][  
reuse-below <num>][max-flap <num>][unreach-decay <num>][reach-decay <num>][  
keep-history <num>]
```

## Mode

Configure.

## Description

The **bgp set dampenflap** command configures the state of Weighted Route Dampening.

## Parameters

|   |   |
|---|---|
| <b>state enable disable</b>                 | Causes the Route Instability History to be maintained (enable option) or not (disable option).  |
| <b>suppress-above</b><br><i>&lt;num&gt;</i> | Value of the instability metric at which route suppression will take place. A route will not be installed in the FIB or announced even if it is reachable during the period that it is suppressed. The default is 3.0.  |
| <b>reuse-below</b> <i>&lt;num&gt;</i>       | Value of the instability metric at which a suppressed route will become <i>unsuppressed</i> , if it is reachable but currently suppressed. The value must be less than that for the suppress-above option. The default is 2.0.  |
| <b>max-flap</b> <i>&lt;num&gt;</i>          | Upper limit of the instability metric. This value must be greater than the larger of 1 and that for suppress-above. The default is 16.0.  |
| <b>unreach-decay</b><br><i>&lt;num&gt;</i>  | Specifies the time in seconds for the instability metric value to reach one-half of its current value when the route is <i>unreachable</i> . This half-life value determines the rate at which the metric value is decayed. The default is 900.   |
| <b>reach-decay</b> <i>&lt;num&gt;</i>       | Specifies the time in seconds for the instability metric value to reach one-half of its current value when the route is <i>reachable</i> . This half-life value determines the rate at which the metric value is decayed. A smaller half-life value will make a suppressed route reusable sooner than a larger value. The default is 300. |

---

|                                    |   |
|------------------------------------|---|
| <b>keep-history</b> < <i>num</i> > | Specifies the period in seconds over which the route flapping history is to maintained for a given route. The size of the configuration arrays is directly affected by this value. The default is 1800. |
|------------------------------------|---|

---

## Restrictions

None.

## bgp set default-metric

### Purpose

Set the metric used when advertising routes through BGP.

### Format

**bgp set default-metric** *<num>*

### Mode

Configure.

### Description

The **bgp set default-metric** command lets you set the default metric BGP uses when it advertises routes. If this command is not specified, no metric is propagated. This metric may be overridden by a metric specified on the neighbor or group statements or in an export policy.

### Parameters

|                    |  |
|--------------------|--|
| <i>&lt;num&gt;</i> | Specifies the default cost. Specify a number from 0 - 65535. |
|--------------------|--|

### Restrictions

None.



# bgp set internal-set-pref

## Purpose

Set the set-pref metric used to allow use of LOCAL\_PREF attribute for internal and routing peers.

## Format

**bgp set internal-set-pref** <num>

## Mode

Configure.

## Description

Allows BGP's LOCAL\_PREF attribute to be used to set the GateD preference on reception, and allows the GateD preference to set the LOCAL\_PREF on transmission. The set-pref metric works as a lower limit, below which the imported LOCAL\_PREF may not set the GateD preference. For internal and routing peers. Specify a number from 0 - 255. This parameter is applied to each configured internal or routing peer. Unless you set this parameter, GateD will ignore the LOCAL\_PREF value received in update packets sent from internal or routing peer groups. When set, the RIB will use LOCAL\_PREF to calculate the preference of routes received in those updates. The preference (Prf1 in the RIB table) is calculated as (254 - LOCAL\_PREF + set-pref). This ensures that you can never set Prf1 lower than the set-pref value by a received LOCAL\_PREF. The global protocol preference (Prf1) determined by the RIB will be used to set LOCAL\_PREF on transmitted updates.

## Parameters

|       |  |
|-------|--|
| <num> | Specifies the default cost. Specify a number from 0-255. |
|-------|--|

## Restrictions

None.

## bgp set multipath

### Purpose

Disables multipath route calculation for BGP routes.

### Format

**bgp set multipath off**

### Mode

Configure.

### Description

The **bgp set multipath** command disables multipath route calculation for BGP routes. No multipath forwarding occurs as a result of this command.

### Parameters

|            |  |
|------------|--|
| <b>off</b> | Disables multipath route calculation for BGP routes. |
|------------|--|

### Restrictions

If you negate this command from the active configuration file, the X-Pedition router will not automatically recreate multipath routes. To recreate multipath routes, stop and restart BGP.

# bgp set peer-group

## Purpose

Set parameters for the specified BGP Peer Group.

## Format

```
bgp set peer-group <number-or-string> [med|reflector-client| no-client-reflect|
[metric-out <num>]] [local-as <num>] | ignore-first-as-hop|
[generate-default enabled|disabled]] [gateway <ipAddr>]] next-hop-self
[preference <num>][preference2 <num>] [local-address <ipAddr>]] [hold-time <num>]]
passive| [send-buffer <num>]] [recv-buffer <num>]] [out-delay <num>]] [keep all|none]]
show-warnings| no-aggregator-id| keep-alives-always| no-v4-asloop| [as-count <num>]]
log-up-down| [ttl <num>]] [optional-attributes-list <number-or-string>]] confederation
```

## Mode

Configure.

## Description

The **bgp set peer-group** command sets parameters for the specified BGP group.

## Parameters

|                                    |  |
|------------------------------------|--|
| <b>group</b><br><number-or-string> | Specifies the group.   |
| <b>med</b>                         | <p>Forces Multi-Exit Discriminator (MED) to be used for route selection process. By default, any metric (Multi_Exit_Disc, or MED) received on a BGP connection is ignored. To use MEDs in route selections, you <i>must</i> specify this option. Furthermore, the X-Pedition router does not send MEDs on external connections. To send MEDs, use the metric option of the <b>ip-router policy create bgp-export-destination</b> command or select the <b>bgp set metric-out</b> command.</p> <p><b>Note:</b> Before the router can process and select the correct route based on the MED values received from other BGP peers, users must set the selection process in the active configuration of the router where the peer is defined. To set the selection process, enter one (or both) of the following commands in the configuration, depending on the type of BGP peer configured (i.e., peer group, peer host, or both):</p> <pre>bgp set peer-group &lt;group_name&gt; med bgp set peer-host &lt;IPaddr&gt; med</pre> |

|   |   |
|---|---|
| <b>reflector-client  <br/>no-client-reflect</b> | <p>The <b>reflector-client</b> option specifies that GateD will act as a route reflector for this group. All routes received from any group member will be sent to all other internal neighbors, and all routes received from any other internal neighbors will be sent to the reflector clients. Since the route reflector forwards routes in this way, the reflector-client group need not be fully meshed. Use only for <i>internal</i> and <i>routing</i> groups.</p> <p>If the <b>no-client-reflect</b> option is specified, routes received from reflector clients will only be sent to internal neighbors which are not in the same group as the sending reflector client. In this case the reflector-client group should be fully meshed. In all cases, routes received from normal internal peers will be sent to all reflector clients.</p> <p><b>Note:</b> It is necessary to export routes from the local AS into the local AS when acting as a route reflector. The <b>reflector-client</b> option specifies that GateD will act as a route reflector for this group. All routes received from any group member will be sent to all other internal neighbors, and all routes received from any other internal neighbors will be sent to the reflector clients. Since the route reflector forwards routes in this way, the reflector-client group need not be fully meshed.</p> |
| <b>confederation</b><br><number-or-string>      | Set this parameter for all groups in the same confederation.  |
| <b>metric-out</b> <num>                         | Specifies the primary metric used on all routes sent to the specified peer group. Specify a number from 0 - 65535.  |
| <b>local-as</b> <num>                           | Identifies the autonomous system which the router is representing to this group of peers. The default is the one configured by the <b>set autonomous_system</b> command. Specify a number from 1 - 65534.   |
| <b>ignore-first-as-hop</b>                      | Some routers, known as Route Servers, are capable of propagating routes without appending their own AS to the AS path. By default, GateD drops such routes. Specifying ignore-first-as-hop here or on either the create peer-group or set peer-host CLI commands disables this feature. This option should only be used if it is positively known that the peer is a route server and not a normal router.  |
| <b>generate-default<br/>enabled disabled</b>    | Specifies whether the router should generate a default route when BGP receives a valid update from its peer. If this option is not specified, then the generation of default route is enabled.  |
| <b>gateway</b> <ipAddr>                         | If a network is not shared with a peer, this option specifies a router on an attached network to be used as the next hop router for routes received from this neighbor. This field is used for EBGp Multihop. The IP address must be a host address on a locally attached network.  |

|                               |  |
|-------------------------------|--|
| <b>next-hop-self</b>          | Causes the next hop in route advertisements set to this peer or group of peers to be set to our own router's address even if it would normally be possible to send a third-party next hop. Use of this option may cause efficient routes to be followed, but it may be needed in some cases to deal with broken bridged interconnect media (in cases where the routers on the shared medium do not really have full connectivity to each other) or broken political situations. Use only for EXTERNAL groups.  |
| <b>preference</b> <num>       | Specifies the preference used for routes learned from these peers. Specify a number from 0-255.  |
| <b>preference2</b> <num>      | In case of a preference tie, this option (second preference), may be used to break the tie. Default is 0. Specify a number from 0-255.   |
| <b>local-address</b> <ipAddr> | Specifies the address to be used on the local end of the TCP connection with the peer or with the peer's gateway when the gateway option is used. A session with an external peer will only be opened when an interface with the appropriate local address (through which the peer or gateway address is directly reachable). In either case incoming connections will only be recognized as matching a configured peer if they are addressed to the configured local address. Use for <i>internal</i> and <i>routing</i> groups only. It should be one of the interface addresses.  |
| <b>hold-time</b> <num>        | <p>Specifies the hold time value (in seconds) to use when negotiating the connection with this peer. If BGP does not receive a keepalive, update, or notification message from a peer within the period specified in the Hold Time field of the BGP Open message, the BGP connection will be closed. The value must be either 0 (no keepalives will be sent) or a value from 6 to 65,535.</p> <p><b>Note:</b> Every time a user changes the hold time for a BGP session (whether for a peer group or peer host), the X-Pedition router will close and re-open the connection when the user saves the change to the active configuration.</p> |
| <b>passive</b>                | Specifies that active OPENs to this peer should not be attempted. BGP would wait for the peer to issue an OPEN. By default, all explicitly configured peers are active, they periodically send OPEN messages until the peer responds. If it is applied to both sides of a peering session, it prevents the session from ever being established.  |
| <b>send-buffer</b> <num>      | Controls the amount of send buffer acquired from the memory subsystem. The maximum supported is 65535 bytes. By default, BGP acquires the maximum supported. Specify a number from 4096 to 65535.  |
| <b>recv-buffer</b> <num>      | Controls the amount of receive buffer acquired from the memory subsystem. The maximum supported is 65535 bytes. By default, BGP acquires the maximum supported. Specify a number from 4096 to 65535.   |

|  |   |
|--|---|
| <b>out-delay</b> <num>                             | Used to dampen route fluctuations. Out delay is the time in seconds a route must be present in the routing table before it is exported to BGP. Specify a number equal to or greater than 0. The default value is 0, meaning that this feature is disabled.  |
| <b>keep-all</b>  none                              | Used to retain routes learned from a peer even if the routes' AS paths contain one of our exported AS numbers.  |
| <b>show-warnings</b>                               | Causes GateD to issue warning messages when receiving questionable BGP updates such as duplicate routes and/or deletions of non-existing routes. Normally these events are silently ignored.  |
| <b>no-aggregator-id</b>                            | Causes GateD to specify the router ID in the aggregator attribute as zero (instead of its router ID) in order to prevent different routers in an AS from creating aggregate routes with different AS paths.   |
| <b>keep-alives-always</b>                          | Causes GateD to always send keepalives, even when an update could have correctly substituted for one. This allows inter-operability with routers that do not completely obey the protocol specifications on this point.   |
| <b>no-v4-asloop</b>                                | Prevents routes with looped AS paths from being advertised to version 4 external peers. This can be useful to avoid advertising such routes to peer which would incorrectly forward the routes on to version 3 neighbors.   |
| <b>as-count</b> <num>                              | <p>Determines how many times the X-Pedition router will insert its own AS number when we send the AS path to an external neighbor.</p> <p>Specify a number between 1 and 25. The default is 1. Higher values typically are used to bias upstream neighbors' route selection. (All else being equal, most routers will prefer to use routes with shorter AS Paths. Using ascount, the AS Path the X-Pedition router sends can be artificially lengthened.)</p> <p>Ascount supersedes the <b>no-v4-asloop</b> option, regardless whether <b>no-v4-asloop</b> is set. The router still sends multiple copies of its own AS if the <b>as-count</b> option is greater than 1. Also, if the ascount value is changed and GateD is reconfigured, routes will not be sent to reflect the new setting. If this is desired, you need to restart the peer session.</p> |
| <b>log-up-down</b>                                 | Causes a message to be logged via the Syslog mechanism whenever a BGP peer enters or leaves the ESTABLISHED state.  |
| <b>ttl</b> <num>                                   | By default, BGP sets the IP TTL for local peers to 1 and the TTL for non-local peers to 255. This option is provided when attempting to communicate with improperly functioning routers that ignore packets sent with a TTL of 1. Specify a number between 1 and 255.   |
| <b>optional-attributes-list</b> <number-or-string> | Specifies the ID of the optional-attributes-list to be associated with this peer-group.   |

## Restrictions

None.

# bgp set peer-host

## Purpose

Set parameters for a BGP peer host.

## Format

```
bgp set peer-host <ipAddr> [group <number-or-string>][metric-out <num>][local-as <num>]
ignore-first-as-hop[generate-default enabled|disabled][gateway <ipaddr>]next-hop-self
[preference <num>][preference2 <num>][local-address <ipaddr>][hold-time <num>]
passive[send-buffer <num>][recv-buffer <num>][out-delay <num>] [keep all|none]
show-warningsno-aggregator-idkeep-alives-alwaysno-v4-asloop[as-count <num>]
[ttl <num>][med]
```

## Mode

Configure.

## Description

The **bgp set peer-host** command lets you set various parameters for the specified BGP peer host.

## Parameters

|  |   |
|--|---|
| <i>&lt;ipAddr&gt;</i>                        | IP address of the BGP peer host.  |
| <b>group</b> <i>&lt;number-or-string&gt;</i> | Specifies the group ID  |
| <b>metric-out</b> <i>&lt;num&gt;</i>         | Specifies the primary metric used on all routes sent to the specified peer. The metric hierarchy is as follows, starting from the most preferred:<br>1) Metric specified by export policy. 2) Peer-level metricout. 3) Group-level metricout 4) Default metric. For <i>internal</i> and <i>routing</i> peers use the group command to set the metric-out. Specify a number from 0 - 65535.  |
| <b>med</b>                                   | Forces med to be used for route selection process. By default, any metric (Multi_Exit_Disc, or MED) received on a BGP connection is ignored. To use MEDs in route selections, you <i>must</i> specify this option. Furthermore, the X-Pedition router does not send MEDs on external connections. To send MEDs, use the <b>metric</b> option of the <b>ip-router policy create bgp-export-destination</b> command or select the <b>metric-out</b> parameter of the <b>bgp set</b> commands. |
| <b>local-as</b> <i>&lt;num&gt;</i>           | Identifies the autonomous system the router is representing to this peer. The default is the one configured using the <b>ip-router global set autonomous-system</b> command. Specify a number from 1 - 65534.   |

|  |   |
|--|---|
| <b>ignore-first-as-hop</b>               | Some routers, known as Route Servers, are capable of propagating routes without appending their own AS to the AS path. By default, GateD will drop such routes. Specifying ignore-first-as-hop here or on either the <b>bgp create peer-group</b> or <b>bgp set peer-host</b> CLI commands disables this feature. This option should only be used if it is positively known that the peer is a route server and not a normal router.  |
| <b>generate-default enabled disabled</b> | Specifies whether the router should generate a default route when BGP receives a valid update from its peer. If this option is not specified, then the generation of default route is enabled.  |
| <b>gateway &lt;ipAddr&gt;</b>            | If a network is not shared with a peer, this option specifies a router on an attached network to be used as the next hop router for routes received from this neighbor. This is used for EBGp multihop. The IP address must be a host address on a locally attached network.  |
| <b>next-hop-self</b>                     | Causes the next hop in route advertisements set to this peer to be set to our own router's address, even if it would normally be possible to send a third-party next hop. Use of this option may cause inefficient routes to be followed, but it may be needed in some cases to deal with broken bridged interconnect media (in cases where the routers in the shared medium do not really have full connectivity to each other) or broken political situations. Use only for external peer hosts.  |
| <b>preference &lt;num&gt;</b>            | Specifies the preference used for routes learned from this peer. This can differ from the default BGP preference set in the bgp set preference statement, so that GateD can prefer routes from one peer, or group of peer, over others. This preference may be explicitly overridden by import policy. Specify a number from 0 - 255.   |
| <b>preference2 &lt;num&gt;</b>           | In case of preference tie, this option (the second preference), may be used to break the tie. Default value is 0. Specify a number from 0 - 255.  |
| <b>local-address &lt;IPaddr&gt;</b>      | Specifies the address to be used on the local end of the TCP connection with the peer or with the peer's gateway when the gateway option is used. A session with an external peer is opened only when an interface with the appropriate local address (through which the peer or gateway address is directly reachable) is operating. For other types of peers, a peer session will be maintained when any interface with the specified local address is operating. In either case incoming connections will only be recognized as matching a configured peer if they are addressed to the configured local address. For <i>internal</i> and <i>routing</i> peers, use the group command to set the local-address—the address should be one of the interface addresses. |
| <b>hold-time &lt;num&gt;</b>             | <p>Specifies the hold time, in seconds, used when negotiating the connection with this peer. If BGP does not receive a keepalive, update, or notification message from a peer within the period specified in the Hold Time field of the BGP Open message, then the BGP connection will be closed. The value must be 0 (no keepalives will be sent) or at least 6.</p> <p>A hold-time of 0 is not negotiated. If the remote peer attempts to negotiate any value other than 0, the higher value is used. To prevent keepalives from being exchanged, configure both peers to use a hold-time of 0.</p>   |



|                           |   |
|---------------------------|---|
| <b>passive</b>            | Specifies that active OPENs to this peer should not be attempted. BGP would wait for the peer to issue an OPEN. By default, all explicitly configured peers are active, they periodically send OPEN messages until the peer responds. Note that if it is applied to both sides of a peering session, it will prevent the session from ever being established.   |
| <b>send-buffer</b> <num>  | Controls the amount of send buffer acquired from the memory subsystem. The maximum supported is 65535 bytes. By default, BGP acquires the maximum supported. Specify a number from 4096 - 65535.  |
| <b>recv-buffer</b> <num>  | Controls the amount of receive buffer acquired from the memory subsystem. The maximum supported is 65535 bytes. By default, BGP acquires the maximum supported. Specify a number from 4096 – 65535.   |
| <b>out-delay</b> <num>    | Used to dampen route fluctuations. Out delay is the amount of time in seconds a route must be present in the routing table before it is exported to BGP. The default value is 0, meaning that this feature is disabled. Specify a number equal to or greater than 0.  |
| <b>keep all none</b>      | Used to retain routes learned from a peer even if the routes' AS paths contain one of our exported AS numbers.  |
| <b>show-warnings</b>      | This option causes GateD to issue warning messages when receiving questionable BGP updates such as duplicate routes and/or deletions of non-existing routes. Normally these events are silently ignored.  |
| <b>no-aggregator-id</b>   | This option causes GateD to specify the router ID in the aggregator attribute as zero (instead of its router ID) in order to prevent different routers in an AS from creating aggregate routes with different AS paths.   |
| <b>keep-alives-always</b> | This option causes GateD to always send keepalives, even when an update could have correctly substituted for one. This allows inter operability with routers that do not completely obey the protocol specifications on this point.   |
| <b>no-v4-asloop</b>       | Prevents routes with looped AS paths from being advertised to version 4 external peers. This can be useful to avoid advertising such routes to peer which would incorrectly forward the routes on to version 3 neighbors.   |
| <b>as-count</b> <num>     | <p>Determines how many times (1-25) the router inserts its own AS number when it sends the AS path to an external neighbor. Specify a number equal to or greater than 0. The default is 1. Higher values are typically used to bias upstream neighbors' route selection.</p> <p><b>Note:</b> <b>As-count</b> supersedes the <b>no-v4-asloop</b> option. If you set the <b>as-count</b> option to something greater than 1, the X-Pedition router will still send multiple copies of its own AS.</p> <p>Also, if you change the value of <b>as-count</b> and reconfigure GateD, routes will not be sent to reflect the new setting. If you want to send new routes containing this information, you must restart the peer session. Use for external peer-hosts only.</p> |
| <b>log-up-down</b>        | Causes a message to be logged via the Syslog mechanism whenever a BGP peer enters or leaves the ESTABLISHED state.  |

---

|                  |  |
|------------------|--|
| <b>ttl</b> <num> | By default, BGP sets the IP TTL for local peers to ONE and the TTL for non-local peers to 255. This option is provided when attempting to communicate with improperly functioning routers that ignore packets sent with a TTL of ONE. Specify a number from 1-255. |
|------------------|--|

---

## Restrictions

When adding multiple peer hosts to a peer group, you may not connect more than one peer group to the same AS.

# **bgp set preference**

## **Purpose**

Set BGP preference.

## **Format**

**bgp set preference** *<num>*

## **Mode**

Configure.

## **Description**

The **bgp set preference** command lets you set the BGP preference for the X-Pedition router.

## **Parameters**

---

|                    |   |
|--------------------|---|
| <i>&lt;num&gt;</i> | Specifies the preference of routes learned from BGP. Specify a number from 0 -255. The default preference is 170. |
|--------------------|---|

---

## **Restrictions**

None.

# bgp show aspaths

## Purpose

Displays BGP AS path information.

## Format

**bgp show aspaths** <aspath>|all [to-terminal|to-file]

## Mode

Enable.

## Description

The **bgp show aspaths** command displays information about a specified AS path or all AS paths. The AS path is listed along with the number of routes that use it.

## Parameters

|                    |   |
|--------------------|---|
| <aspath>           | Displays information about the specified AS path.                   |
| <b>all</b>         | Displays information about all AS paths.                            |
| <b>to-terminal</b> | Causes output to be displayed on the terminal. This is the default. |
| <b>to-file</b>     | Causes output to be saved in the file /gatedtrc/gated.dmp.          |

## Restrictions

None.

## Example

To display information about all AS paths:

```
xp# bgp show aspaths all
Hash Ref Path
0 5 IGP (Id 1)
2 1 (64900) 64901 64902 IGP (Id 3)
7 4 (64900) 64901 IGP (Id 2)
```

# bgp show cidr-only

## Purpose

Display routes in the BGP routing table with CIDR network masks.

## Format

**bgp show cidr-only** *<ip-addr-mask>* | **all** [**to-terminal** | **to-file**]

## Mode

Enable.

## Description

The **bgp show cidr-only** command displays the same type of route information as the **bgp show routes** command. The difference is that the **bgp show cidr-only** command limits the display to CIDR routes only.

## Parameters

|                             |  |
|-----------------------------|--|
| <i>&lt;ip-addr-mask&gt;</i> | Displays information about the specified CIDR route.                     |
| <b>all</b>                  | Displays information about all CIDR routes.                              |
| <b>to-terminal</b>          | Causes output to be displayed on the terminal.                           |
| <b>to-file</b>              | Causes output to be saved in the file <code>/gatedtrc/gated.dmp</code> . |

## Restrictions

None.

## Example

To display information all CIDR routes in the X-Pedition BGP route table:

```
xp# bgp show cidr-only all
Proto Route/Mask NextHop      ASPath
BGP 12.2.19/25  207.135.89.65 (64800) 64753 64752 64751 6379 3561 11277 IGP (Id 13805)
BGP 2.5.172/22  207.135.89.65 (64800) 64753 64752 64751 6379 3561 1 IGP (Id 173)
BGP 12.5.252/23 207.135.89.65 (64800) 64753 64752 64751 6379 5646 1 7018 6301 IGP (Id 926)
BGP 12.6.42/23  207.135.89.65 (64800) 64753 64752 64751 6379 5646 1 7018 11090 IGP (Id 979)
BGP 12.6.134/23 207.135.89.65 (64800) 64753 64752 64751 6379 5646 1 701 7314 10562 IGP (Id 388)
BGP 12.7.214/23 207.135.89.65 (64800) 64753 64752 64751 6379 5646 7018 4129 IGP (Id 31004)
```

# bgp show community

## Purpose

Displays routes that belong to a specified community.

## Format

**bgp show community** <standard-community-string>| <extended-community-string>|  
no-export|no-advertise|no-export-subconfed]] [to-terminal|to-file]

## Mode

Enable.

## Description

The **bgp show community** command displays routes that belong to a specified community in a specified autonomous system.

## Parameters

|                             |  |
|-----------------------------|--|
| <standard-community-string> | A standard community string in the form:<br><AS-identifier>:<community-identifier> |
| <AS-identifier>             | An autonomous system number. Can be any value from 0 to 65535.                     |
| <community-identifier>      | A community identifier. Can be any value from 0 to 65535.                          |

|  |  |
|--|--|
| <code>&lt;extended-community-string&gt;</code> | An extended community string, in the form:<br><code>&lt;type&gt;:{&lt;AS-identifier   &lt;IPaddr&gt;}:&lt;id&gt;</code>  |
| <code>&lt;type&gt;</code>                      | Type of this extended community. You can specify one of the following:<br><br><b>target</b> Target community identifies the destination to which a router is going.<br><br><b>origin</b> Origin community identifies where a route originated. |
| <code>&lt;AS-identifier&gt;</code>             | Autonomous system number. Can be any value from 1 to 65535.  |
| <code>&lt;ipAddr&gt;</code>                    | IP address.  |
| <code>&lt;id&gt;</code>                        | ID of this extended community, which identifies the local provider. This ID is two bytes long when used with IP addresses and four bytes long when used with AS numbers.   |
| <b>no-export</b>                               | A special community that indicates the routes associated with this attribute must not be advertised outside a BGP confederation boundary.  |
| <b>no-advertise</b>                            | A special community indicating that the routes associated with this attribute must not be advertised to other BGP peers.   |
| <b>no-export-subconfed</b>                     | A special community indicating the routes associated with this attribute must not be advertised to external BGP peers. (This includes peers in other members' autonomous systems inside a BGP confederation.)                                  |
| <b>to-terminal</b>                             | Causes output to be displayed on the terminal. This is the default.  |
| <b>to-file</b>                                 | Causes output to be saved in the file /gatedtrc/gated.dmp.   |

## Restrictions

None.

## Example

To display routes that belong to community 160 in AS 64900:

| xp# <b>bgp show community 64900:160</b> |            |               |             |                                |
|---|------------|---------------|-------------|--------------------------------|
| Rs                                      | Proto      | Route/Mask    | NextHop     | AS Path                        |
| u                                       | BGP        | 192.68.20/24  | 172.16.20.2 | (64901) 64900 IGP (Id 5)       |
| +                                       | Community: | 64900:160     |             |                                |
| u                                       | BGP        | 192.68.222/24 | 172.16.20.2 | (64901 64902) 64900 IGP (Id 6) |
| +                                       | Community: | 64900:160     |             |                                |



# bgp show flap-statistics

## Purpose

Displays route flapping dampen and suppression information.

## Format

**bgp show flap-statistics** [*<ip-addr-mask>* | **damped** | **history** | **suppressed** |**to-terminal**|**to-file**]

## Mode

Enable.

## Description

The **bgp show flap-statistics** command displays information about routers which are flapping. This is useful when bgp set flapDampen is used on the configuration. Can be used to determine which routes have a history of flapping, and whether they are reachable, damped, or suppressed.

## Parameters

|                             |   |
|-----------------------------|---|
| <i>&lt;ip-addr-mask&gt;</i> | IP address and subnet mask of the route to be displayed. If not supplied, all routes are displayed. |
| <b>damped</b>               | Shows routes that are reachable and are being damped due to flapping.                               |
| <b>suppressed</b>           | Shows routes that are reachable and suppressed due to excessive flapping.                           |
| <b>history</b>              | Shows routes that are unreachable and have a history of flapping.                                   |
| <b>to-terminal</b>          | Causes output to be displayed on the terminal. This is the default.                                 |
| <b>to-file</b>              | Causes output to be saved in the file /gatedtrc/gated.dmp.  |

## Restrictions

None.

## Example

To display all routes which are damped:

```
xp# bgp show flap-statistics damped
BGP table : Local router ID is 192.68.11.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

  Network          Next Hop      Metric   Last-Flap   Reuse        Path
*>d 172.16.20/24    172.16.20.2   0.99      00:02:34
*>d 172.16.70/24    172.16.20.2   2.45      00:00:50    00:08:23    64901 i
*>d 172.16.220/24   172.16.20.2   0.76      00:01:34    64901 i
```

# bgp show peer-as

## Purpose

Displays information about TCP and BGP connections to an autonomous system.

## Format

**bgp show peer-as** <number> [to-terminal|to-file]

## Mode

Enable.

## Description

The **bgp show peer-as** command displays information about routers in a specified autonomous system that are peered with the X-Pedition router.

## Parameters

|                         |   |
|-------------------------|---|
| <b>peer-as</b> <number> | AS number of a peer autonomous system.                              |
| <b>to-terminal</b>      | Causes output to be displayed on the terminal. This is the default. |
| <b>to-file</b>          | Causes output to be saved in the file /gatedtrc/gated.dmp.          |

## Restrictions

None.

## Example

To display information about TCP and BGP connections to autonomous system 64901:

```
xp# bgp show peer-as 64901
group type External AS 64901 local 64900 flags <>
peer 172.16.20.2 version 4 lcladdr (null) gateway (null)
flags 0x20
state 0x6 <Established>
options 0x0 <>
metric_out -1 preference 170 preference2 0
recv buffer size 0 send buffer size 0
messages in 10039 (updates 5, not updates 10034) 190863 octets
messages out 10037 (updates 1, not updates 10036) 190743 octets
```

# bgp show peer-group-type

## Purpose

Displays status information about BGP peers by group.

## Format

**bgp show peer-group-type** **external**| **internal**| **routing** [**to-terminal**|**to-file**]

## Mode

Enable.

## Description

The **bgp show peer-group-type** command displays status information about BGP peers according to their group.

## Parameters

|                    |   |
|--------------------|---|
| <b>external</b>    | Displays status information about external peers.                   |
| <b>internal</b>    | Displays status information about internal peers.                   |
| <b>routing</b>     | Displays status information about routing peers.                    |
| <b>to-terminal</b> | Causes output to be displayed on the terminal. This is the default. |
| <b>to-file</b>     | Causes output to be saved in the file /gatedtrc/gated.dmp.          |

## Restrictions

None.

## Example

To display status information about external peers:

```
xp# bgp show peer-group-type external
Group      Neighbor    V  AS    MsgRcvd  MsgSent  State
external   172.16.20.2  4  64901  10045    10044    Established
BGP summary, 1 peers in group type "external"
```

# bgp show peer-host

## Purpose

Displays status information about BGP peer hosts.

## Format

**bgp show peer-host** *<ipAddr>* **received-routes|all-received-routes| advertised-routes**  
**[to-terminal|to-file]**

## Mode

Enable.

## Description

The **bgp show peer-host** command displays information related to a specified BGP peer host. Three types of information can be displayed: routes received and accepted from a BGP peer host, all BGP routes (both accepted and rejected) from a peer host, and all routes the X-Pedition router has advertised to a peer host.

## Parameters

|                            |  |
|----------------------------|--|
| <i>&lt;ipAddr&gt;</i>      | IP address of a BGP peer host.   |
| <b>received-routes</b>     | Displays all valid BGP routes received and accepted from the specified peer host.    |
| <b>all-received-routes</b> | Displays all BGP routes (both accepted and rejected) from the specified peer host.   |
| <b>advertised-routes</b>   | Displays all routes the X-Pedition router has advertised to the specified peer host. |
| <b>to-terminal</b>         | Causes output to be displayed on the terminal. This is the default.                  |
| <b>to-file</b>             | Causes output to be saved in the file /gatedtrc/gated.dmp.                           |

## Restrictions

When adding multiple peer hosts to a peer group, you may not connect more than one peer group to the same AS.

## Examples

To display all valid BGP routes received and accepted from peer host 172.16.20.2:

| xp# <b>bgp show peer-host 172.16.20.2 received-routes</b>                      |             |        |        |      |
|--|-------------|--------|--------|------|
| BGP table : Local router ID is 192.68.11.1                                     |             |        |        |      |
| Status codes: s suppressed, d damped, h history, * valid, > best, i - internal |             |        |        |      |
| Origin codes: i - IGP, e - EGP, ? - incomplete                                 |             |        |        |      |
| Network  | Next Hop    | Metric | LocPrf | Path |
| *> 172.16.70/24  | 172.16.20.2 | 64901  |        | i    |
| *> 172.16.220/24   | 172.16.20.2 | 64901  |        | i    |
| *> 192.68.20/24  | 172.16.20.2 | 64901  |        | i    |
| *> 192.68.222/24   | 172.16.20.2 | 64901  | 64902  | i    |

To display all BGP routes (both accepted and rejected) from peer host 172.16.20.2:

| xp# <b>bgp show peer-host 172.16.20.2 all-received-routes</b>                  |             |        |        |      |
|--|-------------|--------|--------|------|
| BGP table : Local router ID is 192.68.11.1                                     |             |        |        |      |
| Status codes: s suppressed, d damped, h history, * valid, > best, i - internal |             |        |        |      |
| Origin codes: i - IGP, e - EGP, ? - incomplete                                 |             |        |        |      |
| Network  | Next Hop    | Metric | LocPrf | Path |
| 172.16.20/24   | 172.16.20.2 | 64901  |        | i    |
| *> 172.16.70/24  | 172.16.20.2 | 64901  |        | i    |
| *> 172.16.220/24   | 172.16.20.2 | 64901  |        | i    |
| *> 192.68.20/24  | 172.16.20.2 | 64901  |        | i    |
| *> 192.68.222/24   | 172.16.20.2 | 64901  | 64902  | i    |

Displays all routes the X-Pedition router has advertised to peer host 172.16.20.2:

| xp# <b>bgp show peer-host 172.16.20.2 advertised-routes</b>                    |             |        |        |      |
|--|-------------|--------|--------|------|
| BGP table : Local router ID is 192.68.11.1                                     |             |        |        |      |
| Status codes: s suppressed, d damped, h history, * valid, > best, i - internal |             |        |        |      |
| Origin codes: i - IGP, e - EGP, ? - incomplete                                 |             |        |        |      |
| Network  | Next Hop    | Metric | LocPrf | Path |
| *> 172.16.20/24  | 172.16.20.1 |        |        | i    |
| *> 192.68.11/24  | 192.68.11.1 |        |        | i    |

# bgp show regexp

## Purpose

Displays the BGP routes matching the AS path regular expression.

## Format

**bgp show regexp** *<string>* **to-terminal|to-file**

## Mode

Enable.

## Description

The **bgp show regexp** command searches through all BGP routes that contain specified keywords belonging to an AS path. These specified keywords are the AS path regular expression upon which the search is executed. The character string can be a combination of AS numbers or names.

Some BGP character string shorthand conventions:

- . Matches any AS number
- \* Zero or more repetitions
- + One or more repetitions
- ? Zero or one repetition
- | Alternation
- () Parentheses group sub expressions

## Parameters

|                       |  |
|-----------------------|--|
| <i>&lt;string&gt;</i> | A character string that specifies the regular expression. Specify an As. |
| <b>to-terminal</b>    | Causes output to be displayed on the terminal. This is the default.      |
| <b>to-file</b>        | Causes output to be saved in the file /gatedtrc/gated.dmp.               |

## Restrictions

None.

## Example

To display the BGP routes starting with “64751”:

```
xp# bgp show regexp “64751 .*” to-terminal
BGP table : Local router ID is 192.68.11.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

  Network          Next Hop        Metric   LocPrf        Path
*> 193.226.64/22   134.141.178.33  64751    6379         1 1239 11331 8338 i
```



# bgp show routes

## Purpose

Displays entries in the BGP routing table.

## Format

**bgp show routes** *<ip-addr-mask>***|all** [**to-terminal**]**|to-file**]

## Mode

Enable.

## Description

The **bgp show routes** command displays the IP address/netmask, next hop, and AS path for each BGP route.

## Parameters

|                             |   |
|-----------------------------|---|
| <i>&lt;ip-addr-mask&gt;</i> | Displays information about the specified route.                     |
| <b>all</b>                  | Displays information about all routes.                              |
| <b>to-terminal</b>          | Causes output to be displayed on the terminal. This is the default. |
| <b>to-file</b>              | Causes output to be saved in the file /gatedtrc/gated.dmp.          |

## Restrictions

None.

## Example

To display the BGP routing table:

| xp# <b>bgp show routes all</b> |       |               |             |     |                                |
|--------------------------------|-------|---------------|-------------|-----|--------------------------------|
| RIB                            | Proto | Route/Mask    | NextHop     | MED | ASPath                         |
|                                | GP    | 172.16.70/24  | 172.16.20.2 |     | (64900) 64901 IGP (Id 2)       |
|                                | BGP   | 172.16.220/24 | 172.16.20.2 |     | (64900) 64901 IGP (Id 2)       |
|                                | BGP   | 192.68.20/24  | 172.16.20.2 |     | (64900) 64901 IGP (Id 2)       |
|                                | BGP   | 192.68.222/24 | 172.16.20.2 |     | (64900) 64901 64902 IGP (Id 3) |

# bgp show summary

## Purpose

Displays the status of all BGP connections.

## Format

**bgp show summary** [**to-terminal**|**to-file**]

## Mode

Enable.

## Description

The **bgp show summary** command displays the status of all BGP peers of the X-Pedition router.

## Parameters

|                    |   |
|--------------------|---|
| <b>to-terminal</b> | Causes output to be displayed on the terminal. This is the default. |
| <b>to-file</b>     | Causes output to be saved in the file /gatedtrc/gated.dmp.          |

## Restrictions

None.

## Example

To display the status of all BGP connections:

|                                |   |       |         |         |           |             |
|--------------------------------|---|-------|---------|---------|-----------|-------------|
| xp# <b>bgp show summary</b>    |   |       |         |         |           |             |
| Neighbor                       | V | AS    | MsgRcvd | MsgSent | Up/Down   | State       |
| 172.16.20.2                    | 4 | 64901 | 10033   | 10031   | 6d23h8m1s | Established |
| BGP summary, 1 groups, 1 peers |   |       |         |         |           |             |

# **bgp show sync-tree**

## **Purpose**

Displays the BGP synchronization tree.

## **Format**

**bgp show sync-tree**

## **Mode**

Enable.

## **Description**

The **bgp show sync-tree** command displays the BGP synchronization tree. The synchronization tree is used by IBGP peers to resolve the next hop (forwarding address). It gives information about routes that are orphaned because the next hop could not be resolved.

## **Parameters**

None.

## **Restrictions**

None.

## Examples

The following example shows the next hops for some of the routes that are not resolved (by showing orphaned routes):

```
xp# bgp show sync tree
Task BGP_Sync_64805:
  IGP Protocol: Any    BGP Group: group type Routing AS 64805

  Sync Tree (* == active, + == active with alternate, - ==
  inactive with alternate:
    Orphaned routes
      Forwarding address 172.23.1.18
        3/255 peer 172.23.1.26 preference 170
        128.36/255.255 peer 172.23.1.26 preference 170
        128.152/255.255 peer 172.23.1.26 preference 170
        129.200/255.255 peer 172.23.1.26 preference 170
        129.253/255.255 peer 172.23.1.26 preference 170
        130.44/255.255 peer 172.23.1.26 preference 170
        130.50/255.255 peer 172.23.1.26 preference 170
        130.132/255.255 peer 172.23.1.26 preference 170
        134.54/255.255 peer 172.23.1.26 preference 170
        134.120/255.255 peer 172.23.1.26 preference 170
        134.173/255.255 peer 172.23.1.26 preference 170
        134.217/255.255 peer 172.23.1.26 preference 170
        134.244/255.255 peer 172.23.1.26 preference 170
        136.1/255.255 peer 172.23.1.26 preference 170
        137.49/255.255 peer 172.23.1.26 preference 170
        137.159/255.255 peer 172.23.1.26 preference 170
        138.239/255.255 peer 172.23.1.26 preference 170
```

The following example shows the next hop for all the routes that are resolved:

```

xp# bgp show sync-tree
Task BGP_Sync_64805:
    IGP Protocol: Any    BGP Group: group type Routing AS 64805

    Sync Tree (* == active, + == active with alternate, - ==
inactive with alternate:
    Node 3/8388608 route 3/255 metric -1 next hops 172.23.1.6 172.23.1.22
    Node 4/8388608 route 4/255 metric -1 next hops 172.23.1.6 172.23.1.22
    Node 6/8388608 route 6/255 metric -1 next hops 172.23.1.6 172.23.1.22
    Node 9.2/32768 route 9.2/255.255 metric -1 next hops 172.23.1.6 172.23.1.22
    Node 9.20/16384 route 9.20/255.255.128 metric -1 next hops 172.23.1.6 172.23.1.22
    Node 10.12.1/2 route 10.12.1/255.255.255.252 metric 0 interface
    Node 10.12.1.4/2 route 10.12.1.4/255.255.255.252 metric 2 next hop 172.23.1.22
    Node 10.200.12/128 route 10.200.12/255.255.255 metric -1 next hops 172.23.1.6 172.23.1.22
    Node 10.203.12/128 route 10.203.12/255.255.255 metric -1 next hops 172.23.1.6 172.23.1.22
    Node 10.204.12/128 route 10.204.12/255.255.255 metric -1 next hops 172.23.1.6 172.23.1.22
    Node 12/8388608 route 12/255 metric -1 next hops 172.23.1.6 172.23.1.22
    Node 12.2.19/64 route 12.2.19/255.255.255.128 metric -1 next hops 172.23.1.6 172.23.1.22
    Node 12.2.97/128 route 12.2.97/255.255.255 metric -1 next hops 172.23.1.6 172.23.1.22
    Node 12.3.123/128 route 12.3.123/255.255.255 metric -1 next hops 172.23.1.6 172.23.1.22
    Node 12.4.5/128 route 12.4.5/255.255.255 metric -1 next hops 172.23.1.6 172.23.1.22
    Node 12.4.164/128 route 12.4.164/255.255.255 metric -1 next hops 172.23.1.6 172.23.1.22
    Node 12.5.164/128 route 12.5.164/255.255.255 metric -1 next hops 172.23.1.6 172.23.1.22
    Node 12.5.172/512 route 12.5.172/255.255.252 metric -1 next hops 172.23.1.6 172.23.1.22
    Node 12.5.252/256 route 12.5.252/255.255.254 metric -1 next hops 172.23.1.6 172.23.1.22

```

## **bgp start|stop**

### **Purpose**

Start or stop Border Gateway Protocol (BGP).

### **Format**

**bgp start|stop**

### **Mode**

Configure.

### **Description**

The **bgp start** command starts BGP on the X-Pedition router.

### **Parameters**

|              |             |
|--------------|-------------|
| <b>start</b> | Starts BGP. |
| <b>stop</b>  | Stops BGP.  |

### **Restrictions**

None.

# bgp trace

## Purpose

Set BGP trace options.

## Format

```
bgp trace packets [detail| send| receive| group <number-or-string>| peer-host <ipAddr>]|  
open [detail| send| receive| group <number-or-string>| peer-host <ipAddr>]|update [detail|  
send| receive| group <number-or-string>| peer-host <ipAddr>]| keep-alive [detail| send| receive|  
group <number-or-string>| peer-host <ipAddr>]|aspath [group <number-or-string>|  
peer-host <ipAddr>]| local-options [all| general| state| normal| policy| task| timer| route|  
group <number-or-string>| peer-host <ipAddr>]
```

## Mode

Configure.

## Description

The **bgp trace** command lets you set BGP trace options for the X-Pedition router.

## Parameters

|                |                                 |   |
|----------------|---------------------------------|---|
| <b>packets</b> | Traces all BGP packets.         |   |
|                | <b>detail</b>                   | Shows detailed information about the specified packets.   |
|                | <b>send</b>                     | Shows the specified packets sent by the router.   |
|                | <b>receive</b>                  | Shows the specified packets received by the router.   |
|                | <b>group</b> <number-or-string> | The ID of the group for which to enable tracing.  |
|                | <b>peer-host</b> <ipAddr>       | The peer-host IP address for which to enable tracing. The peer-host has to be qualified by the group to which it belongs. |

|                   |   |   |
|-------------------|---|---|
| <b>open</b>       | Traces BGP OPEN packets, which are used to establish a peer relationship.           |   |
|                   | <b>detail</b>   | Shows detailed information about the specified packets.   |
|                   | <b>send</b>   | Shows the specified packets sent by the router.   |
|                   | <b>receive</b>  | Shows the specified packets received by the router.   |
|                   | <b>group</b> <number-or-string>   | The ID of the group for which to enable tracing.  |
|                   | <b>peer-host</b> <ipAddr>   | The peer-host IP address for which to enable tracing. The peer-host has to be qualified by the group to which it belongs. |
| <b>update</b>     | Traces BGP update packets, which are used to pass network reachability information. |   |
|                   | <b>detail</b>   | Shows detailed information about the specified packets.   |
|                   | <b>send</b>   | Shows the specified packets sent by the router.   |
|                   | <b>receive</b>  | Shows the specified packets received by the router.   |
|                   | <b>group</b> <number-or-string>   | The ID of the group for which to enable tracing.  |
|                   | <b>peer-host</b> <ipAddr>   | The peer-host IP address for which to enable tracing. The peer-host has to be qualified by the group to which it belongs. |
| <b>keep-alive</b> | Traces BGP KEEPALIVE packets, which are used to verify reachability.                |   |
|                   | <b>detail</b>   | Shows detailed information about the specified packets.   |
|                   | <b>send</b>   | Shows the specified packets sent by the router.   |
|                   | <b>receive</b>  | Shows the specified packets received by the router.   |
|                   | <b>group</b> <number-or-string>   | The ID of the group for which to enable tracing.  |
|                   | <b>peer-host</b> <ipAddr>   | The peer-host IP address for which to enable tracing. The peer-host has to be qualified by the group to which it belongs. |



---

|                                 |   |
|---------------------------------|---|
| <b>aspath</b>                   | Traces aspath related events.   |
| <b>group</b> <number-or-string> | The ID of the group for which to enable tracing.  |
| <b>peer-host</b> <ipAddr>       | The peer-host IP address for which to enable tracing. The peer-host has to be qualified by the group to which it belongs. |
| <b>local-options</b>            | Sets trace options for this protocol only. You can specify the following:   |
| <b>all</b>                      | Traces all additions, changes, and deletions to the GateD routing table.  |
| <b>general</b>                  | Activates normal and route tracing.   |
| <b>state</b>                    | Traces state machine transitions in the protocol.   |
| <b>normal</b>                   | Traces normal protocol occurrences. (Abnormal protocol occurrences are always traced.)                                    |
| <b>policy</b>                   | Traces the application of protocol and user-specified policies to routes being imported and exported.                     |
| <b>task</b>                     | Traces system interface and processing associated with this protocol or peer.   |
| <b>timer</b>                    | Traces timer usage by this with this protocol or peer.  |
| <b>route</b>                    | Traces routing table changes for routes installed by this protocol or peer.   |
| <b>group</b> <number-or-string> | The ID of the group for which to enable tracing.  |
| <b>peer-host</b> <ipAddr>       | The peer-host IP address for which to enable tracing. The peer-host has to be qualified by the group to which it belongs. |

---

**Note:** If neither the group nor peer-host is specified, tracing is enabled for all groups and peers. If the group is specified and the peer-host is not specified, tracing is enabled for that group. If both the peer-host and group are specified, tracing is enabled for that peer-host in the specified group.

## Restrictions

None.



# Chapter 10

## cdp Commands

### Command Summary

[Table 10](#) lists the **cdp** commands. The sections following the table describe the command syntax.

**Table 10. cdp Commands**

|   |
|---|
| <b>cdp set global-status auto-enabled  enabled  disabled</b>  |
| <b>cdp set transmit-frequency</b> <i>&lt;number&gt;</i>   |
| <b>cdp set authentication-code</b> <i>&lt;string&gt;</i>  |
| <b>cdp set port-status port</b> <i>&lt;port-list&gt;</i>   <b>all-ports</b> autoenabled enabled  disabled |
| <b>cdp show neighbors</b> [detail]  |
| <b>cdp show global-info</b>   |
| <b>cdp show stats</b>   |
| <b>cdp show port-status port</b> <i>&lt;port-list&gt;</i>   <b>all-ports</b>                              |

# cdp set global-status

## Purpose

Set the global-status of all ports.

## Format

**cdp set global-status auto-enabled |enabled |disabled**

## Mode

Configure.

## Description

The **cdp set global-status** command allows you to set the global status of all ports to auto-enabled, enabled, or disabled. The default **global-status** is **disabled**, indicating that if a port receives a CDP packet, the X-Pedition router will **not** begin transmitting CDP hello packets from that port. This setting applies to all ports on the system. You can set individual ports differently by using [cdp set port-status on page 193](#). The port-status takes precedence over the global-status.

**Note:** Before you can run CDP, you must enable the *task* and the *ports* on which it will run.

## Parameters

None.

## Restrictions

The port-status takes precedence over the global-status.

## Example

Set the global-status to enabled:

```
xp(config)(cdp-set)# global-status enabled
```

# cdp set transmit-frequency

## Purpose

Set CDP hello packet transmission frequency.

## Format

**cdp set transmit-frequency** *<number>*

## Mode

Configure.

## Description

The **cdp set transmit-frequency** command specifies the amount of time (in seconds) between successive CDP hello packet transmissions.

**Note:** The X-Pedition router automatically sets the CDP *hold-time* to 3 times the transmission frequency. Hold-time refers to the amount of time to retain a neighbor entry after receiving the last hello packet.

## Parameters

---

|                       |  |
|-----------------------|--|
| <i>&lt;number&gt;</i> | Enter a transmit frequency of 5-300 (inclusive). |
|-----------------------|--|

---

## Restrictions

None.

## Example

Set the CDP hello packet transmission frequency to 50 seconds:

```
xp(config)(cdp-set)# transmit-frequency 50
```

# cdp set authentication-code

## Purpose

Sets authentication code for transmitted CDP packets.

## Format

**cdp set authentication-code** <string>

## Mode

Configure.

## Description

The **cdp set authentication-code** command allows you to set the authentication code for transmitted CDP packets. The authentication code (a string) has a maximum length of 16 bytes.

## Parameters

---

|                            |  |
|----------------------------|--|
| <b>authentication-code</b> | A character string whose maximum length is 16 bytes. |
|----------------------------|--|

---

<string>

## Restrictions

None.

## Example

Assign an authentication code for transmitted packets:

```
xp(config)(cdp-set)# authentication-code enterasys
```

# cdp set port-status

## Purpose

Set port status for an individual port.

## Format

**cdp set port-status status** [**auto-enable** | **enable** | **disable**] **port** <port-list> | **all-ports**

## Mode

Configure.

## Description

The default status is **disable**, indicating that if a port receives a CDP packet, the X-Pedition router will **not** transmit CDP hello packets from that port. This applies to all ports on the system. The **cdp set port-status** command allows you to override the global status set for the port. (See [cdp set global-status](#) on page 190.)

**Note:** Before you can run CDP, you must enable the *task* and the *ports* on which it will run.

## Parameters

|   |                    |  |
|---|--------------------|--|
| <b>status</b> [ <b>auto-enable</b>   <b>enable</b>   <b>disable</b> ] | <b>auto-enable</b> | Automatically sets the port status to <b>enable</b> upon receipt of a CDP packet.  |
|   | <b>enable</b>      | Enables the port to transmit CDP hello packets, whether or not the router receives a CDP packet.                                 |
|   | <b>disable</b>     | Prevents the port from transmitting CDP hello packets.   |
| <b>port</b> <port-list>   |                    | The port(s) you wish to autoenable, enable, or disable. You may use the keyword <b>all-ports</b> to set the status of all ports. |

## Restrictions

None.

## Example

The following example enables all the ports:

```
xp(config)(cdp-set)# port-status status enable port all-ports
```

# cdp show neighbors

## Purpose

Show CDP neighbors.

## Format

**cdp show neighbors [detail]**

## Mode

Enable.

## Description

The **cdp show neighbors** command displays the neighbor table which outlines which port the neighbor is seen on, information about the MAC address, IP address, neighbor's port that connects to your port, neighbor type, and capabilities.

## Parameters

---

|                 |  |
|-----------------|--|
| <b>[detail]</b> | Display more verbose information about the neighbor. |
|-----------------|--|

---

## Restrictions

None.



## Example

The following example shows the output of the **cdp show neighbors** command:

```
xp(cdp-show)# neighbors
```

Following are the CDP neighbors:

Type:

|     |   |                                |
|-----|---|--------------------------------|
| SF7 | Network Switch running Secure Fast version 1.7 or lower   |                                |
| SF8 | Network Switch running Secure Fast version 1.8 or greater |                                |
| ROU | Router  | BRG Bridge                     |
| VLM | Enterasys VLAN Manager                                    | NSR Network Server(NT)         |
| NWS | Network Workstation(NT)                                   | W95 Windows95                  |
| W98 | Windows98   | USR UNIX Server                |
| UWS | UNIX Workstation  | RWA RoamAbout wireless acc pnt |

Capabilities:

|    |                                |                           |
|----|--------------------------------|---------------------------|
| IG | IGMP enabled on sending port   |                           |
| RP | Uses RIP for routing           | BG Uses BGP for routing   |
| OS | Uses OSPF for routing          | DV Supports DVMRP         |
| 1Q | Has 802.1Q support             | GV Supports GVRP          |
| GM | Supports GMRP                  | IS Supports IGMP snooping |
| SB | Performs source route bridging |                           |
| TB | Performs transparent bridging  |                           |
| L1 | Performs Level 1 functionality |                           |

| Local Port | Neighbor MAC      | Neighbor IP    | Neighbor Port N | Type | Capabilities |
|------------|-------------------|----------------|-----------------|------|--------------|
| -----      | -----             | -----          | -----           | ---  | -----        |
| et.2.4     | 00:E0:63:68:5F:F1 | 10.136.136.104 | et.3.1          | ROU  | OS DV L1     |
| et.7.15    | 00:01:F4:09:F2:7B | 0.0.0.0        | et.1.1          | ROU  | OS DV L1     |
| et.13.24   | 00:E0:63:A2:38:6F | 10.136.136.204 | et.1.1          | ROU  | OS DV L1     |
| gi.12.8    | 00:E0:63:68:12:F1 | 10.136.136.202 | gi.5.1          | ROU  | OS DV L1     |

## **cdp show global-info**

### **Purpose**

Show CDP global information.

### **Format**

**cdp show global-info**

### **Mode**

Enable.

### **Description**

The **cdp show global-info** command displays the current global settings for transmit frequency, holdtime, CDP status (autoenabled, enabled, disabled), and authentication code.

### **Restrictions**

None.

### **Example**

The following example shows the output of the **cdp show global-info** command:

```
xp(cdp-show)# global-info

CDP Global Information:
  Transmit frequency is 60 seconds
  Holdtime is 180 seconds
  CDP status is Auto Enabled
  Authentication code is Default
```

# cdp show stats

## Purpose

Show CDP traffic.

## Format

**cdp show stats**

## Mode

Enable.

## Description

The **cdp show stats** command displays the total number of CDP packets sent and received. Also displayed are error statistics for packets received with an unsupported version of CDP, the number of packets that could not be parsed, packet transmission errors, number of memory errors, and number of packets received with invalid authentication code.

## Restrictions

None.

## Example

The following example shows the output of the **cdp show stats** command

```
xp(cdp-show)# stats
CDP statistics:
  Total number of CDP Packets sent           : 0
  Total number of valid CDP Packets received : 0
  Packets received with unsupported CDP Version : 0
  Number of CDP packets that could not be parsed : 0
  Packet transmission errors                 : 0
  Number of memory errors                    : 0
  Number of packets received with invalid auth code : 0
```

# cdp show port-status

## Purpose

Show status of selected ports.

## Format

**cdp show port-status port** *<port-list>* |**all-ports**

## Mode

Enable.

## Description

The **cdp show port-status** command displays the current status of a specific port(s) including packets sent and received, errors, current link state, and CDP status of port (autoenabled, enabled, or disabled).

## Parameters

---

|                                      |  |
|--------------------------------------|--|
| <b>port</b> <i>&lt;port-list&gt;</i> | The port(s) for which you will display the current status. You may enter a series of ports (et.1.3,et.(1,2).(4,6-8)) or enter the keyword <b>all-ports</b> to display the status of all ports. |
|--------------------------------------|--|

---

## Restrictions

None.

## Example

The following example shows the port status of various Ethernet ports:

```
xp(cdp-show)# port-status port et.1.3,et.(1,2).(4,6-8)
```

| Port   | Port Status  | Pkts Sent | Pkts Received | Errors | Link State | TRNK  |
|--------|--------------|-----------|---------------|--------|------------|-------|
| ----   | -----        | -----     | -----         | -----  | -----      | ----- |
| et.1.3 | Auto Enabled | 0         | 0             | 0      | Down       |       |
| et.1.4 | Auto Enabled | 0         | 0             | 0      | Down       |       |
| et.1.6 | Auto Enabled | 0         | 0             | 0      | Down       |       |
| et.1.7 | Auto Enabled | 0         | 0             | 0      | Down       |       |
| et.1.8 | Auto Enabled | 0         | 0             | 0      | Down       |       |
| et.2.4 | Auto Enabled | 0         | 0             | 0      | Down       |       |
| et.2.6 | Auto Enabled | 0         | 0             | 0      | Down       |       |
| et.2.7 | Auto Enabled | 0         | 0             | 0      | Down       |       |
| et.2.8 | Auto Enabled | 0         | 0             | 0      | Down       |       |



# Chapter 11

## cli Commands

The **cli** commands allow you to change the behavior of the CLI in terms of command completion and command history recall.

### Command Summary

[Table 11](#) lists the **cli** commands. The sections following the table describe the command syntax.

**Table 11. cli Commands**

|   |
|---|
| <b>cli search</b> <i>&lt;phrase&gt;</i> whole-phrase skip-keywords skip-help    |
| <b>cli set command completion</b> on off  |
| <b>cli set common</b>   |
| <b>cli set history size</b> <i>&lt;num&gt;</i>  default maxsize                 |
| <b>cli set terminal</b> [columns <i>&lt;num&gt;</i> ][rows <i>&lt;num&gt;</i> ] |
| <b>cli show history</b>   |
| <b>cli show terminal</b>  |
| <b>cli terminal monitor</b> on off  |

# cli search command

## Purpose

Allow users to search for any ASCII string in the CLI command set.

## Format

**cli search** *<phrase>* **whole-phrase**| **skip-keywords**| **skip-help**

## Mode

Login and Enable modes.

## Description

The **cli search** command lets you search through the CLI commands and help text to find a specific text string. The text string can be a few characters, a single word, or a phrase. The command displays where the text string was found. The command displays one information line for each instance of the text string found in the CLI. If no instances of the text string were found, the command prompt returns immediately after displaying the legend.

## Parameters

|                       |  |
|-----------------------|--|
| <i>&lt;phrase&gt;</i> | The text string you wish to search for. It can contain up to 255 ASCII characters, including spaces. If spaces are used, the phrase must be enclosed by quotes.  |
| <b>whole-phrase</b>   | Limits the search to instances where the whole phrase exists. For example, searching for “hat” will also find words that contain these letters, such as “that.” With <b>whole-phrase</b> , the utility displays a list of only those instances where the phrase “hat” exists as a separate word. |
| <b>skip-keywords</b>  | Prevents the utility from searching for <i>&lt;phrase&gt;</i> in the keyword-list associated with objects or options.  |
| <b>skip-help</b>      | Prevents the utility from searching the help strings for <i>&lt;phrase&gt;</i> . In the example, the second instance would not be displayed if this option is used.  |

## Restrictions

None.



## Example

The following example searches the CLI for the phrase, “rows:”

```

xp# cli search rows
Searching Command Line Interface for "rows"...
CLI Mode Legend:
=====
L-->Login; E-->Enable; C-->Config 0-->Other (ACL Edit, ARE-Config); ?-->Unknown
M   Found In           For           Command Structure
=   =====           =====           =====
L   Option              Option        cli-->set-->terminal-->rows
C   Help                Object          snmp-->set-->retro-mib-ifspeed
C   Option              Option          system-->set-->terminal-->rows

```

The utility found three (3) instances of “rows” in the CLI. The first instance was:

L Option    Option    cli-->set-->terminal-->rows

The <phrase>, “rows,” exists as an option in the command, **cli set terminal**. The complete command is **cli set terminal rows** and the command can be executed in Login mode (which means it is also accessible in Enable mode).

The second instance was:

C Help      Object    snmp-->set-->retro-mib-ifspeed

The <phrase>, “rows,” exists in the Help string for the Object in the command, **snmp set retro-mib-if-speed**. The command can be executed in config mode. Entering **snmp set ?** in config mode would display the help strings for each of the objects. One of the displays would include “rows” as follows:

retro-mib-ifspeed - ifSpeed for IP Interface rows will return speed of first operational port

The final instance was:

C Option    Option    system-->set-->terminal-->rows

This instance is like the first instance except that the command must be executed from configuration mode. Also, the phrase shows up as an option in the command instead of an object, and the command structure is different.

## Field Definitions

| Field             | Description   |
|-------------------|---|
| M                 | <p>Informs what CLI Mode the user must be in to issue the command. A single letter represents each mode:</p> <p>L = Login Mode</p> <p>E = Enable Mode</p> <p>C = Configuration Mode</p> <p>O = Other Mode (ACL editor, ARE-Config or others)</p> <p>? = Unknown (mode cannot be determined)</p>   |
| Found In          | Displays which element of the CLI command contained <i>&lt;phrase&gt;</i> . This option includes Facility, Command, Object, Option, Keyword, and Help.  |
| For               | Displays which CLI Element that is part of the actual command contains <i>&lt;phrase&gt;</i> . It differs from the Found In section in that this section is actually part of the command. For example: <i>&lt;phrase&gt;</i> may have been found in the Help String for the command's object. If so, the previous section would report "Help" and this section would report "Object". If <i>&lt;phrase&gt;</i> was associated with the object itself then this section and the Found In section would report "Object". Valid entries include: Facility, Command, Object and Option. |
| Command Structure | Shows the command structure and indicates how to enter the command from the CLI. An arrow (-->) separates each command element (e.g., the command cli set terminal would appear as cli-->set-->terminal).   |

# cli set command completion

## Purpose

Turn on or off command completion support.

## Format

**cli set command completion on|off**

## Mode

User and Configure.

## Description

The **cli set command completion** command lets you enable or disable command completion support. This command works in both User and Configure mode. When executed in Configure mode, it turns on or off command completion support for the entire system. When executed in User mode, the command affects only the current login session of the user issuing that command.

## Parameters

|            |                              |
|------------|------------------------------|
| <b>on</b>  | Turn on command completion.  |
| <b>off</b> | Turn off command completion. |

## Restrictions

None.

## **cli set common**

### **Purpose**

Switch to the Common CLI mode.

### **Format**

**cli set common**

### **Mode**

Enable.

### **Description**

The **cli set common** command changes the CLI environment from the Native to the Common CLI. When executed in Enable mode, this command configures the system's CLI to use the Common CLI commands and attributes. All users currently logged in and all subsequent users will switch to the Common CLI.

**Note:** To toggle between Common mode and Native mode, enter the **terminal set ssr** command.

### **Parameters**

None.

### **Restrictions**

None.

# cli set history

## Purpose

Modify command history recall characteristics.

## Format

**cli set history size** <num>|default|maxsize

## Mode

User and Configure.

## Description

The **cli set history** command lets you to set the size of the command history buffer. Each command stored in this buffer can be recalled without having the user type in the same, complete command again. By setting the size of this history buffer, one tells the router how many of the most recently executed commands should be stored. When the buffer is full, the oldest command is pushed out to make space for the newest command. The **cli set history** command works in both User and Configure mode. When executed in Configure mode, it sets the history size of the entire system. When executed in User mode, the command affects only the current login session of the user issuing that command.

## Parameters

|                |  |
|----------------|--|
| <num>          | Specifies how many of the most recently executed commands should be kept. To disable history support, specify a size of 0. |
| <b>default</b> | Sets the history size to the system default.   |
| <b>maxsize</b> | Sets the history size to the system maximum.   |

## Restrictions

None.

## Example

To set the history buffer size to 100 commands:

```
xp# cli set history size 100
```

# cli set terminal

## Purpose

Modify current session's terminal settings.

## Format

**cli set terminal** [**columns** <num>] [**rows** <num>]

## Mode

User.

## Description

The **cli set terminal** command lets you modify the terminal screen size of the current session. Specifying the number of rows available on your terminal causes the system to automatically pause when screen output fills the entire screen.

## Parameters

|                |   |
|----------------|---|
| <b>columns</b> | Number of columns for your terminal. Minimum acceptable value is 20.  |
| <b>rows</b>    | Number of rows for your terminal. The default row size is 25. To prevent output from pausing after one screen full, set the value to 0.<br><br>Row and column settings must match the client-side terminal settings. If these settings differ, screen output may not format correctly. This is especially notable when displaying multiple pages of output. |

## Restrictions

None.

## Example

To set the number of rows to 50 lines:

```
xp# cli set terminal rows 50
```

# cli show history

## Purpose

Display the command history from the current CLI session.

## Format

**cli show history**

## Mode

User.

## Description

The **cli show history** command shows the commands you have issued during the current CLI session. A number is associated with each command. A command's number is useful for re-entering, modifying, or negating the command.

**Note:** You also can perform a command history recall by entering **!\*** at any command prompt.

## Parameters

None.

## Restrictions

None.

# **cli show terminal**

## **Purpose**

Display information about the current terminal settings.

## **Format**

**cli show terminal**

## **Mode**

User.

## **Description**

The **cli show terminal** command shows information about the terminal settings. The terminal settings affect the display characteristics of your CLI session.

## **Parameters**

None.

## **Restrictions**

None.



# cli terminal monitor

## Purpose

Allows the current CLI session to receive or not receive console output.

## Format

**cli terminal monitor on|off**

## Mode

Enable.

## Description

The X-Pedition router normally sends some system, diagnostic, and tracing messages to the management console only. The **cli terminal monitor** command allows users to configure the current Telnet or SSH CLI session to receive these messages as well.

**Note:** Enabling the CLI terminal monitor will not display ACL logging messages in Telnet or SSH sessions. This prevents potential session flooding with repeat ACL logging messages.

## Parameters

|            |                                     |
|------------|-------------------------------------|
| <b>on</b>  | Turn on receipt of console output.  |
| <b>off</b> | Turn off receipt of console output. |

## Restrictions

None.



# Chapter 12

## comment Commands

The **comment** commands allow users to add user-defined comment lines to the active configuration file and are often used to log configuration changes and additions. To remove a line of comments, use the **negate** *<numrange>* command. The X-Pedition router does not require the use of the **save active** command in conjunction with comment commands.

### Command Summary

[Table 12](#) lists the **comment** commands. The sections following the table describe the command syntax.

**Table 12. comment Commands**

|  |
|--|
| <b>comment in</b> <i>&lt;num&gt;</i>                         |
| <b>comment line</b> <i>&lt;num&gt;</i> <i>&lt;string&gt;</i> |
| <b>comment move</b> <i>&lt;num&gt;</i>                       |
| <b>comment out</b> <i>&lt;num&gt;</i>                        |

**Note:** The comment commands take effect *immediately*—they do not require the **save active** command to activate them.

## comment in

### Purpose

Reactivates a command in the active configuration file.

### Format

**comment in** <num>

### Mode

Configure.

### Description

The **comment in** command allows you to reactivate a command that you previously negated using the **comment out** command. This is done by specifying the line number for the negated command or commands in the active configuration file.

**Note:** When you use the **comment out** command to disable an **snmp set user** command, the X-Pedition router will delete the passwords for that user. If you attempt to reactivate the command through the **comment in** command, the **snmp set user** command will fail and you will need to re-enter the command and create a new account for the user. To disable users and prevent them from accessing the router through SNMP, **comment out** the user's corresponding **snmp set user-to-group** command. This will prevent you from having to recreate user accounts.

**Note:** The comment commands take effect *immediately*—they do not require the **save active** command to activate them. Because these commands directly modify the active configuration, use caution when commenting commands into the active configuration that are dependent upon other commands.

### Parameters

---

|       |   |
|-------|---|
| <num> | Specifies the line number or numbers from the active configuration file that corresponds to the command you wish to reactivate. |
|-------|---|

---

### Restrictions

You may **comment in** only those commands that were previously commented out.

## Example

To reactivate line 10 in the active configuration file:

```
xp# comment in 10
```

## comment line

### Purpose

Adds a comment line to the active configuration file.

### Format

**comment line** <num> <string>

### Mode

Configure.

### Description

The **comment line** command allows you to add a comment line to the active configuration file. This comment line will be added directly above the command(s) that is currently occupying the line number(s). Comment lines are denoted with a “C” following the line number, and a “!!” directly before the actual line of comments.

**Note:** The comment commands take effect *immediately*—they do not require the **save active** command to activate them.

### Parameters

|          |   |
|----------|---|
| <num>    | Specifies the line number or numbers to which you wish to add a comment line.                 |
| <string> | Specifies the comment line character string. Enclose the character string in quotation marks. |

### Restrictions

The character string must be enclosed in quotation marks.

## Example

To add the comment “this is an ethernet port” to line 10 only, enter the following:

```
xp# comment line 10 “this is an ethernet port”
10C: !!this is an ethernet port
11:  interface create ip ether1 address-netmask 10.1.1.2/24 port et.4.1
```

A new line containing the comment is inserted at line 10.

To add the comment “ethernet port” to multiple lines (10-12):

```
xp(config)# comment line 10-12 “ethernet port”
10C: !!ethernet port
11:  interface create ip ether1 address-netmask 10.1.1.2/24 port et.4.1
    !
12C: !!ethernet port
13:  interface create ip ether2 address-netmask 20.1.1.2/24 port et.4.2
    !
14C: !!ethernet port
15:  interface create ip ether3 address-netmask 30.1.1.2/24 port et.4.3
```

**Note:** The **interface create** commands previously occupied lines 10, 11, and 12. With the comments added, these commands now occupy 11, 13, and 15.

## comment move

### Purpose

Moves a comment line from one line number to another line number in the active configuration file.

### Format

**comment move** <num>

### Mode

Configure.

### Description

The **comment move** command allows you to move a comment line or range of comment lines from one line number to another line number within the active configuration file.

**Note:** The comment commands take effect *immediately*—they do not require the **save active** command to activate them.

### Parameters

---

|       |  |
|-------|--|
| <num> | Specify the current line number(s) before the comma, and specify the new line number(s) after the comma. The format is as follows:<br><current line number(s), new line number(s)> |
|-------|--|

---

### Restrictions

Do not attempt to move actual commands. When moving a range of comment lines, the line number ranges must be the same size.

### Example

To move the comments in lines 1-2 to lines 7-8:

```
xp# comment move 1-2,7-8
```



# comment out

## Purpose

Negates a command in the active configuration file, leaving the command as a comment.

## Format

**comment out** <num>

## Mode

Configure.

## Description

The **comment out** command allows you to negate a command or set of commands and leave them as a comment in the active configuration file. This is done by specifying the line number of the command or commands that you wish to negate from active configuration. The command will then be left in the active configuration file as a comment.

**Note:** When you use the **comment out** command to disable an **snmp set user** command, the X-Pedition router will delete the passwords for that user. If you attempt to reactivate the command through the **comment in** command, the **snmp set user** command will fail and you will need to re-enter the command and create a new account for the user. To disable users and prevent them from accessing the router through SNMP, **comment out** the user's corresponding **snmp set user-to-group** command. This will prevent you from having to recreate user accounts.

**Note:** The comment commands take effect *immediately*—they do not require the **save active** command to activate them. Because these commands directly modify the active configuration, use caution when commenting commands out of the active configuration that are dependent upon other commands.

## Parameters

---

|       |   |
|-------|---|
| <num> | Specifies the line number or numbers from the active configuration file that corresponds to the command you wish to negate. |
|-------|---|

---

## Restrictions

None.

## Example

To negate command #10 in the active configuration file:

```
xp# comment out 10
```

# Chapter 13

## configure Command

The **configure** command exits Enable mode and places the CLI session in Configure mode. From Configure mode, users may set and change X-Pedition parameters.

### Purpose

Enters the CLI's Configure mode.

### Format

**configure**

### Mode

Enable.

### Description

Configure mode provides the capabilities to configure all features and functions on the X-Pedition router. These include router configuration, access control lists and spanning tree. To enter Configure mode, enter the command **config** from Enable mode.

**Note:** Up to four Telnet sessions can be run simultaneously on the X-Pedition router. All four sessions can be in Configure mode at the same time, so you should consider limiting access to the router to authorized users.

The Configure mode command prompt consists of the X-Pedition name followed by **(config)** and a pound sign (#):

|             |
|-------------|
| xp(config)# |
|-------------|

---

To exit Configure mode and return to Enable mode, either type **exit** and press Return, or press Ctrl+Z.

## Parameters

None.

## Restrictions

To enter Configure mode, you must already be in Enable mode.

# Chapter 14

## copy Command

### Format

**copy** {active|rcp-server|scratchpad|startup|tftp-server|<[device:]filename>|<url>} to {active|backup-CM|ethers|rcp-server|scratchpad|startup|tftp-server|<[device:]fileame>|<url>}

### Mode

Enable.

### Description

The **copy** command is used primarily to transfer configuration information—to copy non-configuration files, users should generally employ the **file copy** command. Users can copy configuration information between the X-Pedition router and external hosts using protocols such as TFTP or RCP. Within the X-Pedition router, users can copy configuration information between the file system, the scratchpad (configuration database), the active (running) configuration, or the Startup configuration. If the X-Pedition router is operating in a dual-CM environment, users may copy the startup configuration of the primary Control Module to the secondary Control Module. The **copy** command also allows users to make backup copies of a configuration file.

**Note:** When copying an external file that contains configuration commands, each command must exist on a single line. If a command breaks over multiple lines, the X-Pedition router will read each line as a separate entry and an error will occur.

| Multi-line command   | Result                                  |
|--|---|
| <b>system set login-banner</b><br>“This is the login banner” | <b>system set login-banner</b> “This is |

---

## Parameters

|                                   |  |
|-----------------------------------|--|
| <b>active</b>                     | Copy information to the active configuration database (the system configuration currently running). Users may copy information into the active configuration from the scratchpad only.   |
| <b>backup-CM</b>                  | Copy the startup configuration from the Primary control module to the Backup control module. A user may specify the <b>backup-CM</b> parameter only as the destination—and only with <b>startup</b> as the source. (The <b>save startup</b> and <b>copy &lt;source_parameter&gt; to startup</b> commands automatically copy the Primary control module's startup configuration to the Backup Control Module.)  |
| <b>ethers</b>                     | The file located on the PCMCIA card that contains IP/MAC address pairings for reverse ARP queries. Each line within the <b>ethers</b> file contains a MAC address and IP address pair. The MAC address and IP address must be in the same format as they would appear on a CLI command (e.g., "00:0d:12:34:56:78 10.136.4.9"). The ethers destination parameter is used only with the <b>tftp-server</b> or the <b>tftp type &lt;url&gt;</b> source parameters.  |
| <b>rcp-server</b>                 | Downloads a file from or uploads a file to an RCP server.  |
| <b>scratchpad</b>                 | Copy configuration changes from the scratchpad.  |
| <b>startup</b>                    | Copies the Startup configuration information stored in the control module's NVRAM.   |
| <b>tftp-server</b>                | Downloads a file from or uploads a file to a TFTP server.  |
| <b>&lt;[device:] filename&gt;</b> | <p>Represented in the CLI help as a character string, this parameter specifies the name of a file on the X-Pedition local file system (NVRAM or PCMCIA Flash Module). The <i>device:</i> is optional and may be one of the following:</p> <p><b>bootflash:</b> The Control Module's NVRAM.</p> <p><b>slot0:</b> The PCMCIA Flash Module in slot 0 (the upper slot).</p> <p><b>Note:</b> The X-Pedition router supports PCMCIA Flash Modules obtained from Enterasys Networks only. For information regarding the PCMCIA Virtual File systems VFS1 and VFS2, see the <i>Enterasys X-Pedition User Reference Manual</i>.</p> |

---

|                          |   |
|--------------------------|---|
| <code>&lt;url&gt;</code> | Specify a <b>tftp</b> or <b>rcp</b> URL:<br><br><b>tftp</b> ://<hostname>/<path><br><br><b>rcp</b> ://<username>@<hostname>/<path><br><br><b>Note:</b> Because a URL refers to an absolute path, you must include a backslash within the path name for both the <b>tftp</b> and <b>rcp</b> URLs, as well as between the hostname and path.<br><br><b>Note:</b> Attention UNIX Users. In order to specify a tftp URL, you must first create the file on the tftp server using the same filename you will to use for the copy command. You must also make certain that all permissions for the file and any directories within its path are world writable. |
|--------------------------|---|

---

## Restrictions

- The X-Pedition router does not allow some source and destination pair combinations. Typically, users cannot specify the same location type for both source and destination (i.e., a user may not copy from one TFTP server directly to another TFTP server, or copy from scratchpad to scratchpad).
- Users may copy information into the active configuration (the system configuration currently running) from the scratchpad only.
- A user may specify the **backup-CM** parameter only as the destination—and only with **startup** as the source.
- The router supports PCMCIA Flash Modules obtained from Enterasys Networks only.
- Because a URL refers to an absolute path, you must include a backslash within the path name for both the **tftp** and **rcp** URLs, as well as between the hostname and path.

The following chart displays valid source and destination combinations:

**Table 13. Valid Source and Destination Parameters for the Copy command**

| Source              | Destination   |
|---------------------|---|
| <b>active</b>       | <b>rcp-server</b>   <b>startup</b>   <b>tftp-server</b>   <[device:]filename>   <url>                       |
| <b>rcp-server</b>   | <b>scratchpad</b>   <b>startup</b>   <[device:]filename>  |
| <b>scratchpad</b>   | <b>active</b>   <b>rcp-server</b>   <b>startup</b>   <b>tftp-server</b>   <[device:]filename>   <url>       |
| <b>startup</b>      | <b>backup-CM</b>   <b>rcp-server</b>   <b>scratchpad</b>   <b>tftp-server</b>   <[device:]filename>   <url> |
| <b>tftp-server</b>  | <b>ethers</b>   <b>scratchpad</b>   <b>startup</b>   <[device:]filename>                                    |
| <[device:]filename> | <b>rcp-server</b>   <b>scratchpad</b>   <b>startup</b>   <b>tftp-server</b>   <[device:]filename>   <url>   |
| <url>               | <b>scratchpad</b>   <b>startup</b>   <[device:]filename>  |

---

## Examples

To copy configuration information from the scratchpad to the active database (causing changes to take immediate effect), enter the following command from the CLI.

```
xp# copy scratchpad to active
```

To copy the file **config.john** to the PCMCIA card, slot0:config.debi:.

```
xp# copy config.john to slot0:config.debi
```

To copy the Startup configuration to a TFTP server for backup purposes, enter the following command. The CLI will then prompt the user for the TFTP server's IP address or hostname and the filename:

```
xp# copy startup to tftp-server
TFTP server? 10.136.11.1
Destination filename? my_startup.cfg
```

To copy a previously saved configuration from a TFTP server to the Startup configuration, enter the following command. Note the use of a URL to specify the TFTP server and the filename.

```
xp# copy tftp://10.1.2.3/backup/config.org to startup
```

To copy the active configuration to a remote server using RCP, enter the following command. Note that this example uses a URL to specify the RCP user name, server, and filename.

```
xp# copy active to rcp://john@server1/config/config.dec25
```

To copy the startup configuration from the Primary control module to the Backup control module:

```
xp# copy startup to backup-CM
```



# Chapter 15

## dhcp Commands

The **dhcp** commands allow you to configure *scopes* (sets of IP address pools and network parameters) that are to be used by Dynamic Host Configuration Protocol (DHCP) clients and apply them to interfaces on the X-Pedition router.

### Command Summary

[Table 14](#) lists the **dhcp** commands. The sections following the table describe the command syntax.

**Table 14. dhcp Commands**

|   |
|---|
| <b>dhcp</b> <scope> <b>attach superscope</b> <superscope>   |
| <b>dhcp</b> <scope> <b>define parameters</b> <parameter> <value>  |
| <b>dhcp</b> <scope> <b>define pool</b> <ip-range>   |
| <b>dhcp</b> <scope> <b>define static-ip</b> <ipaddr> <b>mac-address</b> <macaddr> [<parameter> <value>] |
| <b>dhcp flush</b>   |
| <b>dhcp global set commit-interval</b> <hours>  |
| <b>dhcp global set lease-database</b> <url>   |
| <b>dhcp show binding</b> [active  expired  static] <ipaddr>]  |
| <b>dhcp show num-clients</b>  |

# dhcp attach superscope

## Purpose

Creates a group of scopes that share a common interface.

## Format

**dhcp** <scope> **attach superscope** <superscope>

## Mode

Configure.

## Description

The **dhcp attach superscope** command allows you to create a “superscope,” a group of scopes that share a common physical interface. For example, you can define and group together scopes for different subnets that are accessed through a single port or VLAN.

## Parameters

|              |  |
|--------------|--|
| <scope>      | The name of a scope that was previously configured with the <b>dhcp define</b> commands. |
| <superscope> | The name of the group to which the specified scope is being attached.                    |

## Restrictions

None.

## Examples

Consider the following example where the scopes ‘client1’ and ‘client2’ exist on the same interface. To group scopes ‘client1’ and ‘client2’ into the superscope ‘allclients’:

```
xp(config)# dhcp client1 attach superscope allclients
xp(config)# dhcp client2 attach superscope allclients
```

# dhcp define parameters

## Purpose

Define parameters to be used by DHCP clients.

## Format

**dhcp** *<scope>* **define parameters** *<parameter>* *<value>...*

## Mode

Configure.

## Description

The **dhcp define parameters** command allows you to define a set of parameters that are to be used by clients when DHCP is enabled. The client uses these parameters to configure its network environment, for example, the default gateway and DNS domain name. The DHCP server on the X-Pedition router supports parameters used by Windows 95/98/NT and MacOS clients.

## Parameters

---

|                      |  |
|----------------------|--|
| <i>&lt;scope&gt;</i> | The name that refers to this set of client parameters. |
|----------------------|--|

---

|  |  |
|--|--|
| <code>&lt;parameter&gt; &lt;value&gt;</code> | Specify one or more of the following client parameters and values:   |
| <b>address-mask</b>                          | (Required) Specifies the address and netmask of the scope's subnet.  |
| <b>Note:</b>                                 | The <b>address-mask</b> parameter is <i>required</i> and must be defined <i>before</i> any other client parameters are specified.  |
| <b>broadcast</b>                             | Specify the broadcast address.   |
| <b>bootfile</b>                              | Specify the client's boot filename.  |
| <b>dns-domain</b>                            | Specify the DNS domain name.   |
| <b>dns-server</b>                            | Specify the IP address of the DNS server.  |
| <b>gateway</b>                               | Specify the IP address of the default gateway.   |
| <b>lease-time</b>                            | Specify how long, in hours, the lease is valid. (A lease is the amount of time that an assigned IP address is valid for a client system.)  |
| <b>lease-time-in-minutes</b>                 | Specify how long (in minutes) the lease will remain valid.   |
| <b>netbios-name-server</b>                   | Specify the IP address of the NetBIOS name server or WINS server.  |
| <b>netbios-node-type</b>                     | Specify the NetBIOS node type of the client.   |
| <b>netbios-scope</b>                         | Specify the NetBIOS scope of the client.   |
| <b>authoritative</b>                         | Causes the router to send DHCPNAK messages if the IP address specified by a DHCP request is not valid. If you do not select this option, the router will not send a DHCPNAK message. |

## Restrictions

None.

## Examples

The following command configures a group of network parameters for the scope 'finance':

```
xp(config)# dhcp finance define parameters address-netmask 10.33.0.0/16 dns-server 10.3.2.1 dns-domain acme.com gateway 10.33.1.1 netbios-node-type b-node lease-time 90 netbios-name-server 10.33.44.55 netbios-scope acme-finance
```

# dhcp define pool

## Purpose

Define a pool of IP addresses to be used by DHCP clients.

## Format

**dhcp** <scope> **define pool** <ip-range>

## Mode

Configure.

## Description

The **dhcp define pool** command allows you to define a pool of IP addresses that can be used by DHCP clients. An IP address pool, along with a set of parameters defined with the **dhcp define parameters** command, make up a DHCP “scope”.

## Parameters

|            |   |
|------------|---|
| <scope>    | A name that refers to the specified pool of addresses.  |
| <ip-range> | The range of IP addresses to be used by the clients. Use a hyphen (-) to designate the range. If you have more than one pool of IP addresses to specify or if the addresses are not contiguous, specify additional addresses using multiple <b>dhcp define pool</b> commands. |

## Restrictions

None.

## Examples

To specify the addresses between 10.1.1.1 to 10.1.1.20 as the pool of IP addresses for the scope ‘clients’:

```
xp(config)# dhcp clients define pool 10.1.1.1-10.1.1.20
```

To specify two separate pools of IP addresses for the scope 'clients':

```
xp(config)# dhcp clients define pool 10.1.1.1-10.1.1.20  
xp(config)# dhcp clients define pool 10.1.1.30-10.1.1.40
```

# dhcp define static-ip

## Purpose

Define a static IP address for a specific MAC address.

## Format

```
dhcp <scope> define static-ip <ipAddr> mac-address <macAddr> [<parameter> <value>...]
```

## Mode

Configure.

## Description

The **dhcp define static-ip** command allows you to configure a static IP address for a specific MAC address. For example, you can define a static IP address for a printer's MAC address to ensure that the printer always receives the same IP address from the DHCP server. Static IP addresses can be used for BOOTP clients as well as DHCP clients.

If you want a single MAC address to have different static IP addresses, depending upon which subnet or interface the machine is on, you can configure different scopes with different IP addresses that map to the same MAC address.

A client configured for a static IP address inherits the client parameters that are configured for the scope. If you want to configure a specific group of parameters for a static IP address, specify those parameters with the **dhcp define static-ip** command.

## Parameters

|           |   |
|-----------|---|
| <scope>   | A name that refers to the specified static IP address.                    |
| <ipAddr>  | The static IP address.  |
| <macAddr> | The MAC address to which the specified static IP address is to be mapped. |

|  |   |
|--|---|
| <b>&lt;parameter&gt; &lt;value&gt;</b> | Specifies the client parameters and values for this static IP address. You can specify one or more of the following client parameters and values: |
| <b>broadcast</b>                       | Specify the broadcast address.  |
| <b>bootfile</b>                        | Specify the client's boot filename.   |
| <b>dns-domain</b>                      | Specify the DNS domain name.  |
| <b>dns-server</b>                      | Specify the IP address of the DNS server.   |
| <b>gateway</b>                         | Specify the IP address of the default gateway.  |
| <b>lease-time</b>                      | Specify how long, in minutes, the lease is valid. (A lease is the amount of time that an assigned IP address is valid for a client system.)       |
| <b>netbios-name-server</b>             | Specify the IP address of the NetBIOS name server or WINS server.   |
| <b>netbios-node-type</b>               | Specify the NetBIOS node type of the client.  |
| <b>netbios-scope</b>                   | Specify the NetBIOS scope of the client.  |

## Restrictions

None.

## Examples

To specify a static IP address 10.1.44.55 to the MAC address 08:00:20:12:34:56 for the scope 'servers':

```
xp(config)# dhcp servers define static-ip 10.1.44.55 mac-address 08:00:20:12:34:56
```

To specify a static IP address 10.1.44.55 to the MAC address 08:00:20:12:34:56 for the scope 'servers' and give it a specific default gateway address:

```
xp(config)# dhcp servers define static-ip 10.1.44.55 mac-address 08:00:20:12:34:56 gateway 10.1.1.2
```

To define two different scopes ('public' and 'private') with two different static IP addresses (10.1.44.55 and 10.2.10.23) that map to the MAC address 08:00:20:12:34:56:

```
xp(config)# dhcp public define static-ip 10.1.44.55 mac-address 08:00:20:12:34:56
xp(config)# dhcp private define static-ip 10.2.10.23 mac-address 08:00:20:12:34:56
```



# dhcp flush

## Purpose

Forces the DHCP server to update its lease database.

## Format

**dhcp flush**

## Mode

Enable.

## Description

The DHCP server normally updates its lease database at the intervals specified with the **dhcp global set commit-interval** command. While the DHCP server is running, you can force the server to immediately update its lease database by using the **dhcp flush** command.

## Parameters

None.

## Restrictions

None.

# dhcp global set commit-interval

## Purpose

Configure the intervals at which the DHCP server updates the lease database.

## Format

**dhcp global set commit-interval** <minutes>

## Mode

Configure.

## Description

After each client transaction, the DHCP server does not immediately update the information in the lease database. Lease update information is stored in flash memory and flushed to the database at certain intervals. You can use the **dhcp global set commit-interval** command to specify this interval.

**Note:** Writing to flash memory can be time-consuming if there are many clients on the network.

## Parameters

|                                   |  |
|-----------------------------------|--|
| <b>commit-interval</b><br><hours> | The interval, in hours, that the DHCP server updates the lease database.<br>The default value is 1 hour. You can specify a value between 1-48. |
|-----------------------------------|--|

## Restrictions

None.

## Example

To configure the DHCP server to update the lease database once every 2 hours:

```
xp(config)# dhcp global set commit-interval 2
```

# dhcp global set lease-database

## Purpose

Specify a TFTP or RCP server where the lease database is backed up.

## Format

**dhcp global set lease-database** <url>

## Mode

Configure.

## Description

By default, the X-Pedition router stores the clients' lease information (the lease database) in its flash memory. You can use the **dhcp global set lease-database** command to specify a TFTP or RCP server where the lease database is to be periodically backed up.

## Parameters

---

|                             |   |
|-----------------------------|---|
| <b>lease-database</b> <url> | The TFTP or RCP server where the lease-database is to be backed up. |
|-----------------------------|---|

---

## Restrictions

None.

## Examples

To configure the lease database to be on a TFTP server (10.50.89.88) with the file name 'lease-db':

```
xp(config)# dhcp global set lease-database tftp://10.50.89.88/lease-db
```

To configure the lease database to be on an RCP server (10.50.89.89) with the user name 'john' and the file name 'lease-db':

```
xp(config)# dhcp global set lease-database rcpx://john@10.50.89.89/lease-db
```

# dhcp show binding

## Purpose

Display information from the lease database.

## Format

**dhcp show binding** [**active**| **expired**| **static**| <ipAddr>]

## Mode

Enable.

## Description

The **dhcp show** command displays information from the lease database. If you do not specify any parameters, the DHCP server displays the entire lease database.

## Parameters

|                |   |
|----------------|---|
| <b>active</b>  | Displays currently active leases only.                                  |
| <b>expired</b> | Displays expired leases only.   |
| <b>static</b>  | Displays leases with static IP address assignments only.                |
| <ipAddr>       | IP address. Will display only the binding for the specified IP address. |

## Restrictions

None.

## Example

To display information from the lease database:

| xp# <b>dhcp show binding</b> |                   |                     |         |
|------------------------------|-------------------|---------------------|---------|
| IP address                   | Hardware Address  | Lease Expiration    | Type    |
| -----                        | -----             | -----               | -----   |
| 10.20.1.22                   | 00:40:05:41:f1:2d | 2003-05-24 17:45:06 | dynamic |
| 10.20.1.23                   | 00:00:b4:b1:29:9c | 2003-05-24 17:45:04 | dynamic |
| 10.20.1.21                   | 00:00:b4:b0:f4:83 | 2003-05-24 17:45:01 | dynamic |
| 10.20.1.20                   | 00:80:c8:e1:20:8a | 2003-05-24 09:24:30 | dynamic |
| 10.30.7.9                    | 08:00:20:11:22:33 |                     | static  |
| 10.30.7.44                   | 08:00:20:44:55:66 |                     | static  |

## **dhcp show num-clients**

### **Purpose**

Display the number of allocated bindings for the DHCP server and the maximum number allowed.

### **Format**

**dhcp show num-clients**

### **Mode**

Enable.

### **Description**

The **dhcp show** command displays the number of allocated bindings for the DHCP server and the maximum number allowed.

### **Parameters**

None.

### **Restrictions**

None.

### **Examples**

To display information:

|  |
|--|
| <pre>xp# <b>dhcp show num-clients</b> 15 current clients (253 maximum)</pre> |
|--|

# Chapter 16

## diff Command

The **diff** command compares the active configuration with the specified configuration file.

### Format

**diff** <filename>|**startup**

### Mode

Configure.

### Parameters

|                |                                 |
|----------------|---------------------------------|
| <filename>     | Name of a configuration file.   |
| <b>startup</b> | The Startup configuration file. |

### Restrictions

None.

### Example

To compare the active configuration with the Startup configuration file:

```
xp# diff startup
```





# Chapter 17

## dvmrp Commands

The **dvmrp** commands let you configure and display information about Distance Vector Multicast Routing Protocol (DVMRP) interfaces.

**Note:** The X-Pedition router does not allow users to enable DVMRP and PIM simultaneously.

### Command Summary

[Table 15](#) lists the **dvmrp** commands. The sections following the table describe the command syntax.

**Table 15. dvmrp Commands**

|   |
|---|
| <b>dvmrp create tunnel local</b> <ipAddr> <b>remote</b> <ipAddr>  |
| <b>dvmrp enable interface</b> <ipAddr> <interface-name> <tunnel-name>   |
| <b>dvmrp enable tunnel</b> <ipAddr/name>  |
| <b>dvmrp set interface</b> <ipAddr> <hostname> [ <b>metric</b> <num>] [ <b>scope</b> <ipAddr/mask>] [ <b>threshold</b> <num>]                                       |
| <b>dvmrp set neighbor-timeout</b> <seconds>   |
| <b>dvmrp set prunetime</b>  |
| <b>dvmrp show</b> <option-list> [ <b>to-terminal</b>   <b>to-file</b> ]   |
| <b>dvmrp start</b>  |
| <b>dvmrp trace</b> <option-list> <b>detail</b>   <b>send</b>   <b>receive</b>   |
| <b>dvmrp trace local-options</b> <b>all</b>   <b>general</b>   <b>none</b>   <b>normal</b>   <b>policy</b>   <b>route</b>   <b>state</b> <b>task</b>   <b>timer</b> |

# dvmrp create tunnel

## Purpose

Creates a DVMRP tunnel.

## Format

**dvmrp create tunnel local** <ipAddr> **remote** <ipAddr>

## Mode

Configure.

## Description

The **dvmrp create tunnel** command creates a tunnel used to pass multicast traffic through a unicast network that resides between DVMRP clouds. As multicast frames exit the DVMRP *source* cloud, they are *encapsulated* in a unicast packet. When frames enter the *destination* cloud, the unicast packets are *un-encapsulated* and returned to the native multicast format.

The X-Pedition control module encapsulates and un-encapsulates each packet, not in the hardware ASICs but via software. Therefore, bandwidth is limited and CPU utilization can increase when sending multicast traffic across the tunnel. The amount of bandwidth and CPU utilization is dependant on many factors, such as: CPU-bound traffic such as learning new flows, ARPs, ACLs, RMON, packet size, traffic rate, and routing updates.

The tunnel is disabled by default. To enable it, use the **dvmrp enable tunnel** command.

## Parameters

|   |  |
|---|--|
| <b>local</b> <ipAddr>   | IP address of the local end point of this tunnel.  |
| <b>Note:</b> The local IP address must already be configured on the router. |  |
| <b>remote</b> <ipAddr>  | IP address of the remote end point of this tunnel. |

## Restrictions

Use caution when creating DVMRP tunnels with the **dvmrp create tunnel** command.

- Tunnels use unicast routing principles. Make sure a route exists between the tunnel source and destination (**local** <ipAddr> and **remote** <ipAddr>) you specify.

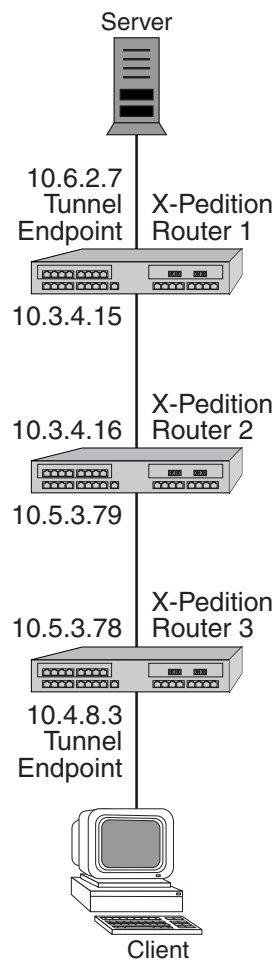
**Note:** The **dvmrp enable interface** command must be set to the DVMRP tunnel endpoint in order to establish a DVMRP neighbor relationship between endpoints.

- An IP interface has to exist before a tunnel can be created from it.
- Note:** A good way to confirm that a tunnel exists is to ping the other end of the tunnel.
- Tunnels cannot be created between two endpoints (i.e., on the same subnet).
  - The X-Pedition router supports a maximum of eight tunnels.

## Example

This example creates a DVMRP tunnel between R1 and R3 for the figure below.

```
R1(config)# dvmrp create tunnel local 10.6.2.7 remote 10.4.8.3
R3(config)# dvmrp create tunnel local 10.4.8.3 remote 10.6.2.7
```



## **dvmrp enable interface**

### **Purpose**

Enables DVMRP on the specified interface.

### **Format**

**dvmrp enable interface** *<ipAddr/name>*

### **Mode**

Configure.

### **Parameters**

---

|                            |   |
|----------------------------|---|
| <i>&lt;ipAddr/name&gt;</i> | IP address or name of the interface on which you are enabling DVMRP.<br><br>Enterasys recommends that you use alphabetic characters when defining interface names, since purely numeric interfaces will be interpreted as IP addresses. The X-Pedition router displays interface names up to 32 characters in length. |
|----------------------------|---|

---

### **Restrictions**

- The Control Module's en0 interface (labeled "10/100 Mgmt") is never used for multicast traffic. It is a management port only.
- The X-Pedition router supports a maximum of 96 multicast interfaces.
- The router does not allow users to enable DVMRP and PIM simultaneously. If a user attempts to enable DVMRP and PIM at the same time, one of the following messages will appear:
  - %CLI-E-NODVMRPFAC, This command cannot be used when PIM has been configured.
  - %CLI-E-NOPIMFAC, This command cannot be used when IGMP or DVMRP has been configured.

To switch between PIM and DVMRP you must remove the protocol's start command from the startup configuration and restart the router.

## Example

To enable DVMRP on the IP interface with IP address 10.50.78.2:

```
xp(config)# dvmrp enable interface 10.50.78.2
```

## **dvmrp enable tunnel**

### **Purpose**

Enables DVMRP on a configured tunnel, using the Local IP address.

### **Format**

**dvmrp enable tunnel** *<ipAddr>*

### **Mode**

Configure.

### **Description**

This command enables DVMRP on a previously created DVMRP tunnel.

### **Parameters**

---

|                       |  |
|-----------------------|--|
| <i>&lt;ipAddr&gt;</i> | IP address of the local end point of the tunnel. |
|-----------------------|--|

---

### **Restrictions**

- Tunnels use unicast routing principles. Make sure a route exists between the tunnel source and destination (**local** *<ipAddr>* and **remote** *<ipAddr>*) you specify.

**Note:** The **dvmrp enable interface** command must be set to the DVMRP tunnel endpoint in order to establish a DVMRP neighbor relationship between endpoints.

- An IP interface has to exist before a tunnel can be created from it.

**Note:** A good way to confirm that a tunnel exists is to ping the other end of the tunnel.

- Tunnels cannot be created between two endpoints (i.e., on the same subnet).
- The X-Pedition router supports a maximum of eight tunnels.

# dvmrp set interface

## Purpose

Configures various DVMRP parameters on an interface.

## Format

```
dvmrp set interface <ipAddr/name> [metric <num>] [scope <ipAddr/mask>]
[threshold <num>]
```

## Mode

Configure.

## Description

The **dvmrp set interface** command sets DVMRP parameters on an IP interface.

## Parameters

|                               |   |
|-------------------------------|---|
| <b>&lt;ipAddr/name&gt;</b>    | IP address or name of the interface on which you are configuring DVMRP parameters.<br><br>Enterasys recommends that you use alphabetic characters when defining interface names—purely numeric interfaces will be interpreted as IP addresses. The X-Pedition router will display interface names up to 32 characters in length.  |
| <b>metric</b> <num>           | The metric (cost) of this interface. Specify a number in the range 1 – 32. The default is 1. Normally you should not change this setting unless the network topology requires it.   |
| <b>scope</b><br><ipAddr/mask> | The multicast scope of this interface. The purpose of this option is to disallow the groups specified by a scope from being forwarded across an interface. This option therefore is a filtering mechanism. The threshold and the scope are two common mechanisms for implementing local simple filtering of a multicasting data.<br><br>Specify an IP address and network mask. Example: 239.0.0.0/8. |
| <b>threshold</b><br><num>     | The multicast threshold of this interface. The purpose of this option is to allow forwarding of a packet on a multicast interface only if the packet's threshold is at least the configured value. The threshold and the scope are two common mechanisms for implementing local simple filtering of a multicasting data.<br><br>Specify a number in the range 1 – 255. The default is 1.              |

## Restrictions

None.

## Example

To configure the interface 10.50.89.90 to have a metric of 5 and a threshold of 16:

```
xp(config)# dvmrp set interface 10.50.89.90 metric 5 threshold 16
```



# **dvmrp set neighbor-timeout**

## **Purpose**

Sets the number of seconds after which the X-Pedition router will consider the neighbor to be down.

## **Format**

**dvmrp set neighbor-timeout** *<seconds>*

## **Mode**

Configure.

## **Description**

This command sets the neighbor-timeout for all interfaces with DVMRP enabled. If you have old routers, this value should be increased to accommodate them; older routers do not send probes or route updates at 40-second intervals.

**Note:** The neighbor timeout value should be set to the same value between neighbors in order to avoid losing contact with the neighbor when values are set differently.

## **Parameters**

---

|                        |   |
|------------------------|---|
| <i>&lt;seconds&gt;</i> | Specifies the timeout value, which can be 40 to 400. The default is 35. |
|------------------------|---|

---

## **Restrictions**

None.

## **dvmrp set prunetime**

### **Purpose**

Set the prune timeout.

### **Format**

**dvmrp set prunetime** *<num>*

### **Mode**

Configure.

### **Description**

Set the prunetime time for all prune messages sent from this router to *<num>*. Default is 7200 seconds. This command is only applied to new prune timers. Any prune timers running when the timeout is changed will run to completion with the previous timeout value. New prune timers will be started with the changed timeout value.

### **Parameters**

---

|                    |   |
|--------------------|---|
| <i>&lt;num&gt;</i> | Specifies the timeout value, which can be from 300 to 7200 seconds. |
|--------------------|---|

---

### **Restrictions**

None.

# dvmrp show

## Purpose

Displays DVMRP parameters.

## Format

**dvmrp show** **all** | **designated forwarder source** *<ipAddr\_mask>* | **grafts** | **interface** [*<ipAddr>*]**all** | *<ipAddr>* | **mfc** | **neighbors** | **prunes-rx** | **prunes-tx** | **route** [*<ipAddr\_mask>*]**all** | [**to-terminal**|**to-file**]

## Mode

Enable.

## Parameters

|   |   |
|---|---|
| <b>all</b>  | Displays all DVMRP tables.  |
| <b>designated forwarder source</b> <i>&lt;ipAddr_mask&gt;</i> | Displays the DVMRP designated forwarder state for the given source IP address and mask.   |
| <b>grafts</b>   | Displays graft packets pending.   |
| <b>interface</b> [ <i>&lt;ipAddr&gt;</i> ] <b>all</b>         | Displays the state of an interface running DVMRP, along with other neighbor-related information. Neighbors are displayed with their DVMRP version and capability flags and Generation IDs; this information can help in debugging. If rules are in effect for an interface, they are indicated by ExportPol or the ImportPol flags. |
| <i>&lt;ipAddr&gt;</i>   | Displays DVMRP information for the specified interface.   |
| <b>mfc</b>  | Displays DVMRP multicast forwarding cache.  |
| <b>neighbors</b>  | Displays DVMRP neighbor and neighbor 2 packets.   |
| <b>prunes-rx</b>  | Displays prune packets received.  |
| <b>prunes-tx</b>  | Displays prune packets sent.  |
| <b>route</b> [ <i>&lt;ipAddr_mask&gt;</i> ] <b>all</b>        | Displays routes learned via DVMRP.  |
| <b>to-terminal</b>  | Displays the information on screen (default).   |
| <b>to-file</b>  | Writes the information to the gated dump file.  |

## Restrictions

None.

## Example

Here is an example of the **dvmrp show interface** command.

| xp# <b>dvmrp show interface all</b> |                   |     |                   |                |               |
|-------------------------------------|-------------------|-----|-------------------|----------------|---------------|
| Interface<br>Address                | Interface<br>Name | VIF | Neighbor<br>Count | Bad<br>Packets | Bad<br>Routes |
| -----                               | -----             | --- | -----             | -----          | -----         |
| 10.15.3.4                           | server1           | 1   | 1                 | 0              | 0             |
| 10.20.129.1                         | engineering       | 2   | 0                 | 0              | 0             |
| 10.121.17.248                       | sales             | 3   | 0                 | 0              | 0             |

# dvmrp start

## Purpose

Starts DVMRP multicast routing.

## Format

**dvmrp start**

## Mode

Configure.

## Description

The **dvmrp start** command starts DVMRP multicast routing on the configured multicast-enabled interfaces and tunnels.

**Note:** By default, DVMRP is not enabled and does not interact with any unicast protocol. However if you need to run a tunnel, make sure that the tunnel is accessible through a unicast routing mechanism.

## Parameters

None.

## Restrictions

The X-Pedition router does not allow users to enable DVMRP and PIM simultaneously. If a user attempts to enable DVMRP and PIM at the same time, one of the following messages will appear:

- %CLI-E-NODVMRPFAC, This command cannot be used when PIM has been configured.
- %CLI-E-NOPIMFAC, This command cannot be used when IGMP or DVMRP has been configured.

To switch between PIM and DVMRP you must remove the protocol's start command from the startup configuration and restart the router.

**Note:** If a user is running one of the multicast protocols and tries to activate the second protocol, an appropriate error message is displayed and the second protocol is not activated. However, the new configuration is entered into the configuration file without it being marked as being in error.

# dvmrp trace

## Purpose

Trace DVMRP protocol events. It is disabled by default.

## Format

**dvmrp trace graft | neighbor | packets | probe | prune | report | [detail|send|receive]**

## Mode

Configure.

## Description

Enables different debug traces from the DVMRP protocol. To have the debug trace messages displayed to the console, execute the **ip-router global set trace-state on** command (in config mode) or **ip-router set trace-state on** command (enable mode).

## Parameters

|                 |  |
|-----------------|--|
| <b>graft</b>    | Traces DVMRP graft packets.                                |
| <b>neighbor</b> | Traces DVMRP neighbor and neighbor 2 packets.              |
| <b>packets</b>  | Traces all DVMRP packets.                                  |
| <b>probe</b>    | Traces DVMRP probe packets.                                |
| <b>prune</b>    | Traces DVMRP prune packets.                                |
| <b>report</b>   | Traces DVMRP route report packets.                         |
| <b>detail</b>   | Show detailed information about the specified packet type. |
| <b>send</b>     | Show only specified packet type sent by the router.        |
| <b>receive</b>  | Show only specified packet type received by the router.    |

## Restrictions

None.

# dvmrp trace local-options

## Purpose

Sets various trace options for the DVMRP protocol only. By default, these trace-options are inherited from those specified by the **ip-router global set trace-options** command.

## Format

**dvmrp trace local-options** **all**| **general**| **none**| **normal**| **policy**| **route**| **state**| **task**| **timer**

## Mode

Configure.

## Description

Enables additional debug tracing for the internal DVMRP mechanism (not protocol related). To have the debug trace messages displayed to the console, execute the **ip-router global set trace-state on** command (config mode) or **ip-router set trace-state on** command (enable mode).

## Parameters

|                |   |
|----------------|---|
| <b>all</b>     | Turns on all tracing.   |
| <b>general</b> | Turns on normal and route tracing.  |
| <b>none</b>    | Specifies that all DVMRP tracing should be turned off.  |
| <b>normal</b>  | Traces normal protocol occurrences. Abnormal protocol occurrences are always traced.            |
| <b>policy</b>  | Traces application of protocol and user-specified policy to routes being imported and exported. |
| <b>route</b>   | Traces routing table changes for routes installed by DVMRP.                                     |
| <b>state</b>   | Traces state machine transitions in the protocols.  |
| <b>task</b>    | Traces system interface and processing associated with DVMRP.                                   |
| <b>timer</b>   | Traces timer usage by DVMRP.  |

## Restrictions

None.





# Chapter 18

## enable Command

The **enable** command switches the CLI session from User mode to Enable mode.

### Format

**enable**

### Mode

User.

### Description

Enable mode provides more facilities than User mode. You can display critical features within Enable mode including router configuration, access control lists, and SNMP statistics. To enter Enable mode from the User mode, enter the command **enable** (or **en**), then supply the password when prompted. If no password is configured, a warning message advising you to configure a password is displayed. If a password is configured and you do not know your password or pressing Return does not work, see the administrator for the X-Pedition router.

The Enable mode command prompt consists of the X-Pedition name followed by the pound sign(#), for example:

|     |
|-----|
| xp# |
|-----|

To exit Enable mode and return to User mode, type **exit** and press Return, or press Ctrl+Z. To proceed from the Enable mode into the Configure mode, use the **configure** command.

### Parameters

None.

---

## Restrictions

None.

# Chapter 19

## erase Command

The **erase** command erases the contents of the scratchpad or Startup configuration files.

### Format

**erase scratchpad|startup**

### Mode

Configure.

### Description

The **erase scratchpad** command erases the contents of the X-Pedition command scratchpad. The **erase startup** command erases the Startup configuration from the Control Module's NVRAM.

### Parameters

|                   |  |
|-------------------|--|
| <b>scratchpad</b> | Erases the contents of the scratchpad. The scratchpad contains configuration commands that you have issued but have not yet activated.   |
| <b>startup</b>    | Erases the contents of the Startup configuration. The Startup configuration is the configuration the X-Pedition router uses to configure itself when you reboot it. When you erase the Startup configuration, then reboot immediately, the X-Pedition router restarts without any configuration information. |

### Restrictions

The erase commands do not delete other types of files. To delete a file, use the **file del** command.



# Chapter 20

## exit Command

The **exit** command exits the current CLI mode to the previous mode. For example, if you are in the Enable mode, **exit** returns you to the User mode. If you are in Configure mode, **exit** returns you to Enable mode. If you are in User mode, **exit** closes your CLI session and logs you off the X-Pedition router.

### Format

**exit**

### Mode

All modes.

### Parameters

None.

### Restrictions

None.



# Chapter 21

## fddi Commands

### Command Summary

The **fddi** commands allow you to define and display parameters for the FDDI modules on the X-Pedition router. [Table 16](#) lists the fddi commands. The sections following the table describe the command syntax.

**Note:** A hardware limitation allows FDDI and SONET modules to increment only the *ifInUcastPkts* and *ifOutUcastPkts* ifMib counters. Non-unicast packet counters (i.e., *ifInNUcastPkts* and *ifOutNUcastPkts*) do not increment and will remain 0.

On gigabit and 10-Gigabit modules, all OCMAC counters increment correctly.

**Table 16. fddi Commands**

|   |
|---|
| <b>fddi reset</b> <i>&lt;port&gt;</i>   |
| <b>fddi set fddi-mode</b> <i>&lt;port&gt;</i> [ <b>sac-mode</b>   <b>das-mode</b> ]   |
| <b>fddi set fddi-fdx-mode</b> <i>&lt;port&gt;</i>   |
| <b>fddi set mac-group</b> <i>&lt;port&gt;</i> <b>trex</b> <i>&lt;number&gt;</i> <b>ma-unit-data-enable</b> [ <b>true</b>   <b>false</b> ]   |
| <b>fddi set mac-restricted-token</b> <i>&lt;port&gt;</i> <i>&lt;value&gt;</i>   |
| <b>fddi set path-group</b> <i>&lt;port&gt;</i> <b>tvx-lower-bound</b> <i>&lt;number&gt;</i> <b>tmax-lower-bound</b> <i>&lt;number&gt;</i><br><b>trex-max</b> <i>&lt;number&gt;</i>  |
| <b>fddi set port-group</b> <i>&lt;port&gt;</i> <b>ler-cutoff</b> <i>&lt;value&gt;</i> <b>ler-alarm</b> <i>&lt;value&gt;</i> <b>connection</b> <i>&lt;a b&gt;</i>  |
| <b>fddi set ring-purger</b> <i>&lt;port&gt;</i>   |
| <b>fddi set smt-group</b> <i>&lt;port&gt;</i> <b>userdata</b> <i>&lt;string or number&gt;</i> <b>connection-policy</b> <i>&lt;number&gt;</i><br><b>tnotify</b> <i>&lt;number&gt;</i> <b>stat-rpt-policy</b> [ <b>on</b>   <b>off</b> ] <b>trace-max-expiration</b> <i>&lt;value&gt;</i> |

**Table 16. fddi Commands (Continued)**

|  |
|--|
| <b>fddi set translation</b> [fddi_ipx_snap fddi_appletalk_arp] to [enet_II   802.3_raw_ipx   802.3_snap] port <port> |
| <b>fddi show fddi-mode</b> <port-list> all ports   |
| <b>fddi show fddi-status</b> <port-list> all ports   |
| <b>fddi show fddi-fdx-mode</b> <port-list> all ports   |
| <b>fddi show mac-group</b> <port-list> all ports   |
| <b>fddi show mac-restricted-token</b> <port-list> all ports  |
| <b>fddi show media-type</b> <port-list> all-ports  |
| <b>fddi show path-group</b> <port-list> all ports  |
| <b>fddi show port-group</b> <port-list> all ports  |
| <b>fddi show ring-purger</b> <port-list> all ports   |
| <b>fddi show smt-config</b> <port-list> all ports  |
| <b>fddi show smt-group</b> <port-list> all ports   |
| <b>fddi show translation</b> <port-list> all ports   |
| <b>fddi show version</b> <port-list> all ports   |



# fddi reset

## Purpose

Resets a specific FDDI port

## Format

**fddi reset** *<port>*

## Mode

Enable.

## Description

The **fddi reset** command allows you to restore a port without disrupting operations on the other port.

## Parameters

---

|                     |   |
|---------------------|---|
| <i>&lt;port&gt;</i> | Specifies the FDDI port. To specify an FDDI port, use the prefix: fi. For example, to specify an FDDI port in slot 5, use fi.5.1. |
|---------------------|---|

---

## Restrictions

None.

## Example

To reset port fi.5.1:

xp# **fddi reset fi.5.1**

## **fddi set fddi-mode**

### **Purpose**

Sets the FDDI operating mode for the specified FDDI port(s).

### **Format**

**fddi set fddi-mode** <port> [**sac-mode**|**das-mode**]

### **Mode**

Configure.

### **Description**

The **fddi set fddi-mode** command allows you to configure the ports as single attachment concentrators (SAC) or dual attachment stations (DAS). SACs attach to the primary ring only. They are used primarily to attach routers to a ring through concentrators. In SAC mode, port A becomes an M port, and port B becomes an S port. The M port in a SAC is used to extend the primary ring, and connects to an A, B, or S (slave) port. The S port in a SAC connects to a single ring only and typically connects to an M port.

A DAS connects to both the primary and secondary FDDI rings. Thus, in case of a device failure, it is capable of wrapping the ring.

### **Parameters**

|                 |   |
|-----------------|---|
| <port>          | Specifies the FDDI port. To specify an FDDI port, use the prefix: fi. For example, to specify an FDDI port in slot 5, use fi.5.1. |
| <b>sac-mode</b> | Sets the operating mode to single attachment concentrator (SAC).  |
| <b>das-mode</b> | Sets the operating mode to dual attachment station (DAS).   |

### **Restrictions**

DAS mode is not available for UTP.

## Example

To set the operating mode of port fi.5.1 to DAS:

```
xp# fddi set fddi-mode fi.5.1 das-mode
```

## **fddi set fddi-fdx-mode**

### **Purpose**

Sets the specified FDDI port to full-duplex mode.

### **Format**

**fddi set fddi-fdx-mode** *<port>*

### **Mode**

Configure.

### **Description**

The **fddi set fddi-fdx-mode** command sets a specific FDDI port to full-duplex mode. When you set the FDDI port to full-duplex mode, it executes a protocol that detects if there is another device on the FDDI ring that is also attempting to run full duplex. If it does detect another device in full-duplex mode and it is the only other device on the ring, the ports will operate in full-duplex mode. But if the port detects that there is more than one other device on the ring, it will cease to operate in full-duplex mode.

**Note:** Changing the station mode on a FDDI port will negate all previously executed FDDI commands.

### **Parameters**

---

|                     |   |
|---------------------|---|
| <i>&lt;port&gt;</i> | Specifies the FDDI port. To specify an FDDI port, use the prefix: fi. For example, to specify an FDDI port in slot 5, use fi.5.1. |
|---------------------|---|

---

### **Restrictions**

The SmartSwitch 6000 does not support FDDI full duplex operation.

### **Example**

To set port fi.5.2 to full-duplex mode:

```
xp# fddi set fddi-fdx-mode fi.5.2
```

# fddi set mac-group

## Purpose

Sets the MAC configuration parameters for the specified FDDI port

## Format

**fddi set mac-group** <port> **treq** <number> **ma-unit-data-enable** [true|false]

## Mode

Configure.

## Description

The **fddi set mac-group** command sets a station's MAC parameters. During the claim process, each station "bids" on the right to initialize the ring. The station's bid is its token rotation time (**treq** value). The station with the fastest rotation time wins the claim as it can support the rotation time of all the other stations.

## Parameters

|   |  |
|---|--|
| <port>                                  | Specifies the FDDI port. To specify an FDDI port, use the prefix: fi. For example, to specify an FDDI port in slot 5, use fi.5.1.  |
| <b>treq</b> <number>                    | Specifies the station's desired token rotation time in milliseconds. This value should be less than or equal to the <b>treq-max</b> value specified in the <b>fddi set path-group</b> command. Enter a value between 4 and 173.01504. Note that because of unit conversions, treq may be rounded slightly down from the value specified. |
| <b>ma-unit-data-enable</b> [true false] | Sets the MA_UNITDATA_ENABLE flag to true or false.<br><br><b>Note:</b> This parameter is included to be consistent with the MIB only. Setting this parameter on the X-Pedition router has no affect on the operation of the network.   |

## Restrictions

None.

## Example

To set the MAC configuration parameters for port fi.4.2:

```
xp# fddi set mac group fi.4.2 treq 15 ma-unit-data-enable true
```

# **fddi set mac-restricted-token**

## **Purpose**

Sets the MAC restricted token time out for the specified FDDI port.

## **Format**

**fddi set mac-restricted-token** *<port>* *<value>*

## **Mode**

Configure.

## **Description**

The **fddi set mac-restricted-token** command specifies how long a station can hold a restricted token. A station that holds the restricted token can use the entire network bandwidth for an extended period. Upon completion of its transmission, the station with the restricted token converts the token to non-restricted, re-issues it to the ring and normal operations continue.

## **Parameters**

|                      |  |
|----------------------|--|
| <i>&lt;port&gt;</i>  | Specifies an FDDI port. To specify an FDDI port, use the prefix: fi. For example, to specify an FDDI port in slot 5, use fi.5.1. |
| <i>&lt;value&gt;</i> | Specifies the MAC restricted token time out in milliseconds. Specify a value between 0 and 10000.                                |

## **Restrictions**

None.

## Example

To set the restricted token time out for port fi.4.2:

```
xp# fddi set mac-restricted-token fi.4.2 25
```



# fddi set path-group

## Purpose

Sets the PATH configuration parameters for the specified FDDI port.

## Format

```
fddi set path-group <port> tvx-lower-bound <number> tmax-lower-bound <number>  
treq-max <number>
```

## Mode

Configure.

## Description

The **fddi set path-group** command sets thresholds for the timers used by any MAC configured in the primary path. The valid transmission timer (tvx) clocks the period between valid transmissions. When the station receives a valid transmission, the tvx resets. If no valid frame, including a token, is received and the tvx expires, the station begins ring initialization.

The **tmax** value is the minimum target rotation time (TTRT) supported by a MAC. The **treq-max** value is the maximum rotation time used by a MAC.

## Parameters

|                                     |   |
|-------------------------------------|---|
| <port>                              | Specifies an FDDI port. To specify an FDDI port, use the prefix: fi. For example, to specify an FDDI port in slot 5, use fi.5.1.  |
| <b>tvx-lower-bound</b><br><number>  | Specifies the minimum TVX value (in milliseconds) that shall be used by any MAC configured in this path. This value should be lower than the <b>treq-max</b> . Enter a value between 0 and 5.20192.           |
| <b>tmax-lower-bound</b><br><number> | Specifies the minimum TMAX value (in milliseconds) supported by any MAC configured in this path. This value should be greater than or equal to the <b>treq-max</b> . Enter a value between 10 and 1331.69152. |

---

|                                       |  |
|---------------------------------------|--|
| <b>trex-max</b> <i>&lt;number&gt;</i> | Specifies the maximum TREX value (in milliseconds) that shall be used by any MAC configured in this path. This value must be greater than the <b>tvx-lower-bound</b> and equal to or less than the <b>tmax-lower-bound</b> . |
|---------------------------------------|--|

**Note:** Due to unit conversions, the **tvx-lower-bound**, **tmax-lower-bound**, and **trex-max** values may be rounded down slightly from the values specified.

---

## Restrictions

None.

## Example

To set the path configuration parameters for port fi.4.2:

|   |
|---|
| <code>xp# fddi set path-group fi.4.2 tvx-lower-bound 5 tmax-lower-bound 18 trex-max 18</code> |
|---|

# fddi set port-group

## Purpose

Sets parameters for the specified FDDI port.

## Format

**fddi set port-group** <port> **ler-cutoff** <value> **ler-alarm** <value> **connection** <a/b>

## Mode

Configure.

## Description

The **fddi set port-group** command allows you to specify link error monitoring (LEM) thresholds for an FDDI port. If the link error rate exceeds the **ler-alarm** value, an alarm is generated. If more errors are detected after the alarm, and the **ler-cutoff** is exceeded, the link is declared faulty and the connection is broken.

## Parameters

|                           |  |
|---------------------------|--|
| <port>                    | Specifies an FDDI port. To specify an FDDI port, use the prefix: fi. For example, to specify an FDDI port in slot 5, use fi.5.1.   |
| <b>ler-cutoff</b> <value> | Specifies the desired link error rate cutoff. If exceeded, the link connection will be broken.   |
| <b>ler-alarm</b> <value>  | Specifies the desired link error rate alarm limit. If exceeded, the link connection will generate an alarm.  |
| <b>connection</b> <a b>   | Specifies the actual or physical port being configured. Specify <b>a</b> to set parameters for the port on the left side of the PHY. Specify <b>b</b> to set parameters for the port on the right side of the PHY. |

## Restrictions

None.

## Example

To set the PORT configuration parameters for port fi.4.2:

```
xp# fddi set port-group fi.4.2 ler-cutoff 17 ler-alarm 20 connection b
```

# **fddi set ring-purger**

## **Purpose**

Turns on the ring purger mode for the specified FDDI port.

## **Format**

**fddi set ring-purger** <port>

## **Mode**

Configure.

## **Description**

The **fddi set ring-purger** command allows the FDDI port to participate in ring purger election. The station “elected” as the ring purger strips the ring of obsolete or stray frames and packets. This prevents old packets from continually circling the ring.

## **Parameters**

|        |  |
|--------|--|
| <port> | Specifies an FDDI port. To specify an FDDI port, use the prefix: fi. For example, to specify an FDDI port in slot 5, use fi.5.1. |
|--------|--|

## **Restrictions**

None.

## **Example**

To enable ring purger mode for port fi.4.2:

```
xp# fddi set ring-purger fi.4.2
```

## **fddi set smt-group**

### **Purpose**

Sets the station management (SMT) parameters for the specified FDDI port.

### **Format**

**fddi set smt-group** <port> **userdata** <string or number>|**connection-policy** <number>|**tnotify** <number>|**stat-rpt-policy** [on|off]|**trace-max-expiration** <value>

### **Mode**

Configure.

### **Description**

The **fddi set smt-group** command sets various station management parameters, as follows:

- The connection policy specifies which type of connection the station will reject. In the policy statement, the first value represents the local port and the second value represents the port of the adjacent station. The Bit # specifies the binary bit position. To specify a connection policy, determine which connections will be rejected, calculate the decimal value of the bit ( $2^{\text{Bit \#}}$ ) for each connection rejected, and add these values together.

| <b>Policy</b> | <b>Bit #</b> |
|---------------|--------------|
| Reject A-A    | 0            |
| Reject A-B    | 1            |
| Reject A-S    | 2            |
| Reject A-M    | 3            |
| Reject B-A    | 4            |
| Reject B-B    | 5            |
| Reject B-S    | 6            |
| Reject B-M    | 7            |
| Reject S-A    | 8            |
| Reject S-B    | 9            |
| Reject S-S    | 10           |
| Reject S-M    | 11           |
| Reject M-A    | 12           |
| Reject M-B    | 13           |
| Reject M-S    | 14           |
| Reject M-M    | 15           |

- Each station on an FDDI ring announces its address to its downstream neighbor by transmitting neighborhood information frames (NIF). Specify the time period between the transmission of NIFs.
- When there is an unexpected network or node change, a station can generate status reporting frames (SRF) which notify the network of the unexpected event or condition (such as a ring wrap). You can turn this feature on or off for a particular port.

## Parameters

|   |  |
|---|--|
| <b>&lt;port&gt;</b>                                 | Specifies an FDDI port. To specify an FDDI port, use the prefix: fi. For example, to specify an FDDI port in slot 5, use fi.5.1.   |
| <b>userdata</b><br><b>&lt;string or number&gt;</b>  | Specifies a text string or numbers. May be up to 7 characters.   |
| <b>connection-policy</b><br><b>&lt;value&gt;</b>    | Specifies a value representing the connection policies in effect in a node. This value is a sum of the decimal values calculated for each connection policy. Note that Bit 15, (rejectM-M), is always set and cannot be cleared.<br><br>Example: Reject A-A, S-M and M-M = ( $2^0 + 2^{11} + 2^{15}$ ) |
| <b>tnotify</b> <b>&lt;value&gt;</b>                 | Specifies the amount of time between the transmission of neighborhood information frames (nifs).   |
| <b>stat-rpt-policy</b> <b>[on off]</b>              | Specifies whether the station will generate status reporting frames for unexpected events and conditions.  |
| <b>trace-max-expiration</b><br><b>&lt;value&gt;</b> | Specifies the amount of time before a trace expires. Enter a value between 6002 and 100000.  |

## Restrictions

None.

# fddi set translation

## Purpose

Sets the IPX/Appletalk ARP frame translation settings for the specified FDDI port.

## Format

**fddi set translation** [**fddi\_ipx\_snap**| **fddi\_appletalk\_arp**] to [**enet\_II**|**802.3\_raw\_ipx**|  
**802.3\_snap**] **port** <*port*>

## Mode

Configure.

## Description

The **fddi set translation** command allows you to specify how FDDI IPX Snap frames or FDDI Appletalk ARP frames are translated to Ethernet. FDDI IPX Snap frames are translated to Ethernet II frames, by default. Alternatively, you can specify that they be translated to 802.3 Raw IPX frames. FDDI Appletalk ARP frames are translated to 802.3 Snap frames by default. Alternatively, you can specify that they be translated to Ethernet II frames.

## Parameters

|                           |  |
|---------------------------|--|
| <b>fddi_ipx_snap</b>      | Specifies that the frames to be translated are IPX Snap frames.  |
| <b>fddi_appletalk_arp</b> | Specifies that the frames to be translated are FDDI Appletalk ARP frames.  |
| <b>enet_II</b>            | Specifies that the frames will be translated as Ethernet II frames.  |
| <b>802.3_raw_ipx</b>      | Specifies that the frames will be translated as 802.3 Raw IPX frames.  |
| <b>802.3_snap</b>         | Specifies that the frames will be translated as 802.3 Snap frames.   |
| < <i>port</i> >           | Specifies an FDDI port. To specify an FDDI port, use the prefix: fi. For example, to specify an FDDI port in slot 5, use fi.5.1. |



## Restrictions

- IPX Snap frames cannot be translated to 802.3 Snap frames.
- Appletalk ARP frames cannot be translated to 802.3 Raw IPX frames.

## Example

To specify the translation settings for port fi.4.2:

```
xp# fddi set translation fddi_ipx_snap toenet_II fi.4.2
```

# fddi show fddi-mode

## Purpose

Displays the operating FDDI mode for the specified port(s).

## Format

**fddi show fddi-mode** *<port-list>* | **all ports**

## Mode

Enable.

## Description

The **fddi show fddi-mode** command displays the operating mode for a specified port. This allows you to determine whether the specified port is operating as a Single Attachment Concentrator (SAC) or Dual Attachment Station (DAS).

## Parameters

|                          |   |
|--------------------------|---|
| <i>&lt;port-list&gt;</i> | Specifies the FDDI port(s). To specify an FDDI port, use the prefix: fi.<br>For example, to specify an FDDI port in slot 5, use fi.5.1. |
| <b>all-ports</b>         | Specifies all FDDI ports.   |

## Restrictions

None.

## Example

To display the operating mode of port fi.5.1:

```
xp# fddi show fddi-mode fi.5.1
```

# fddi show fddi-status

## Purpose

Displays the FDDI status for the specified FDDI port(s).

## Format

**fddi show fddi-status** <port-list>|**all ports**

## Mode

Enable.

## Description

The **fddi show fddi-status** command displays FDDI status information for the specified ports. This includes station ID, upstream and downstream neighbors, and station state.

## Parameters

|                  |   |
|------------------|---|
| <port-list>      | Specifies the FDDI port(s). To specify an FDDI port, use the prefix: fi.<br>For example, to specify an FDDI port in slot 5, use fi.5.1. |
| <b>all-ports</b> | Specifies all FDDI ports.   |

## Restrictions

None.

## Example

To display the fddi status of ports fi.5.1 and fi.5.2:

```
xp# fddi show fddi-status fi.5.(1-2)
```

## **fddi show fddi-fdx-mode**

### **Purpose**

Displays the FDDI full duplex value for the specified FDDI port(s).

### **Format**

**fddi show fddi-fdx-mode** *<port-list>*|**all ports**

### **Mode**

Enable.

### **Description**

The **fddi show fddi-fdx-mode** command displays the full duplex value for a specific FDDI port or ports. This allows you to determine whether or not the specified port is active and running in full-duplex mode. Note that the FDDI port will operate in full-duplex mode only if there is one other station on the ring that is running full-duplex. It will cease running in full-duplex if there are multiple stations on the ring.

**Note:** Because FDDI full duplex is not an industry standard, its implementation in the SSR-FDDI-02 is based on the Digital Equipment Corporation (DEC) standard and will interoperate with all DEC products and most Enterasys FDDI products.

### **Parameters**

|                          |   |
|--------------------------|---|
| <i>&lt;port-list&gt;</i> | Specifies the FDDI port(s). To specify an FDDI port, use the prefix: fi.<br>For example, to specify an FDDI port in slot 5, use fi.5.1. |
| <b>all-ports</b>         | Specifies all FDDI ports.   |

### **Restrictions**

None.

## Example

To display the full-duplex status of port fi.5.2:

```
xp# fddi show fddi-fdx-mode fi.5.2
```

## **fddi show mac-group**

### **Purpose**

Displays the MAC configuration parameters for the specified FDDI port(s).

### **Format**

**fddi show mac-group** *<port-list>* | **all ports**

### **Mode**

Enable.

### **Description**

The **fddi show mac-group** command allows you to display the requested rotation time (treq value) and MAC Unit Data Enable flag of the specified port(s).

### **Parameters**

|                          |   |
|--------------------------|---|
| <i>&lt;port-list&gt;</i> | Specifies the FDDI port(s). To specify an FDDI port, use the prefix: fi.<br>For example, to specify an FDDI port in slot 5, use fi.5.1. |
| <b>all-ports</b>         | Specifies all FDDI ports.   |

### **Restrictions**

None.

### **Example**

To display the MAC parameters of port fi.3.2:

```
xp# fddi show mac-group fi.3.2
```

# **fddi show mac-restricted token**

## **Purpose**

Displays the MAC restricted token time for the specified FDDI port(s).

## **Format**

**fddi show mac-restricted-token** *<port-list>*|**all ports**

## **Mode**

Enable.

## **Description**

The **fddi show mac-restricted-token** command allows you to display the restricted token time for the specified port(s). A station that holds the restricted token can use the entire network bandwidth until the restricted token time expires.

## **Parameters**

|                          |   |
|--------------------------|---|
| <i>&lt;port-list&gt;</i> | Specifies the FDDI port(s). To specify an FDDI port, use the prefix: fi.<br>For example, to specify an FDDI port in slot 5, use fi.5.1. |
| <b>all-ports</b>         | Specifies all FDDI ports.   |

## **Restrictions**

None.

## **Example**

To display the restricted token time for port fi.4.1:

```
xp# fddi show mac-restricted-token fi.4.1
```

## **fddi show media-type**

### **Purpose**

Displays the media type for the specified FDDI port(s).

### **Format**

**fddi show media-type** *<port-list>* | **all ports**

### **Mode**

Enable.

### **Description**

The **fddi show media-type** command allows you to display the media type and PHY states of the specified FDDI port(s). The media types are Single-Mode Fiber, Multi-Mode Fiber (MMF), and Unshielded Twisted Pair (UTP).

### **Parameters**

|                          |   |
|--------------------------|---|
| <i>&lt;port-list&gt;</i> | Specifies the FDDI port(s). To specify an FDDI port, use the prefix: fi.<br>For example, to specify an FDDI port in slot 5, use fi.5.1. |
| <b>all-ports</b>         | Specifies all FDDI ports.   |

### **Restrictions**

None.

### **Example**

To display the media type of ports fi.4.1 and fi.4.2:

```
xp# fddi show media-type fi.4.(1-2)
```



# fddi show path-group

## Purpose

Displays the PATH configuration parameters for the specified port(s).

## Format

**fddi show path-group** *<port-list>* | **all ports**

## Mode

Enable.

## Description

The **fddi show path-group** command allows you to display the various thresholds for the timers used by the MACs in the primary path. These include the minimum valid transmission time (tvx), which is the period between valid transmissions; the minimum tmax value, which is the lowest target token rotation time supported by a MAC; and the maximum **trreq** value, which is the maximum target rotation time that may be requested by a station in the primary path.

## Parameters

|                          |   |
|--------------------------|---|
| <i>&lt;port-list&gt;</i> | Specifies the FDDI port(s). To specify an FDDI port, use the prefix: fi.<br>For example, to specify an FDDI port in slot 5, use fi.5.1. |
| <b>all-ports</b>         | Specifies all FDDI ports.   |

## Restrictions

None.

## Example

To display the PATH parameters for port fi.3.2:

```
xp# fddi show media-type fi.3.2
```

# **fddi show port-group**

## **Purpose**

Displays the PORT configuration parameters for the specified FDDI port(s).

## **Format**

**fddi show port-group** *<port-list>* | **all ports**

## **Mode**

Enable.

## **Description**

The **fddi show port-group** command allows you to display PORT configuration parameters for the specified FDDI port(s). These include the port connections; the link error rate alarm (ler-alarm) value, which is the number of link errors detected before an alarm is generated; and the link error rate cutoff (ler-cutoff) value, which is the number of link errors detected before the link is declared faulty and the connection is broken.

## **Parameters**

|                          |   |
|--------------------------|---|
| <i>&lt;port-list&gt;</i> | Specifies the FDDI port(s). To specify an FDDI port, use the prefix: fi.<br>For example, to specify an FDDI port in slot 5, use fi.5.1. |
| <b>all-ports</b>         | Specifies all FDDI ports.   |

## **Restrictions**

None.

## Example

To display the PORT parameters for port fi.4.2:

```
xp# fddi show port-group fi.4.2
```

# fddi show ring-purger

## Purpose

Displays the ring purger value for the specified port(s).

## Format

**fddi show ring-purger** <port-list>|**all ports**

## Mode

Enable.

## Description

The **fddi show ring-purger** command allows you to display the ring purger status of the specified port(s). When this feature is turned on, the FDDI port participates in ring purger election.

## Parameters

|                  |   |
|------------------|---|
| <port-list>      | Specifies the FDDI port(s). To specify an FDDI port, use the prefix: fi.<br>For example, to specify an FDDI port in slot 5, use fi.5.1. |
| <b>all-ports</b> | Specifies all FDDI ports.   |

## Restrictions

None.

## Example

To display the ring purger status of port fi.4.1:

```
xp# fddi show ring-purger fi.4.1
```

## **fddi show smt-config**

### **Purpose**

Displays the current SMT configurations for the specified FDDI port(s).

### **Format**

**fddi show smt-config** *<port-list>* | **all ports**

### **Mode**

Enable.

### **Description**

The **fddi show smt-config** command allows you to display station management (SMT) information for the specified FDDI port(s). These include the SMT version; the *treq* value, which is the station's requested token rotation time; the *tneg* value, which is the token rotation time negotiated by the station during the claim process; and the *tnotify* value, which is the period between the generation of neighborhood information frames.

### **Parameters**

|                          |  |
|--------------------------|--|
| <i>&lt;port-list&gt;</i> | Specifies the FDDI port(s). To specify an FDDI port, use the prefix: <i>fi</i> . For example, to specify an FDDI port in slot 5, use <i>fi.5.1</i> . |
| <b>all-ports</b>         | Specifies all FDDI ports.  |

### **Restrictions**

None.

## Example

To display SMT information for port fi.4.2:

```
xp# fddi show smt-config fi.4.2
```

# fddi show smt-group

## Purpose

Displays the SMT configuration parameters for the specified FDDI port(s).

## Format

**fddi show smt-group** *<port-list>*|**all ports**

## Mode

Enable.

## Description

The **fddi show smt-group** command allows you to display Station Management (SMT) parameters that were set for the specified port(s). These include the user data; connection policy, which specifies the type of connections rejected by the port(s); the status report policy, which specifies whether a station generates Status Reporting Frames (SRF) when unexpected events or conditions occur; the time period between the generation of Neighborhood Information Frames (NIF); and the trace max expiration time.

## Parameters

|                          |   |
|--------------------------|---|
| <i>&lt;port-list&gt;</i> | Specifies the FDDI port(s). To specify an FDDI port, use the prefix: fi.<br>For example, to specify an FDDI port in slot 5, use fi.5.1. |
| <b>all-ports</b>         | Specifies all FDDI ports.   |

## Restrictions

None.



## Example

To display SMT parameters configured for port fi.4.1:

```
xp# fddi show smt-group fi.4.1
```

# fddi show translation

## Purpose

Displays the frame translation settings for the specified port(s).

## Format

**fddi show translation** *<port-list>* | **all-ports**

## Mode

Enable.

## Description

The **fddi show translation** command allows you to display the IPX/Appletalk ARP frame translation settings.

## Parameters

|                          |   |
|--------------------------|---|
| <i>&lt;port-list&gt;</i> | Specifies the FDDI port(s). To specify an FDDI port, use the prefix: fi.<br>For example, to specify an FDDI port in slot 5, use fi.5.1. |
| <b>all-ports</b>         | Specifies all FDDI ports.   |

## Restrictions

None.

## Example

To display the translation settings configured for port fi.4.1:

```
xp# fddi show translation fi.4.1
```

# fddi show version

## Purpose

Displays the firmware version of the specified FDDI port(s).

## Format

**fddi show version** <port-list>|**all ports**

## Mode

Enable.

## Description

The **fddi show version** command allows you to display the firmware version of the specified port(s).

## Parameters

|                  |   |
|------------------|---|
| <port-list>      | Specifies the FDDI port(s). To specify an FDDI port, use the prefix: fi.<br>For example, to specify an FDDI port in slot 5, use fi.5.1. |
| <b>all-ports</b> | Specifies all FDDI ports.   |

## Restrictions

None.

## Example

To display the firmware version of port fi.4.1:

```
xp# fddi show version fi.4.1
```



# Chapter 22

## file Commands

The **file** commands enable you to display a directory of the files on a storage device, display the contents of a file on the console, and delete a file.

### Command Summary

[Table 17](#) lists the **file** commands. The sections following the table describe the command syntax.

**Table 17. file Commands**

|   |
|---|
| <b>file copy</b> backup-cm  primary-cm [bootflash:  slot0:] <src-file-name> { [bootflash:  slot0:] <dest-file-name> } |
| <b>file delete</b> backup-cm  primary-cm { [bootflash:  slot0:] <file-name> }   |
| <b>file dir</b> backup-cm  primary-cm { bootflash:  slot0: } [directory-name]   |
| <b>file rename</b> [device-name] <original-file-name> <new-file-name>   |
| <b>file type</b> <file-name>  |

# file copy

## Purpose

Copy a file.

## Format

```
file copy backup-cm| primary-cm {[bootflash:| slot0:] <src-file-name>}  
{[bootflash:| slot0:] <dest-file-name>}
```

## Mode

User.

## Description

Copies a file from a specified CM's device to a device on the Primary CM.

## Parameters

|  |   |
|--|---|
| <b>backup-cm</b>   | The source file to copy from is on the Backup CM.                                 |
| <b>primary-cm</b>  | The source file to copy from is on the Primary CM.                                |
| <b>bootflash:</b>  | The Control Module's NVRAM—the default if device-name not specified.              |
| <b>slot0:</b>  | The PCMCIA Flash Module in slot 0 (the upper slot).                               |
| <b>Note:</b> Device names end with a colon and are not followed by a space.<br><br>The X-Pedition router supports PCMCIA Flash Modules obtained from Enterasys Networks only. For information regarding the PCMCIA Virtual File systems VFS1 and VFS2, see the <i>Enterasys X-Pedition User Reference Manual</i> . |   |
| <b>&lt;src-file-name&gt;</b>   | Name of the file to copy from, located on either the Backup CM or the Primary CM. |
| <b>&lt;dest-file-name&gt;</b>  | Name of the file to copy to the Primary CM only.                                  |

## Restrictions

You can copy a file from either the Backup CM or Primary CM to the Primary CM only. Copying files to the Backup CM is not allowed.

## Example

To copy a file named **core** from the slot0 device on the backup CM to the bootflash device on the primary CM and rename it to **core1**:

```
xp# file copy backup-cm slot0:core bootflash:core1
```

To copy a file named **core** from the slot0 device on the primary CM to the bootflash device on the primary CM and rename it to **core1**(if no device is specified, then the default device will be the bootflash):

```
xp# file copy primary-cm slot0:core core1
```

To copy a file named **tempfile** from the bootflash device on the backup CM to the bootflash device on the primary CM and rename it to **newfile** (if no device is specified, then the default device will be the bootflash):

```
xp# file copy backup-cm tempfile newfile
```

# file delete

## Purpose

Delete a file.

## Format

**file delete** **backup-cm**| **primary-cm** { [**bootflash:**| **slot0:**] <*file-name*> }

## Mode

Enable.

## Description

The **file delete** command deletes the specified file from either the Primary CM or the Backup CM. By default, if a device-name is not specified, it is assumed to be the **bootflash:** device.

## Parameters

|                      |   |
|----------------------|---|
| <b>backup-cm</b>     | The file to delete is on the Backup CM.   |
| <b>primary-cm</b>    | The file to delete is on the Primary CM.  |
| <b>bootflash:</b>    | The Control Module's NVRAM—the default if device-name not specified.  |
| <b>slot0:</b>        | The PCMCIA Flash Module in slot 0 (the upper slot).   |
|                      | <b>Note:</b> Device names end with a colon and are NOT followed by a space. The X-Pedition router supports PCMCIA Flash Modules obtained from Enterasys Networks only. For information regarding the PCMCIA Virtual File systems VFS1 and VFS2, see the <i>Enterasys X-Pedition User Reference Manual</i> . |
| < <i>file-name</i> > | Name of the file to delete.   |

## Restrictions

None.



## Examples

To delete the file bootflash:config.old from the Primary CM:

```
xp# file delete primary-cm bootflash:config.old
```

To delete the file slot0:core.backup from the Backup CM:

```
xp# file delete backup-cm slot0:config.old
```

To delete the file config.save (default bootflash:) on the Backup CM:

```
xp# file delete backup-cm config.save
```

## file dir

### Purpose

Display contents of a file system.

### Format

**file dir backup-cm| primary-cm { bootflash:| slot0: } [directory-name]**

### Mode

User.

### Description

Displays a directory of the files on the specified storage device.

### Parameters

|                       |   |
|-----------------------|---|
| <b>backup-cm</b>      | Display the contents of a file system on the Backup control module.   |
| <b>primary-cm</b>     | Display the contents of a file system on the Primary control module.  |
| <b>device-name</b>    | Device name of file system to list. You can specify one of the following:<br><br><b>bootflash:</b> The Control Module's NVRAM.<br><b>slot0:</b> The PCMCIA Flash Module in slot 0 (the upper slot).<br><br><b>Note:</b> Device names end with a colon and are not followed by a space.<br><br>The X-Pedition router supports PCMCIA Flash Modules obtained from Enterasys Networks only. For information regarding the PCMCIA Virtual File systems VFS1 and VFS2, see the <i>Enterasys X-Pedition User Reference Manual</i> . |
| <b>directory-name</b> | Optional directory to list.   |

### Restrictions

None.

## Example

To display the contents of a file system:

```
xp# file dir backup-cm bootflash:  
xp# file dir primary-cm slot0:tmp/
```

# file rename

## Purpose

Rename a file.

## Format

**file rename** [**device-name**] <original-file-name> <new-file-name>

## Mode

User.

## Description

Renames a file from the original file name to a new file name within the same directory.

## Parameters

|                      |   |
|----------------------|---|
| <b>device-name</b>   | Optional device name of file system where the file is located. You can specify one of the following options:<br><br><b>bootflash:</b> The Control Module's NVRAM (the default if device-name not specified).<br><br><b>slot0:</b> The PCMCIA Flash Module in slot 0 (the upper slot).<br><br><b>Note:</b> Device names end with a colon and are not followed by a space.<br><br>The X-Pedition router supports PCMCIA Flash Modules obtained from Enterasys Networks only. For information regarding the PCMCIA Virtual File systems VFS1 and VFS2, see the <i>Enterasys X-Pedition User Reference Manual</i> . |
| <original-file-name> | File you wish to rename.  |
| <new-file-name>      | The new name of the file, which will exist in the same directory specified by the original-file-name. Users are not allowed to use a device name or directory name as part of the <i>new-file-name</i> .  |

## Restrictions

Not available for files on the Backup CM.

## Examples

To rename a file:

```
xp# file rename slot0:core tempcore
```

```
xp# file rename file1 file2
```

## file type

### Purpose

Display contents of a file.

### Format

**file type** <file-name>

### Mode

Enable.

### Description

Displays the contents of a file.

### Parameters

|               |   |
|---------------|---|
| <file-name>   | Name of the file to display. The filename can include a device-name using this format: <device-name>:<file-name>. By default, if a device-name is not specified, it is assumed to be the <b>bootflash:</b> device. The <b>bootflash:</b> device is the default device for storing configuration files.  |
| <device-name> | Device name. You can specify one of the following:<br><br><b>Note:</b> Device names end with a colon.<br><br><b>bootflash:</b> The Control Module's NVRAM.<br><br><b>slot0:</b> The PCMCIA Flash Module in slot 0 (the upper slot).<br><br><b>slot1:</b> The PCMCIA Flash Module in slot 1 (the lower slot).<br><br>The X-Pedition router supports PCMCIA Flash Modules obtained from Enterasys Networks only. For information regarding the PCMCIA Virtual File systems VFS1 and VFS2, see the <i>Enterasys X-Pedition User Reference Manual</i> . |

### Restrictions

None.

## Example

To display the contents of the file startup (the startup configuration file):

```
xp# file type startup
```





# Chapter 23

## filters Commands

The **filters** commands let you create and apply the following types of security filters:

- **Address filters.** Address filters block traffic based on a frame's source MAC address, destination MAC address, or both. Address filters are always configured and applied on the input port.
- **Static entry filters.** Static entry filters allow or force traffic to go to a set of destination ports based on a frame's source MAC address, destination MAC address, or both. Static entry filters are always configured and applied on the input port. You can configure source static entry filters, destination static entry filters, and flow static entry filters. Source static entry filters allow or disallow frames based on their source MAC address; destination static entry filters allow or disallow frames based on their destination MAC address. Flow static entries allow or disallow traffic based on their source *and* destination MAC addresses.
- **Port-to-address locks.** Port-to-address lock filters “lock” a user to a port or set of ports, disallowing them access to other ports.
- **Secure ports.** Secure port filters shut down Layer 2 access to the X-Pedition router from a specific port or drop all Layer 2 packets received by a port. Used by themselves, secure ports secure unused X-Pedition ports. When used in conjunction with static entry filters, secure ports drop all received or sent traffic (depending on the static entry filter) except traffic forced to or from the port by the static entry filter.

## Command Summary

Table 18 lists the **filters** commands. The sections following the table describe the command syntax.

**Table 18. filters Commands**

|  |
|--|
| <b>filters add address-filter</b> name <name> <b>source-mac</b> <MACaddr><br><b>source-mac-mask</b> <MACaddr> <b>dest-mac</b> <MACaddr> <b>dest-mac-mask</b> <MACaddr><br><b>vlan</b> <VLAN-num> <b>in-port-list</b> <port-list>   |
| <b>filters add port-address-lock</b> name <name> <b>source-mac</b> <MACaddr> <b>vlan</b> <VLAN-num><br><b>in-port-list</b> <port-list>   |
| <b>filters add secure-port</b> name <name> <b>direction</b> source destination <b>vlan</b> <VLAN-num><br><b>in-port-list</b> <port-list>   |
| <b>filters add static-entry</b> name <name> <b>restriction</b> allow disallow <br><b>force</b> <b>source-mac</b> <MACaddr> <b>source-mac-mask</b> <MACaddr> <b>dest-mac</b> <MACaddr><br><b>dest-mac-mask</b> <MACaddr> <b>vlan</b> <VLAN-num> <b>in-port-list</b> <port-list><br><b>out-port-list</b> <port-list> |
| <b>filters show address-filter</b> [all-source all-destination all-flow]<br>[ <b>source-mac</b> <MACaddr> <b>dest-mac</b> <MACaddr>] [ <b>ports</b> <port-list>][ <b>vlan</b> <VLAN-num>]  |
| <b>filters show port-address-lock</b> <b>ports</b> [ports <port-list>] [ <b>vlan</b> <VLAN-num>]<br>[ <b>source-mac</b> <MACaddr>]   |
| <b>filters show secure-port</b>  |
| <b>filters show static-entry</b> [all-source all-destination all-flow] <b>ports</b> <port-list><br><b>vlan</b> <VLAN-num> [ <b>source-mac</b> <MACaddr> <b>dest-mac</b> <MACaddr>]   |

# filters add address-filter

## Purpose

Applies an address filter.

## Format

```
filters add address-filter name <name> source-mac <MACaddr>
source-mac-mask <MACaddr> dest-mac <MACaddr> dest-mac-mask <MACaddr>
vlan <VLAN-num> in-port-list <port-list>
```

## Mode

Configure.

## Description

The **filters add address-filter** command blocks traffic based on a frame's source MAC address (**source-mac**), destination MAC address (**dest-mac**), or a flow (specified using both a source MAC address and a destination MAC address).

## Parameters

|                                  |   |
|----------------------------------|---|
| <b>name</b> <name>               | Specifies the name of the filter. Must be less than 25 characters.                                  |
| <b>source-mac</b> <MACaddr>      | Specifies the source MAC address. Use this option for source or flow address filters.               |
| <b>source-mac-mask</b> <MACaddr> | Specifies the source MAC Mask address. Use this option for source or flow address filters.          |
| <b>dest-mac</b> <MACaddr>        | Specifies the destination MAC address. Use this option for destination or flow address filters.     |
| <b>dest-mac-mask</b> <MACaddr>   | Specifies the destination MAC Mask address. Use this option for destination or flow static entries. |
| <b>vlan</b> <VLAN-num>           | Specifies the VLAN.   |
| <b>in-port-list</b> <port-list>  | Specifies the ports to which you want to apply the filter.  |

## Restrictions

You should apply flow filters (specified using both a source MAC address and a destination MAC address) only to ports that are using flow-based bridging.

# filters add port-address-lock

## Purpose

Applies a port address lock.

## Format

**filters add port-address-lock name** <name> **source-mac** <MACaddr> **vlan** <VLAN-num>  
**in-port-list** <port-list>

## Mode

Configure.

## Description

The **filters add port-address-lock** command locks a user (identified by the user's MAC address) to a specific port or set of ports. The source MAC address will be allowed to reach only those stations and other ports that are connected to a port specified by **in-port-list**.

## Parameters

|                                    |  |
|------------------------------------|--|
| <b>name</b> <name>                 | Specifies the name of the lock filter. This parameter must be less than 25 characters. |
| <b>source-mac</b><br><MACaddr>     | Specifies the source MAC address.  |
| <b>vlan</b> <VLAN-num>             | Specifies the VLAN.  |
| <b>in-port-list</b><br><port-list> | Specifies the ports to which you want to apply the lock.                               |

## Restrictions

None.

# filters add secure-port

## Purpose

Applies a port security filter.

## Format

**filters add secure-port** **name** <name> **direction** source|destination **vlan** <VLAN-num>  
**in-port-list** <port-list>

## Mode

Configure.

## Description

The **filters add secure-port** command shuts down Layer 2 access to the X-Pedition router from the ports specified by **in-port-list**. The X-Pedition router drops all traffic received from these ports.

**Note:** You can use port-to-address lock filters to force traffic to a port secured by the **filters add secure-port** command.

## Parameters

|   |   |
|---|---|
| <b>name</b> <name>                            | Specifies the name of the filter. This parameter must be less than 25 characters. |
| <b>direction</b><br><b>source destination</b> | Specifies whether the filter is to secure a source port or a destination port.    |
| <b>vlan</b> <VLAN-num>                        | Specifies the VLAN.   |
| <b>in-port-list</b> <port-list>               | Specifies the ports to which you want to apply the filter.                        |

## Restrictions

None.

# filters add static-entry

## Purpose

Applies a static entry.

## Format

```
filters add static-entry name <name> restriction allow|disallow|force source-mac <MACaddr>  
source-mac-mask <MACaddr> dest-mac <MACaddr> dest-mac-mask <MACaddr>  
vlan <VLAN-num> in-port-list <port-list> out-port-list <port-list>
```

## Mode

Configure.

## Description

The **filters add static-entry** command allows, disallows, or forces traffic to go to a set of destination ports based on a frame's source MAC address (**source-mac**), destination MAC address (**dest-mac**), or a flow (specified using both a source MAC address and a destination MAC address).

## Parameters

|   |  |   |
|---|--|---|
| <b>name</b> <name>                                | Specifies the name of the static-entry filter. This parameter must be less than 25 characters.     |   |
| <b>restriction</b><br><b>allow disallow force</b> | Specifies the forwarding behavior of the static entry, which can be one of the following keywords: |   |
|   | <b>allow</b>   | Allows packets to go to the set of ports specified by out-port-list.  |
|   | <b>disallow</b>  | Prohibits packets from going to the set of ports specified by out-port-list.  |
|   | <b>force</b>   | Forces packets to go to the set of ports specified by out-port-list, despite any port locks in effect on the ports. |
| <b>source-mac</b><br><MACaddr>                    | Specifies the source MAC address. Use this option for source or flow static entries.               |   |
| <b>source-mac-mask</b><br><MACaddr>               | Specifies the source MAC address. Use this option for source or flow static entries.               |   |
| <b>dest-mac</b><br><MACaddr>                      | Specifies the destination MAC address. Use this option for destination or flow static entries.     |   |

---

|                                     |  |
|-------------------------------------|--|
| <b>dest-mac-mask</b><br><MACaddr>   | Specifies the destination MAC address. Use this option for destination or flow static entries. |
| <b>vlan</b> <VLAN-num>              | Specifies the VLAN.  |
| <b>in-port-list</b><br><port-list>  | Specifies the ports to which you want to apply the static entry.                               |
| <b>out-port-list</b><br><port-list> | Specifies the ports to which you are allowing, disallowing, or forcing packets.                |

---

## Restrictions

You should apply flow filters (specified using both a source MAC address and a destination MAC address) only to ports that are using flow-based bridging.

## filters show address-filter

### Purpose

Displays the address filters.

### Format

```
filters show address-filter [all-source|all-destination|all-flow]  
[source-mac <MACaddr> dest-mac <MACaddr>] [ports <port-list>] [vlan <VLAN-num>]
```

### Mode

Enable.

### Description

The **filters show address-filter** command displays the address filters currently configured on the X-Pedition router.

### Parameters

|  |   |
|--|---|
| <b>all-source</b><br><b>all-destination</b><br><b>all-flow</b> | Specifies the types of filters you want to display.   |
| <b>source-mac</b><br><MACaddr>                                 | Restricts the display to only those address filters that have been applied to this source MAC address.      |
| <b>dest-mac</b><br><MACaddr>                                   | Restricts the display to only those address filters that have been applied to this destination MAC address. |
| <b>ports</b><br><port-list>                                    | Restricts the display to only those address filters that have been applied to the specified ports.          |
| <b>vlan</b> <VLAN-num>   | Restricts the display to only those address filters that have been applied to the specified VLANs.          |

### Restrictions

None.



# filters show port-address-lock

## Purpose

Display the port address locks.

## Format

```
filters show port-address-lock [ports <port-list>] [vlan <VLAN-num>]  
[source-mac <MACaddr>]
```

## Mode

Enable.

## Description

The **filters show port-address-lock** command displays the port-address-lock filters currently configured on the X-Pedition router.

## Parameters

|                                |   |
|--------------------------------|---|
| <b>ports</b> <port-list>       | Restricts the display to only those port address locks that have been applied to the specified ports.     |
| <b>vlan</b> <VLAN-num>         | Restricts the display to only those port address locks that have been applied to the specified VLANs.     |
| <b>source-mac</b><br><MACaddr> | Restricts the display to only those port address locks that have been applied to this source MAC address. |

## Restrictions

None.

## **filters show secure-port**

### **Purpose**

Display the port security filters.

### **Format**

**filters show secure-port**

### **Mode**

Enable.

### **Description**

The **filters show secure-port** command displays the secure-port filters currently configured on the X-Pedition router.

### **Parameters**

None.

### **Restrictions**

None.

# filters show static-entry

## Purpose

Displays the static entry filters.

## Format

**filters show static-entry** [**all-source**|**all-destination**|**all-flow**] **ports** <port-list>  
**vlan** <VLAN-num> [**source-mac** <MACaddr> **dest-mac** <MACaddr>]

## Mode

Configure.

## Description

The **filters show static-entry** command displays the static-entry filters currently configured on the X-Pedition router.

## Parameters

|  |  |
|--|--|
| <b>all-source</b>  <br><b>all-destination</b>  <br><b>all-flow</b> | Specifies the types of static entries you want to display.   |
| <b>ports</b><br><port-list>  | Restricts the display to only those static entries that have been applied to the specified ports.          |
| <b>vlan</b> <VLAN-num>   | Restricts the display to only those static entries that have been applied to the specified VLANs.          |
| <b>source-mac</b><br><MACaddr>                                     | Restricts the display to only those static entries that have been applied to this source MAC address.      |
| <b>dest-mac</b><br><MACaddr>                                       | Restricts the display to only those static entries that have been applied to this destination MAC address. |

## Restrictions

None.



# Chapter 24

## frame-relay Commands

The **frame-relay** commands allow you to define frame relay service profiles, and specify and monitor frame relay High-Speed Serial Interface (HSSI) and standard serial ports.

### Command Summary

[Table 19](#) lists the **frame-relay** commands. The sections following the table describe the command syntax.

**Table 19. frame-relay Commands**

|  |
|--|
| <b>frame-relay apply service</b> <i>&lt;service name&gt;</i> <b>ports</b> <i>&lt;port list&gt;</i>   |
| <b>frame-relay clear stats-counter</b> [ <b>frame-drop-qdepth-counter</b> ]<br>[ <b>max-frame-enqueued-counter</b> ] [ <b>frame-drop-red-counter</b> ] [ <b>rmon</b> ] <b>ports</b> <i>&lt;port list&gt;</i>   |
| <b>frame-relay create vc</b> <i>&lt;port&gt;</i>   |
| <b>frame-relay define service</b> <i>&lt;service name&gt;</i> [ <b>Bc</b> <i>&lt;number&gt;</i> ] [ <b>Be</b> <i>&lt;number&gt;</i> ]<br>[ <b>becn-adaptive-shaping</b> <i>&lt;number&gt;</i> ] [ <b>cir</b> <i>&lt;number&gt;</i> ] [ <b>high-priority-queue-depth</b> <i>&lt;number&gt;</i> ]<br>[ <b>low-priority-queue-depth</b> <i>&lt;number&gt;</i> ] [ <b>med-priority-queue-depth</b> <i>&lt;number&gt;</i> ] [ <b>red on off</b> ]<br>[ <b>red-maxTh-high-prio-traffic</b> <i>&lt;number&gt;</i> ] [ <b>red-maxTh-low-prio-traffic</b> <i>&lt;number&gt;</i> ]<br>[ <b>red-maxTh-med-prio-traffic</b> <i>&lt;number&gt;</i> ] [ <b>red-minTh-high-prio-traffic</b> <i>&lt;number&gt;</i> ]<br>[ <b>red-minTh-low-prio-traffic</b> <i>&lt;number&gt;</i> ] [ <b>red-minTh-med-prio-traffic</b> <i>&lt;number&gt;</i> ]<br>[ <b>de-mark on off</b> ] |
| <b>frame-relay set fr-encaps-bgd</b> <b>ports</b> <i>&lt;port list&gt;</i>   |
| <b>frame-relay set lmi</b> [ <b>error-threshold</b> <i>&lt;number&gt;</i> ] [ <b>full-enquiry-interval</b> <i>&lt;number&gt;</i> ]<br>[ <b>monitored-events</b> <i>&lt;number&gt;</i> ] [ <b>polling-interval</b> <i>&lt;number&gt;</i> ] [ <b>state enable disable</b> ]<br>[ <b>type ansi617d-1994 q933a rev1</b> ] <b>ports</b> <i>&lt;port list&gt;</i>  |
| <b>frame-relay set payload-compress</b> [ <b>type frf9_model1_stac</b> ] <b>ports</b> <i>&lt;port list&gt;</i>   |
| <b>frame-relay set peer-addr</b> [ <b>ip-address</b> <i>&lt;IP address&gt;</i> ] [ <b>ipx-address</b> <i>&lt;ipx address&gt;</i> ]<br>[ <b>ports</b> <i>&lt;port list&gt;</i> ]  |

**Table 19. frame-relay Commands (Continued)**

|  |
|--|
| <b>frame-relay show service</b> <i>&lt;service name&gt;</i> <b> all</b>  |
| <b>frame-relay show stats ports</b> <i>&lt;port name&gt;</i> [ <b>last-error</b> ] [ <b>lmi</b> ] [ <b>mibII</b> ] |
| <b>frame-relay show stats ports</b> <i>&lt;port name&gt;</i> <b>summary</b>  |

# frame-relay apply service ports

## Purpose

Apply a pre-defined service profile to a frame relay virtual circuit (VC).

## Format

**frame-relay apply service** <service name> **ports** <port list>

## Mode

Configure.

## Description

Issuing the **frame-relay apply service** command allows you to apply a previously defined service profile to a given frame relay VC.

## Parameters

|                |   |
|----------------|---|
| <service name> | The name of the previously defined service profile you wish to apply to the given port(s) or interfaces.                              |
| <port list>    | The port(s) to which you wish to apply the pre-defined service profile. You can specify a single VC or a comma-separated list of VCs. |

## Restrictions

Usage is restricted to frame relay VCs only.

## Example

To apply the service “s1” to slot 2, VC 100 on serial ports 1 and 2:

```
xp(config)# frame-relay apply service s1 ports se.2.1.100,se.2.2.100
```

# frame-relay clear stats-counter

## Purpose

Clears the specified statistics counter.

## Format

**frame-relay clear stats-counter** [**frame-drop-qdepth-counter**] [**max-frame-enqueued-counter**]  
[**frame-drop-red-counter**] [**rmon**] **ports** <port list>

## Mode

Enable.

## Description

The **frame-relay clear stats-counter** command allows you to specify a particular statistic counter and have those statistics reset to zero. There are statistic counters on each WAN port, and you can use the **frame-relay clear stats-counter** to clear the counter for an individual WAN port or for a group of ports.

## Parameters

|                                   |  |
|-----------------------------------|--|
| <b>frame-drop-qdepth-counter</b>  | Specify this optional parameter to reset the frame drop counter to zero.         |
| <b>max-frame-enqueued-counter</b> | Specify this optional parameter to reset the max enqueuedframes counter to zero. |
| <b>frame-drop-red-counter</b>     | Specify this optional parameter to reset the packet drop counter to zero.        |
| <b>rmon</b>                       | Specify this optional parameter to reset the rmon counter to zero.               |
| <port list>                       | The WAN port(s) that you wish to clear the counter.                              |

## Restrictions

Usage is restricted to WAN ports only.



## Example

To clear the frame drop counter to zero on WAN port hs.3.1:

```
xp# frame-relay clear stats-counter frame-drop-qdepth-counter port hs.3.1
```

# frame-relay create vc

## Purpose

Create frame relay virtual circuits (VCs).

## Format

**frame-relay create vc** <port>

## Mode

Configure.

## Description

The **frame-relay create vc** command allows you to create a frame-relay virtual circuit on a slot and port location specified in the command line.

## Parameters

|              |   |
|--------------|---|
| <hr/>        |   |
| <port>       | The port on which you wish to create a frame relay virtual circuit. Specify the port in the following format: <b>media.slot.port.dlci</b> . |
| <b>media</b> | Is the media type.  |
| <b>slot</b>  | Is the slot number where the module is installed.   |
| <b>port</b>  | Is the port number.   |
| <b>dlci</b>  | Is the Data Link Connection Identifier. Specify any number between 16-1007.   |
| <hr/>        |   |

## Restrictions

Usage is restricted to frame relay ports only.

## Example

To create a frame relay virtual circuit with a DLCI of 100 on serial port 1 of slot 3:

```
xp(config)# frame-relay create vc port se.3.1.100
```

# frame-relay define service

## Purpose

Configure service profiles for frame relay ports.

## Format

```
frame-relay define service <service name> [Bc <number>] [Be <number>]  
[becn-adaptive-shaping <number>] [cir <number>] [high-priority-queue-depth <number>]  
[low-priority-queue-depth <number>] [med-priority-queue-depth <number>] [red on|off]  
[red-maxTh-high-prio-traffic <number>] [red-maxTh-low-prio-traffic <number>]  
[red-maxTh-med-prio-traffic <number>] [red-minTh-high-prio-traffic <number>]  
[red-minTh-low-prio-traffic <number>] [red-minTh-med-prio-traffic <number>]  
[de-mark on|off]
```

## Mode

Configure.

## Description

The **frame-relay define service** command allows you to specify the following attributes for a newly created service profile:

- Number of bits per second contained in a committed burst for frame relay virtual circuits.
- Number of bits per second contained in an excessive burst for frame relay virtual circuits.
- Whether or not to simultaneously enable and specify the threshold at which adaptive shaping will activate when receiving BECN frames
- The committed information rate (in bits per second) for frame relay virtual circuits.
- The allowable queue depth for high-, low-, and medium-priority frames on frame relay VCs.
- Activation or deactivation of Random Early Discard (RED) for frame relay circuits.
- The maximum and minimum threshold values for RED high-, low-, and medium-priority traffic.

In general, Enterasys recommends that the maximum threshold values be less than or equal to the respective high-, low-, or medium-priority queue depth. The minimum threshold values should be one-third of the respective maximum threshold.

## Parameters

---

|                |   |
|----------------|---|
| <service name> | The name you wish to assign to the newly created service profile. |
|----------------|---|

---

|   |  |
|---|--|
| <b>Bc</b> <number>                          | The number of bits per second contained in a committed burst for a frame relay virtual circuit. You can specify a number between 1 and 2,147,483,646 bits per second.                                      |
| <b>Be</b> <number>                          | The number of bits per second contained in an excessive burst for a frame relay virtual circuit. You can specify a number between 1 and 2,147,483,646 bits per second.                                     |
| <b>becn-adaptive-shaping</b> <number>       | The threshold (number of frames) at which adaptive shaping will activate when receiving BECN frames. You can specify a number between 1 and 100,000 frames.  |
| <b>cir</b> <number>                         | The committed information rate (in bits per second) for frame relay virtual circuits. You can specify a number between 1 and 2,147,483,646 bits.   |
| <b>high-priority-queue-depth</b> <number>   | The number of high-priority frames allowed in the frame relay queue. You can specify a number between 1 and 65,535. Enterasys recommends a value within the 5 - 100 item range. The default value is 20.   |
| <b>low-priority-queue-depth</b> <number>    | The number of low-priority frames allowed in the frame relay queue. You can specify a number between 1 and 65,535. Enterasys recommends a value within the 5 - 100 item range. The default value is 20.    |
| <b>med-priority-queue-depth</b> <number>    | The number of medium-priority frames allowed in the frame relay queue. You can specify a number between 1 and 65,535. Enterasys recommends a value within the 5 - 100 item range. The default value is 20. |
| <b>red on off</b>                           | Specifying the <b>on</b> keyword enables RED for frame relay ports. Specifying the <b>off</b> keyword disables RED for frame relay ports.  |
| <b>red-maxTh-high-prio-traffic</b> <number> | The maximum allowable number of frames for high-priority RED traffic. You can specify a number between 1 and 65,535. The default value is 12.  |
| <b>red-maxTh-low-prio-traffic</b> <number>  | The maximum allowable number of frames for low-priority RED traffic. You can specify a number between 1 and 65,535. The default value is 12.   |
| <b>red-maxTh-med-prio-traffic</b> <number>  | The maximum allowable number of frames for medium-priority RED traffic. You can specify a number between 1 and 65,535. The default value is 12.  |
| <b>red-minTh-high-prio-traffic</b> <number> | The minimum allowable number of frames for high-priority RED traffic. You can specify a number between 1 and 65,535. The default value is 4.   |
| <b>red-minTh-low-prio-traffic</b> <number>  | The minimum allowable number of frames for low-priority RED traffic. You can specify a number between 1 and 65,535. The default value is 4.  |
| <b>red-minTh-med-prio-traffic</b> <number>  | The minimum allowable number of frames for medium-priority RED traffic. You can specify a number between 1 and 65,535. The default value is 4.   |
| <b>de-mark on off</b>                       | Specifying the <b>on</b> keyword enables DE marking for best traffic. Specifying the <b>off</b> keyword disables DE marking for best traffic. Default is <b>off</b> .                                      |

## Restrictions

When defining a value for **Bc**, you *must* also be sure to define an appropriate value for **cir**, and vice-versa.

## Examples

Suppose you wish to specify a frame relay virtual circuit with the following attributes:

- Committed burst value of 35 million and excessive burst value of 30 million
- BECN active shaping at 65 thousand frames
- Committed information rate (CIR) of 120 million bits per second
- Leave high-, low-, and medium-priority queue depths set to factory defaults
- Random Early Discard (RED) disabled

The command line necessary to set up a service profile with the above attributes would be as follows:

```
xp(config)# frame-relay define service profile1 Bc 35000000 Be 30000000 becn-adaptive-shaping
65000 cir 120000000 red off
```

## frame-relay set fr-encaps-bgd

### Purpose

Force the ingress packets to be encapsulated in bridged format.

### Format

**frame-relay set fr-encaps-bgd ports** *<port list>*

### Mode

Configure.

### Description

Issuing the **frame-relay set fr-encaps-bgd** command allows you to use bridged format encapsulation on a given frame relay VC.

### Parameters

|                          |   |
|--------------------------|---|
| <i>&lt;port list&gt;</i> | The port(s) to which you wish to use bridged encapsulation. You can specify a single VC or a comma-separated list of VCs. |
|--------------------------|---|

### Restrictions

Usage is restricted to frame relay VCs only.

### Example

To force the bridged encapsulation to slot 2, VC 100 on serial ports 1 and 2:

```
xp(config)# frame-relay set fr-encaps-bgd ports se.2.1.100,se.2.2.100
```

# frame-relay set lmi

## Purpose

Set frame relay Local Management Interface (LMI) parameters.

## Format

```
frame-relay set lmi [error-threshold <number>] [full-enquiry-interval <number>]  
[monitored-events <number>] [polling-interval <number>] [state enabled|disabled]  
[type ansi617d-1994|q933a|rev1] ports <port list>
```

## Mode

Configure.

## Description

The **frame-relay set lmi** command allows you to specify the following attributes:

- The number of times the router will attempt to poll an LMI interface before declaring it down. You can define a value between 1 and 10, inclusive.
- The number of status enquiries that will be sent before a full status enquiry is requested. You can define a value between 1 and 255, inclusive.
- The number of status enquiries over which various pieces of LMI information can be collected and tabulated. For example, you can tabulate the number of times an interface was declared down/lost due to a lack of proper responses to status enquiries. You can define a value between 1 and 10, inclusive.
- The number of seconds that pass between successive status enquiry messages. You can define a value between 5 and 30, inclusive.
- Whether or not LMI messages are sent. LMI messages are not sent by default.
- The LMI type for frame relay WAN ports.

## Parameters

|  |   |
|--|---|
| <b>error-threshold</b><br><number>       | The number of unanswered status enquiries that the router will make before declaring an interface to be down.   |
| <b>full-enquiry-interval</b><br><number> | The number of status enquiries that will be sent before a full report on status is compiled and transmitted.  |
| <b>monitored-events</b><br><number>      | The number of status enquiries over which collection and tabulation of various pieces of LMI information will take place.   |
| <b>polling-interval</b><br><number>      | The amount of time (in seconds) that will pass before a subsequent status enquiry takes place.  |
| <b>state</b><br><b>enabled disabled</b>  | Enables the sending and receiving of LMI messages. If LMI messages are enabled, the operational status of each VC is determined by the LMI messages. If LMI messages are disabled, each VC is assumed to be operationally “up”. LMI messages are disabled by default. |
| <b>type ansi617d-1994 q933a rev1</b>     | The LMI type for frame relay WAN ports. You can only specify the <b>ansi617d-1994</b> , <b>q933a</b> , or <b>rev1</b> keywords to define as the LMI type for WAN ports.   |
| <b>ports</b> <port list>                 | The port or ports that will assume the LMI service profile behavior.  |

## Restrictions

None.

## Example

To set the number of status enquiries that will be sent before compilation and transmission of a full status report for serial port 2 of slot 2 to 75 enquiries:

```
xp(config)# frame-relay set lmi full-enquiry-interval 75 ports se.2.2
```



# frame-relay set payload-compress

## Purpose

Enable packet compression for frame-relay ports.

## Format

**frame-relay set payload-compress** [**type frf9\_mode1\_stac**] **ports** <port list>

## Mode

Configure.

## Description

The **frame-relay set payload-compress** command allows you to enable packet compression according to Mode 1 of FRF 9. If this command is not configured, packet compression is not enabled.

## Parameters

|                             |   |
|-----------------------------|---|
| <b>type frf9_mode1_stac</b> | Specifies the Stacker FRF 9, Mode 1 compression algorithm. This is the default value.   |
| <port list>                 | The port(s) on which you wish to enable the packet compression. You can specify a single VC or a comma-separated list of VCs. |

## Restrictions

Usage is restricted to frame relay VCs only.

## Example

To enable Stacker FRF 9, Mode 1 packet compression on slot 3, VC 300 on serial port 1:

```
xp(config)# frame-relay set payload-compress ports se.3.1.300
```

# frame-relay set peer-addr

## Purpose

Set the peer address in case that InArp is not supported on the remote device.

## Format

**frame-relay set peer-addr** [**ip-address** <IP address>] [**ipx-address** <IPX address>]  
[**ports** <port list>]

## Mode

Configure.

## Description

Issuing the **frame-relay set peer-addr** command allows you to set the peer address if it cannot be resolved by InArp.

## Parameters

|               |   |
|---------------|---|
| <IP address>  | The IP address you wish to use.                                   |
| <IPX address> | The IPX address you wish to use.                                  |
| <port list>   | The location of the port to which you wish to assign the address. |

## Restrictions

Usage is restricted to frame relay VCs only.

## Example

To assign an IP address 10.1.1.1/16 to slot 2, VC 100 on serial port 1:

```
xp(config)# frame-relay set peer-addr ip-address 10.1.1.1/16 ports se.2.1.100
```

# frame-relay show service

## Purpose

Displays frame relay service profiles.

## Format

**frame-relay show service** <service name>/all

## Mode

Enable.

## Description

The **frame-relay show service** command allows you to display the available frame relay service profiles.

## Parameters

|                |   |
|----------------|---|
| <service name> | The name of a particular pre-defined service profile.       |
| <b>all</b>     | Displays all of the available frame relay service profiles. |

## Restrictions

None.

## Example

To display the available frame relay service profiles named “prof1”:

```
xp# frame-relay show service prof1
```

# frame-relay show stats

## Purpose

Displays frame relay statistics.

## Format

**frame-relay show stats ports** <port name> [**last-error**] [**lmi**] [**mibII**]

## Mode

Enable.

## Description

The **frame-relay show stats** command allows you to display the following frame relay port statistics for the given port:

- The last reported frame relay error.
- The active frame relay LMI parameters.
- The MIBII statistics for frame relay WAN ports.

## Parameters

|                          |  |
|--------------------------|--|
| <b>ports</b> <port name> | Port or ports for which you want to display statistics.          |
| <b>last-error</b>        | Displays the last reported frame relay error for the given port. |
| <b>lmi</b>               | Displays the active frame relay LMI parameters.                  |
| <b>mibII</b>             | Displays the MIBII statistics for frame relay WAN ports.         |

## Restrictions

The **last-error**, **mibII**, and **lmi** commands are for ports only (no VC designators allowed). Otherwise, the port name may have the “VC” designator.

## Examples

To display the last recorded error and MIB II statistics and for serial port 1 of slot 3:

```
xp# frame-relay show stats ports se.3.1 last-error mibII
```

To display the VC statistics for serial port 1, slot 3, VCs 1-10:

```
xp# frame-relay show stats ports se.3.1.1-10
```

## frame-relay show stats summary

### Purpose

Displays a summary of all VC statistics.

### Format

**frame-relay show stats summary ports** *<port name>*

### Mode

Enable.

### Description

The **frame-relay show stats summary** command allows you to display all of the summary information for VC statistics.

### Parameters

---

|                          |   |
|--------------------------|---|
| <i>&lt;port name&gt;</i> | The port or ports for which you wish to display summary statistics. |
|--------------------------|---|

---

### Restrictions

None.

### Example

To display summary statistics for serial port 1 of slot 4, VC 100:

|  |
|--|
| xp# <b>frame-relay show stats summary ports se.4.1.100</b> |
|--|

# Chapter 25

## garp Commands

The following commands allow you to set and show the GARP timers.

### Command Summary

[Table 20](#) lists the **garp** commands. The sections following the table describe the command syntax.

**Table 20. garp Commands**

|   |
|---|
| <b>garp set timers</b> <i>&lt;port-list&gt;</i> <b>join</b> <i>&lt;num&gt;</i>   <b>leave</b> <i>&lt;num&gt;</i>   <b>leaveall</b> <i>&lt;num&gt;</i> |
| <b>garp show timers</b> <i>&lt;port-list&gt;</i>   <b>all-ports</b>   |

## garp set timers

### Purpose

Sets the values of GARP timers.

### Format

**garp set timers** <port-list> **join** <num> / **leave** <num> / **leaveall** <num>

### Mode

Configure.

### Description

The **garp set timers** command allows setting of GARP join, leave, and leaveall timers for specified port(s).

### Parameters

|                         |   |
|-------------------------|---|
| <b>port</b> <port-list> | Specifies ports for which to display GARP timer values.                             |
| <b>join</b> <num>       | Sets join timer to value specified. Value must fall between 20 and 1000 cs.         |
| <b>leave</b> <num>      | Sets leave timer to value specified. Value must fall between 60 and 3000 cs.        |
| <b>leaveall</b> <num>   | Sets leave all timer to value specified. Value must fall between 1000 and 18000 cs. |

### Restrictions

Timers should satisfy the following relationship: **Leave** >= **Join**\*3, and **LeaveAll** > **Leave**.

### Example

To set GARP timers for port et.1.1:

```
xp# garp set timers et.1.1 join 1000 leave 2500 leaveall 18000
```



# garp show timers

## Purpose

Display values of GARP timers.

## Format

**garp show timers** *<port-list>* | **all-ports**

## Mode

Enable.

## Description

The **garp show timers** command allows display of the values of the GARP join timer, leave timer, and leaveall timer for specified port(s).

## Parameters

|                          |   |
|--------------------------|---|
| <i>&lt;port-list&gt;</i> | Specifies port(s) for which to display GARP timer values. |
| <b>all-ports</b>         | Displays timer values for every port.                     |

## Restrictions

None.

## Example

To display values of GARP timers for port et.1.1:

```
er# garp show timers et.1.1
```



# Chapter 26

## gvrp Commands

The following commands allow you to display and alter GVRP parameters on the X-Pedition router.

### Command Summary

[Table 21](#) lists the **gvrp** commands. The sections following the table describe the command syntax.

**Table 21. gvrp Commands**

|  |
|--|
| <b>gvrp show statistics</b> <i>&lt;port-list&gt;</i>   <b>all ports</b>                            |
| <b>gvrp show status</b>  |
| <b>gvrp show registration-mode</b> <i>&lt;port-list&gt;</i>   <b>all-ports</b>                     |
| <b>gvrp show applicant-status</b> <i>&lt;port-list&gt;</i>   <b>all-ports</b>                      |
| <b>gvrp clear statistics</b> <i>&lt;port-list&gt;</i>   <b>all-ports</b>                           |
| <b>gvrp enable dynamic-vlan-creation</b>   |
| <b>gvrp enable ports</b> <i>&lt;port-list&gt;</i>  |
| <b>gvrp set registration-mode forbidden ports</b> <i>&lt;port-list&gt;</i>   <b>all-ports</b>      |
| <b>gvrp set applicant status non-participant ports</b> <i>&lt;port-list&gt;</i>   <b>all-ports</b> |
| <b>gvrp start</b>  |

## **gvrp show statistics**

### **Purpose**

Displays various GVRP statistics for ports.

### **Format**

**gvrp show statistics** *<port-list>* | **all ports**

### **Mode**

Enable.

### **Description**

The **gvrp show statistics** command displays statistics for the specified port(s).

### **Parameters**

None.

### **Restrictions**

None.

### **Example**

```
gvrp show statistics et.1.1-2
```

# **gvrp show status**

## **Purpose**

Shows status of GVRP.

## **Format**

**gvrp show status**

## **Mode**

Enable.

## **Description**

The **gvrp show status** command displays current status of GVRP.

## **Parameters**

None.

## **Restrictions**

None.

## **Example**

```
gvrp show status
```

## gvrp show registration-mode

### Purpose

Shows GVRP registration-mode for specified port(s).

### Format

**gvrp show registration-mode ports** *<port-list>* | **all-ports**

### Mode

Enable.

### Description

The **gvrp show registration-mode** command displays the GVRP registration-mode of specified port(s).

### Parameters

|                          |   |
|--------------------------|---|
| <i>&lt;port-list&gt;</i> | Specifies port(s) for which information will display. |
| <b>all-ports</b>         | Displays information for all X-Pedition ports.        |

### Restrictions

None.

### Example

```
gvrp show registration-mode ports et.1.1-2
```

# gvrp show applicant-status

## Purpose

Shows GVRP applicant-status for specified port(s).

## Format

**gvrp show registration-mode ports** <port-list> | **all-ports**

## Mode

Enable.

## Description

The **gvrp show applicant-status** command displays the GVRP applicant-status of specified port(s).

## Parameters

|                  |   |
|------------------|---|
| <port-list>      | Specifies port(s) for which information will display. |
| <b>all-ports</b> | Displays information for all X-Pedition ports.        |

## Restrictions

None.

## Example

gvrp show registration-mode ports et.1.1-2

## gvrp clear statistics

### Purpose

Clears GVRP statistics for specified port(s).

### Format

**gvrp clear statistics** *<port-list>* | **all-ports**

### Mode

Enable.

### Description

The **gvrp clear statistics** command clears GVRP statistics for specified port(s).

### Parameters

|                          |   |
|--------------------------|---|
| <i>&lt;port-list&gt;</i> | Specifies port(s) for which statistics will be cleared. |
| <b>all-ports</b>         | Clears statistics on all X-Pedition ports.              |

### Restrictions

None.

### Example

```
gvrp clear statistics et.1.1-2
```



# **gvrp enable dynamic-vlan-creation**

## **Purpose**

Allows GVRP to dynamically create VLANs.

## **Format**

**gvrp enable dynamic-vlan-creation**

## **Mode**

Configure.

## **Description**

The **gvrp enable dynamic-vlan-creation** command allows GVRP to dynamically create VLANs on the X-Pedition router. If not enabled, GVRP will continue to propagate VLANs to other network devices; however, VLANs will not be created dynamically.

## **Parameters**

None.

## **Restrictions**

None.

## **Example**

To enable dynamic VLAN creation:

```
xp(config)# gvrp enable dynamic-vlan-creation
```

## gvrp enable ports

### Purpose

Enables GVRP on specified port(s).

### Format

**gvrp enable ports** *<port-list>*

### Mode

Configure.

### Description

The **gvrp enable ports** command enables GVRP on specified port(s).

### Parameters

|                          |  |
|--------------------------|--|
| <i>&lt;port-list&gt;</i> | Specifies port(s) upon which GVRP will be enabled. |
|--------------------------|--|

### Restrictions

None.

### Example

To enable GVRP on ports et.1.1 and et.1.2:

```
xp(config)# gvrp enable ports et.1.1 and et.1.2
```

# gvrp set registration-mode forbidden

## Purpose

Sets GVRP registration-mode for specified port(s).

## Format

**gvrp set registration-mode forbidden ports** *<port-list>* | **all-ports**

## Mode

Configure.

## Description

The **gvrp set registration-mode forbidden** command enables the user to disallow VLAN registration on specified port(s).

**Note:** The system default allows VLAN registration.

## Parameters

|                          |   |
|--------------------------|---|
| <i>&lt;port-list&gt;</i> | Specifies port(s) on which VLAN registration will be forbidden. |
| <b>all-ports</b>         | Forbids VLAN registration on all X-Pedition ports               |

## Restrictions

None.

## Example

To forbid registration on port et.1.1:

```
xp(config)# gvrp registration-mode forbidden ports et.1.1
```

# gvrp set applicant-status non-participant

## Purpose

Sets GVRP applicant-status for specified port(s).

## Format

**gvrp set applicant-status non-participant ports** *<port-list>* | **all-ports**

## Mode

Configure.

## Description

The **gvrp set applicant-status non-participant** command stops GVRP from propagating VLAN information on specified port(s). These port(s) may still create VLANs from other network devices if so configured.

## Parameters

|                          |  |
|--------------------------|--|
| <i>&lt;port-list&gt;</i> | Specifies port(s) on which to halt VLAN propagation. |
| <b>all-ports</b>         | Halts VLAN propagation on all X-Pedition ports       |

## Restrictions

None.

## Example

To set port et.1.1 to a non-participant:

```
xp(config)# gvrp applicant-status non-participant ports et.1.1
```

# **gvrp start**

## **Purpose**

Starts GVRP on the X-Pedition router.

## **Format**

**gvrp start**

## **Mode**

Configure.

## **Description**

The **gvrp start** command enables GVRP.

## **Parameters**

None.

## **Restrictions**

None.

## **Example**

To enable GVRP:

```
xp(config)# gvrp start
```



# Chapter 27

## igmp Commands

The **igmp** commands let you display and set IGMP parameters.

### Command Summary

[Table 22](#) lists the **igmp** commands. The sections following the table describe the command syntax.

**Table 22. igmp Commands**

|   |
|---|
| <b>igmp enable interface</b> <intf>   <b>all</b> [ <b>nosend</b>   <b>query-interval</b> <sec>   <b>robustness</b> <num>]                                   |
| <b>igmp enable vlan</b> <vlan-name>   |
| <b>igmp join group</b> <ipAddr> <b>interface</b> <name/ipAddr>  |
| <b>igmp set</b> [ <b>queryinterval</b> <sec>] [ <b>responsetime</b> <sec>] [ <b>robustness</b> <num>]   |
| <b>igmp set vlan</b> <vlan-name> [ <b>host-timeout</b> <num>] [ <b>querier-timeout</b> <num>]<br>[ <b>router-timeout</b> <num>] <b>leave-timeout</b> <num>] |
| <b>igmp show groups</b> [ <b>to-terminal</b>   <b>to-file</b> ]   |
| <b>igmp show interfaces all</b>  <ipAddr> [ <b>to-terminal</b>   <b>to-file</b> ]   |
| <b>igmp show vlans</b>  |
| <b>igmp start</b>   <b>stop</b>   |
| <b>igmp start-snooping</b>  |
| <b>igmp trace packets</b>   <b>query</b>   <b>report</b>   <b>leave</b>   <b>mtrace</b> [ <b>detail</b> ] [ <b>send</b> ] [ <b>receive</b> ]                |
| <b>igmp trace local-options</b> <option-list>   |

# igmp enable interface

## Purpose

Enables IGMP processing on a specific interface.

## Format

**igmp enable interface** <intf> | **all** [**nosend** | **query-interval** <sec> | **robustness** <num>]

## Mode

Configure.

## Description

The **igmp enable interface** command enables IGMP processing on a specific interface. The parameters you select will apply only to the interface specified.

## Parameters

|                             |  |
|-----------------------------|--|
| <intf>  <b>all</b>          | Specifies the interface on which you are enabling IGMP by IP address or interface name. Use the <b>all</b> keyword to specify all interfaces.  |
| <b>nosend</b>               | Allows the interface to receive—not send—IGMP packets.   |
| <b>query-interval</b> <sec> | Specifies the time (in seconds) between Host Membership Queries on this interface if the router is the Designated Querier for the subnet. The default time is 125 seconds. The range is 11 to 65535.   |
| <b>robustness</b> <num>     | The maximum number of lost packets to allow (2 to 65,535) before ceasing to send additional packets. By default, this value is 2. Each time a port sends out a query and does not receive a response, it counts against the robustness value specified. When the number of lost packets equals the robustness value minus one (robustness - 1), the port will stop sending packets.<br><br><b>Note:</b> Do not enter a 1 for the robustness value. |

## Restrictions

None.



## Example

To enable interface “foo” to receive but not send IGMP packets, the following:

```
xp(config)# igmp enable interface foo nosend
```

To enable interface “foo2” to operate IGMP with a query-interval of 200 and to be robust to 3 packet losses, use the following:

```
xp(config)# igmp enable interface foo2 query-interval 200 robustness 4
```

# igmp enable vlan

## Purpose

Enables IGMP snooping on a VLAN.

## Format

**igmp enable vlan** <vlan-name>

## Mode

Configure.

## Description

The **igmp enable vlan** command enables IGMP snooping on a specified VLAN. By default, IGMP snooping is disabled on all VLANs.

**Note:** The **igmp start-snooping** command must be present for the **igmp enable vlan** command to function properly, and the **igmp start-snooping** command supports IGMP-enabled VLANs only—it is not intended for use with IGMP-enabled interfaces. See *igmp start-snooping* [on page 374](#).

## Parameters

---

|             |   |
|-------------|---|
| <vlan-name> | Is the name of the VLAN where IGMP snooping is to be enabled. |
|-------------|---|

**Note:** The X-Pedition router displays VLAN names up to 32 characters in length.

---

## Restrictions

- Layer 3 multicasting and layer-2 snooping cannot be run simultaneously on the same VLAN.
- Only configured VLANs are allowed to be enabled for igmp snooping. For more information regarding configured VLANs, see *vlan create* [on page 1435](#).

## Example

To enable igmp snooping on VLAN blue:

```
xp(config)# igmp enable vlan blue
```

# igmp join group

## Purpose

Allows you to configure a static IGMP group onto an interface.

## Format

**igmp join group** <ipAddr> **interface** <name/ipAddr>

## Mode

Configure.

## Description

The **igmp join group** command allows an interface to join an IGMP group statically. Most interfaces join IGMP groups dynamically, outside the control of the user. This command configures an IGMP group onto an interface statically.

## Parameters

|                                   |   |
|-----------------------------------|---|
| <b>group</b> <ipAddr>             | Specifies the multicast address.  |
| <b>interface</b><br><name/ipAddr> | Specifies the interface name or IP address.<br><br><b>Note:</b> Enterasys recommends that you use alphabetic characters when defining interface names—purely numeric interfaces will be interpreted as IP addresses. The X-Pedition displays interface names up to 32 characters in length. |

## Restrictions

None.

## Examples

To configure the IGMP group '255.2.0.0' on interface 200.1.1.1:

```
xp(config)# igmp join group 255.2.0.0 interface 200.1.1.1
```

# igmp set

## Purpose

Set router-wide options for IGMP.

## Format

**igmp set** [**queryinterval** <sec>] [**responsetime** <sec>] [**robustness** <num>]

## Mode

Configure.

## Description

The **igmp set** command allows you to set router-wide options for IGMP. These options apply to all interfaces; however, options set through **igmp enable interface** take precedence.

## Parameters

|                            |   |
|----------------------------|---|
| <b>queryinterval</b> <sec> | Specifies the time (in seconds) between Host Membership Queries if the router is the Designated Querier for a subnet. By default, the query interval is 125. The range is 11 to 65535.  |
| <b>responsetime</b> <sec>  | <p>The Max Response Time inserted into the periodic General Queries. The default is 10 seconds. The valid range is 1 to 25.</p> <p>By varying the responsetime, an administrator may tune the burstiness of IGMP messages on the subnet. Larger values make the traffic less bursty, as host responses are spread out over a larger interval. The number of seconds represented by the responsetime must be less than the queryinterval.</p>  |
| <b>robustness</b> <num>    | <p>The Robustness Variable allows tuning for the expected packet loss on a subnet. If a subnet is expected to be lossy, the Robustness Variable may be increased. IGMP is robust to (Robustness Variable-1) packet losses. Default is 2. The valid range is 2 to 65535.</p> <p>Note that the time that must pass after the receipt of the last membership report, before a multicast router decides there are no more members of a group on a network, is equal to (robustness x queryinterval) + responsetime.</p> |

**Note:** Only one parameter can be set at a time.

## Restrictions

None.

## Example

To set the router wide query-interval to 200, and the packet-loss tolerance to 3, enter the following:

```
xp(config)# igmp set queryinterval 200  
xp(config)# igmp set robustness 4
```

# igmp set vlan

## Purpose

Sets parameters for IGMP snooping on a VLAN.

## Format

```
igmp set vlan <vlan-name> [host-timeout <num>] [querier-timeout <num>]  
[router-timeout <num> leave-timeout <num>] [filter-ports <port-list>]  
[permanent-ports <port-list>]
```

## Mode

Configure.

## Description

The **igmp set vlan** command allows you to set parameters for VLAN-based IGMP snooping.

## Parameters

|  |  |
|--|--|
| <b>&lt;vlan-name&gt;</b>                 | The name of the VLAN for which you will set IGMP snooping parameters.<br><br><b>Note:</b> The X-Pedition router displays VLAN names up to 32 characters in length.   |
| <b>host-timeout &lt;num&gt;</b>          | Allows adjusting to long host timeout values that may have been set up for the IGMP querier. The default value is 250 seconds.   |
| <b>querier-timeout &lt;num&gt;</b>       | Allows adjusting to long timeout values that may have been set up for the IGMP querier. The default value is 260 seconds.  |
| <b>router-timeout &lt;num&gt;</b>        | Allows adjusting to long timeout values that may have been set up for the routers. Different versions of DVMRP can have different time outs. The default value is 140 seconds.   |
| <b>leave-timeout &lt;num&gt;</b>         | Allows quicker timeout if IGMP v2 leave messages are used. The value is nominally 10 seconds.  |
| <b>filter-ports &lt;port-list&gt;</b>    | Allows forced filtering of certain ports from multicast data. Setting ports as filter ports ensures that no host there will join any memberships. A port can optionally be either a permanent port or a filter port, but not both. |
| <b>permanent-ports &lt;port-list&gt;</b> | Allows forcing of mulicast data if present on certain ports. A port can optionally be either a permanent port or a filter port, but not both.  |

## Restrictions

None.

## Example

To set parameters for IGMP snooping on the VLAN blue:

```
xp(config)# igmp set vlan blue host-timeout 125 querier-timeout 130 router-timeout 70
```

# igmp show groups

## Purpose

Display IGMP group membership.

## Format

**igmp show groups** [**to-terminal**|**to-file**]

## Mode

Enable.

## Description

Display IGMP group memberships received from subscribers.

## Parameters

|                    |   |
|--------------------|---|
| <b>to-terminal</b> | Displays the information on screen. If you do not specify how to output the information, the X-Pedition router will select the <b>to-terminal</b> option (the default). |
| <b>to-file</b>     | Writes the information to the gated dump file.  |

## Restrictions

None.

## Example

To display IGMP group membership information on screen, enter the following:

```
xp(enable)# igmp show groups
```

To write IGMP group membership to the gated dump file, enter the following:

```
xp(enable)# igmp show groups to-file
```



# igmp show interfaces

## Purpose

Shows the interfaces running IGMP.

## Format

**igmp show interfaces all**|<ipAddr> [**to-terminal**|**to-file**]

## Mode

Enable.

## Description

The **igmp show interfaces** command displays an interface (or all interfaces) by address configured to use the IGMP protocol, along with configured values for the interface.

## Parameters

|                    |  |
|--------------------|--|
| <b>all</b>         | Displays all IGMP interfaces.  |
| <ipAddr>           | Enter the IP address of the specific IGMP interface you wish to display.   |
| <b>to-terminal</b> | Displays the information on screen. If you do not specify how to output the information, the X-Pedition router will select the to-terminal option (the default). |
| <b>to-file</b>     | Writes the information to the gated dump file.   |

## Restrictions

None.

## Example

To display information on screen about a specific IGMP interface, enter the following:

```
xp(enable)# igmp show interfaces 10.250.66.3 to-terminal
```

To write information about all IGMP interfaces to the gated dump file, enter the following:

```
xp(enable)# igmp show interfaces all to-file
```

# igmp show vlans

## Purpose

Displays IGMP VLANs.

## Format

**igmp show vlans** [**detail**] [**name** <name>] [**timers**]

## Mode

Enable.

## Description

The **igmp show vlans** command displays IGMP VLANs.

## Parameters

|                    |   |
|--------------------|---|
| <b>detail</b>      | Shows all IGMP membership information.  |
| <b>name</b> <name> | Shows IGMP membership information for the specified VLAN.<br><br><b>Note:</b> Enterasys recommends that you use alphabetic characters when defining interface names—purely numeric interfaces will be interpreted as IP addresses. The X-Pedition router displays VLAN and interface names up to 32 characters in length. |
| <b>timers</b>      | Shows all IGMP L2 snooping related timers.  |

## Restrictions

None.

## Example

To display IGMP VLAN information, enter the following:

```
xp(enable)# igmp show vlans
Vlan: vlan1          VLAN-ID: 3    Ports: et.9.(1-10)
Group: 226.0.1.1     Ports:et.9.9
Group: 226.0.1.2     Ports:et.9.9
Group: 226.0.1.3     Ports:et.9.9
```

## **igmp start|stop**

### **Purpose**

Enable or disable IGMP protocol processing.

### **Format**

**igmp start|stop**

### **Mode**

Configure.

### **Description**

The **igmp start|stop** command allows you to enable or disable IGMP protocol processing.

### **Parameters**

None.

### **Restrictions**

None.

### **Example**

After entering other igmp commands, enter the following syntax to start IGMP:

|                               |
|-------------------------------|
| xp(enable)# <b>igmp start</b> |
|-------------------------------|

## igmp start-snooping

### Purpose

Starts passive IGMP snooping on enabled VLANs.

### Format

**igmp start-snooping**

### Mode

Configure.

### Description

The **igmp start-snooping** command starts IGMP snooping on enabled VLANs. This task is independent of L3 multicasting.

**Note:** The **igmp start-snooping** command must be present for the **igmp enable vlan** command to function properly, and the **igmp start-snooping** command supports IGMP-enabled VLANs only—it is not intended for use with IGMP-enabled interfaces. See *igmp enable vlan* [on page 364](#).

### Parameters

None.

### Restrictions

None.

# igmp trace

## Purpose

Set IGMP trace options.

## Format

**igmp trace packets|query|report|leave|mtrace [detail] [send] [receive]**

## Mode

Configure.

## Description

The **igmp trace** command allows you to trace IGMP packet processing. When the X-Pedition router sends or receives a packet, the router displays a message to the console.

## Parameters

|                |  |
|----------------|--|
| <b>packets</b> | Trace IGMP packets in general.                         |
| <b>query</b>   | Trace IGMP Query packets.                              |
| <b>report</b>  | Trace IGMP Membership Report packets.                  |
| <b>leave</b>   | Trace IGMP Leave packets.                              |
| <b>mtrace</b>  | Trace mtrace packets.                                  |
| <b>detail</b>  | Show a detailed trace message instead of a brief one.  |
| <b>send</b>    | Show only those packets that are sent from the router. |
| <b>receive</b> | Show only those packets received by the router.        |

## Restrictions

Specify each trace target separately. Instead of **igmp trace query report detail send**, use **igmp trace query detail send** and **igmp trace report detail send**.

## Example

To start tracing Membership Reports sent by the router, use the following:

```
xp(config)# igmp trace report send
```

To trace queries received by the router in detail, enter the following:

```
xp(config)# igmp trace query detail receive
```

# igmp trace local-options

## Purpose

Set gated trace-options specific to IGMP.

## Format

**igmp trace local-options** *<option-list>*

## Mode

Configure.

## Description

The **igmp trace local-options** command allows you to set gated trace options specific to IGMP—these options are inherited from **ip-router global set trace-options** and modified for IGMP.

## Parameters

The following lists the trace options available for *<option-list>*:

|                |  |
|----------------|--|
| <b>all</b>     | Turn on all tracing.   |
| <b>none</b>    | Specifies that all tracing should be turned off for this protocol or peer.                   |
| <b>startup</b> | Trace startup events.  |
| <b>general</b> | Turn on normal and route tracing.  |
| <b>state</b>   | Trace state machine transitions in protocols.  |
| <b>normal</b>  | Trace normal protocol occurrences. The X-Pedition router always traces abnormal occurrences. |
| <b>policy</b>  | Traces the application of policy to imported and exported routes.                            |
| <b>task</b>    | Traces system interfaces and task processing associated with this protocol or peer.          |
| <b>timer</b>   | Traces timer usage by this protocol or peer.   |
| <b>route</b>   | Traces routing table changes for routes installed by this protocol or peer.                  |

## Restrictions

None.

## Example

To trace IGMP timer usage, enter the following:

```
xp(enable)# igmp trace local-options timer
```



# Chapter 28

## interface Commands

The **interface** commands allow the user to create AppleTalk, IPv4, IPv6, and IPX interfaces. They also allow the addition of network mask and broadcast address information to existing IP interfaces, and they display configuration information for AppleTalk, IP, and IPX interfaces.

### Command Summary

[Table 23](#) lists the **interface** commands. The sections following the table describe the command syntax.

**Table 23. interface Commands**

|  |
|--|
| <b>interface add appletalk</b> <InterfaceName> <b>zone</b> <ZoneName> [default]  |
| <b>interface add ip</b> <InterfaceName> <b>address-netmask</b> <IPaddr-mask> [peer-address <IPaddr>] [broadcast <IPaddr>]  |
| <b>interface add ipv6</b> <InterfaceName> <b>address-prefix</b> <address[/prefix-len]> [eui64] [anycast] [peer-address <address>]  |
| <b>interface add ipx</b> <InterfaceName> <b>address</b> <IPXaddr> [peer-address <IPXaddr>] [output-mac-encapsulation <MACencap>]   |
| <b>interface create appletalk</b> <InterfaceName> <b>vlan</b> <name>  <b>port</b> <port> <b>cable-range</b> <range> [zone <ZoneName>] [address <Net.Node>] [up down]   |
| <b>interface create appletalk</b> <InterfaceName> <b>vlan</b> <name>  <b>port</b> <port> <b>noseed</b> [up down]   |
| <b>interface create ip</b> <InterfaceName> <b>address-netmask</b> <IPaddr-mask> [broadcast <IPaddr>] [peer-address <IPaddr>] <b>vlan</b> <name>  <b>port</b> <port> <b>mtu</b> <num> [output-mac-encapsulation <MACencap>] [up down] [mac-addr <MACaddr-spec>] |
| <b>interface create ipv6</b> <InterfaceName> [address-prefix <address[/prefix-len]> [eui64] [anycast] [mtu <num>]] {<PortParameters>   <TunnelParameters>} [up   down]   |

**Table 23. interface Commands (Continued)**

|   |
|---|
| <b>interface create ipx</b> <InterfaceName> <b>address</b> <IPXaddr> <b>peer-address</b> [<IPXaddr>]<br><b>vlan</b> <name>   <b>port</b> <port> [ <b>output-mac-encapsulation</b> <MACencap>] [ <b>up down</b> ]<br>[ <b>mac-addr</b> <MACaddr-spec>] [ <b>mtu</b> <num>] |
| <b>interface show appletalk</b> <InterfaceName>  <b>all</b> [ <b>brief</b> ]  |
| <b>interface show ip</b> <InterfaceName>  <b>all</b> [ <b>brief</b> ]   |
| <b>interface show ipv6</b> {<InterfaceName>   <b>all</b>   <b>tunnels</b> } [ <b>brief</b> ]  |
| <b>interface show ipx</b> <InterfaceName>  <b>all</b> [ <b>brief</b> ]  |

# interface add appletalk

## Purpose

Adds zones to an existing AppleTalk interface.

## Format

**interface add appletalk** <InterfaceName> **zone** <ZoneName> [**default**]

## Mode

ARE-Configure.

## Description

The **interface add appletalk** command configures additional zones for an existing interface.

**Note:** The interface must already exist. To create an interface, enter the **interface create appletalk** command.

## Parameters

|                        |   |
|------------------------|---|
| <InterfaceName>        | Name of the IP interface; for example, int4.<br><br><b>Note:</b> Enterasys recommends that you use alphabetic characters when defining interface names—purely numeric interfaces will be interpreted as IP addresses. The X-Pedition router will display interface names up to 32 characters in length. |
| <b>zone</b> <ZoneName> | Name of the additional zone; for example, “myzone.” Up to 253 zones may be assigned to an interface.  |
| <b>default</b>         | Changes the default zone for the local network attached to the interface. Specified zone name will become the new default zone. If this parameter is not used, the default zone will not change.  |

## Restrictions

You must be in ARE-Configure mode before using this command. To learn more about this mode, please see [Chapter 6, are Commands](#).

You can use this command only on an interface that has already been created using the **interface create appletalk** command.

## Example

To configure an additional zone with the name myzone, and to make it the new default:

```
xp(are-config)# interface add appletalk int4 zone myzone default
```

# interface add ip

## Purpose

Configure secondary addresses for an existing IPv4 interface.

## Format

**interface add ip** *<InterfaceName>* **address-netmask** *<IPaddr-mask>* [**peer-address** *<IPaddr>*] [**broadcast** *<IPaddr>*]

## Mode

Configure.

## Description

The **interface add ip** command configures secondary addresses for an existing IPv4 interface. Use this command to configure a secondary IPv4 address and netmask, a secondary peer-address, and a secondary broadcast address. To configure a secondary address for an existing IPv6 interface, use the **interface add ipv6** command.

**Note:** The interface must already exist. To create an interface, enter the **interface create ip** command.

## Parameters

---

|                              |  |
|------------------------------|--|
| <i>&lt;InterfaceName&gt;</i> | Name of the IPv4 interface; for example, int4. |
|------------------------------|--|

**Note:** Enterasys recommends that you use alphabetic characters when defining interface names—purely numeric interfaces will be interpreted as IP addresses. The X-Pedition router will display interface names up to 32 characters in length.

---

|   |  |
|---|--|
| <b>address-netmask</b><br><IPv4addr-mask> | Secondary IPv4 address and netmask of this interface. You can specify the address and mask information using the traditional format (example: 10.1.2.3/255.255.0.0) or the CIDR format (example: 10.1.2.3/16). If you specify an address without mask information, the X-Pedition router uses the natural mask for the address (/8 for Class A, /16 for Class B or /24 for Class C). |
| <b>peer-address</b><br>[<IPaddr>]         | Secondary IPv4 address of the peer for this port. Primarily used for setting up connection with another WAN port or setting up a VC with another ATM port.<br><br>For WAN and ATM ports only.  |
| <b>broadcast</b> <IPaddr>                 | Secondary broadcast address of this interface.   |

## Restrictions

You can use this command only on an interface that has already been created using the **interface create ip** command.

## Example

To configure a secondary address of 10.23.4.36 with a 24-bit netmask (255.255.255.0) on the IP interface int4:

```
xp(config)# interface add ip int4 address-mask 10.23.4.36/24
```

# interface add ipv6

## Purpose

Add additional IPv6 addresses to an existing IPv6 interface.

## Format

**interface add ipv6** <InterfaceName> **address-prefix** <address[/prefix-len]> [**eui64**] [**anycast**] [**peer-address** <address>]

## Mode

Configure.

## Description

Use this command to add additional IPv6 addresses to existing IPv6 interfaces. When adding an IPv6 address to an IPv6-in-IPv4 tunnel interface, you must specify *both* the local address, with the **address-prefix** parameter, *and* the remote peer address, with the **peer-address** parameter.

A link-local address is generated when an IPv6 interface is created. You cannot specify a different link-local address with this command.

**Note:** The IPv6 interface must already exist. To create an interface, enter the **interface create ipv6** command.

Use the **no** or **negate** command to remove a secondary IPv6 address.

## Parameters

|                 |  |
|-----------------|--|
| <InterfaceName> | Name of the previously created IPv6 interface.   |
| <b>Note:</b>    | Enterasys recommends that you use alphabetic characters when defining interface names—purely numeric interfaces will be interpreted as IP addresses. The X-Pedition router will display interface names up to 32 characters in length. |

|   |  |
|---|--|
| <b>address-prefix</b><br><address[/prefix-len]> | <p>Secondary IPv6 address and network prefix being added to this interface. The default prefix length for port-based interfaces is 64. The default prefix length for IPv6-in-IPv4 interfaces is 128.</p> <p><b>Note:</b> When adding an address to a tunnel interface, you must also specify the remote peer address with the <b>peer-address</b> parameter. The only allowed prefix-length for a tunnel address is /128.</p> <p>Use the <b>eui64</b> or <b>anycast</b> options to tailor the behavior of <b>address-prefix</b> on port-based IPv6 interfaces.</p> |
| <b>eui64</b>                                    | <p>Automatically fills the specified site-local or global IPv6 address with an interface identifier (that follows the EUI-64 format) in the lower-most 64 bits of the IPv6 address automatically. The given &lt;address[/prefix-len]&gt; should not exceed 64 bits, since the last 64 bits will be filled with the interface identifier.</p> <p>This option is not valid with IPv6-in-IPv4 tunnel interfaces.</p>  |
| <b>anycast</b>                                  | <p>Specified address is an anycast address. Anycast addresses will not be used as the source address of any outgoing IPv6 packets.</p>   |
| <b>peer-address</b><br><address>                | <p>Specifies the IPv6 address (with no prefix) for the remote end of the tunnel that is associated with the local IPv6 address specified with the <b>address-prefix</b> parameter.</p> <p>This parameter is required when adding an additional address to an IPv6-in-IPv4 interface, but is not allowed when adding an additional address to a port-based IPv6 interface.</p>  |

## Restrictions

You can use this command only on an interface that has already been created using the **interface create ipv6** command.

## Example

The following example adds a global unicast address to the previously created IPv6 port-based interface named IPv6\_1. The entire address and prefix are entered with the **address-prefix** parameter.

```
xp(config)# interface add ipv6 IPv6_1 address-prefix 20::2/64
```

This example adds an IPv6 address to the previously created tunnel interface named tunnel\_1.

```
xp(config)# interface add ipv6 tunnel_1 address-prefix 1234::1/128 peer-address 1234::2
```



# interface add ipx

## Purpose

Configure secondary addresses for an existing IPX interface.

## Format

```
interface add ipx <InterfaceName> address <IPXaddr> [peer-address <IPXaddr>]  
[output-mac-encapsulation <MACencap>]
```

## Mode

Configure.

## Description

The **interface add ipx** command configures secondary addresses for an existing IPX interface.

**Note:** The interface must already exist. To create an interface, enter the **interface create ipx** command.

## Parameters

|                                  |   |
|----------------------------------|---|
| <InterfaceName>                  | Name of the IP interface; for example, int4.<br><br><b>Note:</b> Enterasys recommends that you use alphabetic characters when defining interface names—purely numeric interfaces will be interpreted as IP addresses. The X-Pedition router will display interface names up to 32 characters in length. |
| <b>address</b> <IPXaddr>         | Secondary IPX network address of this interface, specified in a hexadecimal number.   |
| <b>peer-address</b><br><IPXaddr> | Secondary IPX address of the peer for this port. Primarily used for setting up connection with another WAN port. The <b>peer-address</b> contains the network address, a period (.), then the mac address. This can be illustrated as follows: <b>a1b2c3d4.aa:bb:cc:dd:ee:ff</b> . For WAN ports only.  |

---

|   |  |
|---|--|
| <b>output-mac-encapsulation</b><br><MACencap> | The output MAC encapsulation associated with this interface. You can specify one of the following: <ul style="list-style-type: none"><li>– <b>ethernet_ii</b> (the default)</li><li>– <b>ethernet 802.3</b></li><li>– <b>ethernet_snap</b></li><li>– <b>ethernet_802.2_ipx</b></li></ul> |
|---|--|

---

## Restrictions

- You can use this command only on an interface that has already been created using the **interface create ipx** command.
- IPX is not supported in partially meshed WAN networks unless each node has a unique network address.

## Example

To configure a secondary address of 10 (hexadecimal) on the IPX interface int4 with an 802.3 output encapsulation scheme:

```
xp(config)# interface add ipx int4 address 10 output-mac-encapsulation ethernet_802.3
```

# interface create appletalk

## Purpose

Creates an AppleTalk interface.

## Format

```
interface create appletalk <InterfaceName> vlan <name>|port <port> cable-range <range>  
[zone <ZoneName>] [address <Net.Node>] [up|down]
```

## Mode

ARE-Configure.

## Description

The **interface create appletalk** command creates and configures an AppleTalk/ARE interface. Configuration of an AppleTalk interface can include creating an interface in a disabled (**down**) state instead of the default enabled (**up**) state. In using this command, you *must* specify a cable range. Otherwise, you should use the **interface create appletalk noseed** command.

Interfaces on the X-Pedition router are logical interfaces. Therefore, you can associate an interface with a single port or with multiple ports.

- To associate an interface with a single port, use the **port** option with the **interface create appletalk** command.
- To associate an interface with multiple ports, first create a VLAN and add ports to it, then use the **vlan** option with the **interface create appletalk** command.

**Note:** You must use either the **port** option or the **vlan** option with the **interface create appletalk** command.

## Parameters

|                                  |  |
|----------------------------------|--|
| <b>&lt;InterfaceName&gt;</b>     | Name of the AppleTalk interface; for example, int4.<br><br><b>Note:</b> Enterasys recommends that you use alphabetic characters when defining interface names—purely numeric interfaces will be interpreted as IP addresses. The X-Pedition router will display interface names up to 32 characters in length.   |
| <b>vlan &lt;name&gt;</b>         | Name of the VLAN associated with this interface.<br><br><b>Note:</b> The X-Pedition router will display VLAN names up to 32 characters in length.  |
| <b>port &lt;port&gt;</b>         | The port associated with this interface.   |
| <b>cable-range &lt;range&gt;</b> | Sets the range of network numbers assigned to this interface. Valid numbers include 1 to 65279. Cable ranges cannot overlap across interfaces that are part of the same network. For example, if one interface has the cable range 1-100 assigned to it, no other interface on the network may have any cable range that includes any number between 1 and 100. A cable range must also be continuous. For example, a cable range of 1-50, 60-100 is invalid.  |
| <b>zone &lt;ZoneName&gt;</b>     | Sets the default zone (up to 32 characters) for the local network connected to the interface. This default zone can be changed using the <b>interface add appletalk zone</b> command. If no zone is specified, a default zone will automatically be assigned to the interface.   |
| <b>address &lt;Net.Node&gt;</b>  | Assigns the network and node number to this interface. Valid network numbers range from 1 to 65279. Valid node numbers range from 1 to 253. If no address is specified, a random valid address will automatically be assigned to the interface.<br><br><b>Note:</b> The network number must lie within the previously specified <b>cable-range</b> . For example, if you set the cable range value at 1-2, then an appropriate network number would be 1 (i.e., 1.121). The address 3.121 would be considered inappropriate. |
| <b>up</b>                        | Sets the state of the interface to up. The interface will activate and attempt to pass traffic. This is the default state.   |
| <b>down</b>                      | Sets the state of the interface to down. The interface will be created. However, it will pass no traffic   |

## Restrictions

You must be in ARE-Configure mode before using this command. To learn more about this mode, please see [Chapter 6, \*are Commands\*](#).

**Note:** If you use a VLAN to create an AppleTalk interface, you must use an AppleTalk protocol-based VLAN.

## Example

To create an interface called “app7” with the cable range 100-1100 and address 1050.88, enter the following command. The interface is associated with port et.1.3.

```
xp(are-config)# interface create appletalk app7 port et.1.3 cable-range 100-1100 address 1050.88
```

To create an interface called “app1” associated with the VLAN called “marketing” and a cable range of 10-200, enter the following command. The interface is created in the down (disabled) state.

```
xp(are-config)# interface create appletalk app1 vlan marketing cable-range 10-200 down
```

## interface create appletalk noseed

### Purpose

Creates a seeded AppleTalk interface.

### Format

**interface create appletalk** <InterfaceName> **vlan** <name>|**port** <port> **noseed** [**up**|**down**]

### Mode

ARE-Configure.

### Description

The **interface create appletalk noseed** command creates and configures a seeded AppleTalk interface. This means that, upon creation, the interface will attempt to “seed” itself on the network. It will take its cable range and default zone from another network router. This command should be used when ever two routers are connected. One router will act as the “seed,” giving a cable range and default zone to the secondary, “non-seeded” router.

Configuration of a seeded AppleTalk interface can also include creating an interface in a disabled (**down**) state instead of the default enabled (**up**) state.

Interfaces on the X-Pedition router are logical interfaces. Therefore, you can associate an interface with a single port or with multiple ports.

- To associate an interface with a single port, use the **port** option with the **interface create appletalk noseed** command.
- To associate an interface with multiple ports, first create a VLAN and add ports to it, then use the **vlan** option with the **interface create appletalk noseed** command.

**Note:** You must use either the **port** option or the **vlan** option with the **interface create appletalk noseed** command.

## Parameters

|                                    |  |
|------------------------------------|--|
| <code>&lt;InterfaceName&gt;</code> | Name of the AppleTalk interface; for example, int4.<br><br><b>Note:</b> Enterasys recommends that you use alphabetic characters when defining interface names—purely numeric interfaces will be interpreted as IP addresses. The X-Pedition router will display interface names up to 32 characters in length. |
| <code>vlan &lt;name&gt;</code>     | Name of the VLAN associated with this interface.<br><br><b>Note:</b> The X-Pedition router will display VLAN names up to 32 characters in length.  |
| <code>port &lt;port&gt;</code>     | The port associated with this interface.   |
| <code>noseed</code>                | Prompts the interface to attempt to “seed” itself on the network. This parameter should be used in place of the <b>cable-range</b> and <b>zone</b> parameters, since the interface will attempt to gain a cable range and zone from another router on the network.   |
| <code>up</code>                    | Sets the state of the interface to up. The interface will activate and attempt to pass traffic. (This is the default state.)   |
| <code>down</code>                  | Sets the state of the interface to down. The interface will be created, however it will pass no traffic.   |

## Restrictions

You may only use this command in ARE-Configure mode. For more about this mode, please see [Chapter 6, \*are Commands\*](#).

## Example

To create an interface called “aps8” which will attempt to seed itself on the network, enter the following command. The interface is associated with port et.1.5.

```
xp(are-config)# interface create appletalk aps8 port et.1.5 noseed
```

# interface create ip

## Purpose

Create an IPv4 interface. To create an IPv6 interface, use the **interface create ipv6** command.

## Format

```
interface create ip <InterfaceName> address-netmask <IPaddr-mask> [broadcast <IPaddr>]  
[peer-address <IPaddr>] vlan <name>[port <port> mtu <num>  
[output-mac-encapsulation <MACencap>] [up/down] [mac-addr <MACaddr-spec>]  
[type broadcast|point-to-point]
```

## Mode

Configure.

## Description

The **interface create ip** command allows you to create and configure an IPv4 interface name, IPv4 address, netmask, broadcast address, and the (subnet) mask to use when you create the interface.

**Note:** When you create an IP interface, the **interface create ip** command requires a logical name for each interface. If you use an IP interface name that begins with **en** or **lo**, the X-Pedition router will disable the proxy ARP on the interface.

**Note:** Enterasys recommends that you use alphabetic characters when defining interface names—purely numeric interfaces will be interpreted as IP addresses. The X-Pedition router will display VLAN and interface names up to 32 characters in length.

If you define a class C address and do not specify a mask, the router will assign the 24-bit (255.255.255.0) class C mask and the broadcast address will set all 8 host bits to 1. The XP also allows you the flexibility to use variable-length subnet masking in your network. If you specify a 27-bit (255.255.255.224) mask to have 6 subnets, the router broadcast will set all 5 host bits to 1. Traditional routers use this same functionality.

Router interface address:

|   |
|---|
| 172.16.1.129/27<br>172.16.1.129/255.255.255.224 |
|---|

Broadcast address with traditional routing:

|              |
|--------------|
| 172.16.1.159 |
|--------------|



Host interface address:

172.16.1.140/24  
172.16.1.159/255.255.255.0

Broadcast address with traditional routing:

172.16.1.255

If the hosts on this network use the class C mask, they will recognize the traditional router broadcast as another host address (the hosts would use the traditional 172.16.1.255 for broadcasts). In this situation, you could configure the router broadcast to 172.16.1.255—then the hosts on the network would recognize the broadcast address. Do not specify the broadcast address if all devices on the subnet are using the same mask.

The X-Pedition router is pre-allocated a pool of 64 MAC addresses. By default, the X-Pedition router configures each new IP interface with the *base* MAC address—the lowest MAC address in the pool. However, you can use the **mac-addr** option to assign a different MAC address to an interface. Interfaces on the X-Pedition router are logical interfaces; therefore, you can associate an interface with a single port or with multiple ports. You can also create an interface in a *disabled* (**down**) state instead of the default *enabled* (**up**) state.

- To associate an interface with a single port, use the **port** option with the **interface create** command.
- To associate an interface with multiple ports, first create an IP VLAN and add ports to it, then use the **vlan** option with the **interface create** command.

**Note:** You must use either the **port** option or the **vlan** option with the **interface create** command.

Parameters

|   |   |
|---|---|
| <InterfaceName>                         | Name of the IP interface; for example, int4.<br><br><b>Note:</b> Enterasys recommends that you use alphabetic characters when defining interface names—purely numeric interfaces will be interpreted as IP addresses. The X-Pedition router will display interface names up to 32 characters in length.   |
| <b>address-netmask</b><br><IPaddr-mask> | IP address and netmask of this interface. You can specify the address and mask information using the traditional format (example: 10.1.2.3/255.255.0.0) or the CIDR format (example: 10.1.2.3/16). If you specify an address without mask information, the X-Pedition router uses the natural mask for the address ( /8 for Class A, /16 for Class B or /24 for Class C). |

|   |  |
|---|--|
| <b>broadcast</b> <IPaddr>                     | IP address and netmask of this interface. You can specify the address and mask information using the traditional format (example: 10.1.2.3/255.255.0.0) or the CIDR format (example: 10.1.2.3/16). If you specify an address without mask information, the X-Pedition router uses the natural mask for the address ( /8 for Class A, /16 for Class B or /24 for Class C).  |
| <b>peer-address</b><br><IPaddr>               | IP address of the peer for this port. Primarily used for setting up connection with another WAN port or setting up a VC with another ATM port.<br><br>For WAN and ATM ports only.  |
| <b>vlan</b> <name>                            | Name of the VLAN associated with this interface.<br><br><b>Note:</b> The X-Pedition router will display VLAN names up to 32 characters in length.  |
| <b>port</b> <port>                            | Port associated with this interface.   |
| <b>mtu</b> <num>                              | Sets the MTU or <i>Maximum Transmission Unit</i> (in bytes) for this interface. By default, this value is equal to the MTU of the physical port minus some Layer-2 overhead (usually 22 bytes). However, users may set the interface MTU to anything less than the MTU of the physical port minus the Layer-2 overhead. In cases where an interface is assigned to a VLAN or SmartTRUNK, the interface MTU must be less than the MTU of the port in the VLAN or SmartTRUNK with the lowest value. When working with jumbo-frame capable ports, users may first need to use the <b>port set</b> <port> <b>mtu</b> <mtu> command to increase the physical port MTU size. |
| <b>up</b>                                     | Sets the state of the interface to up. (This is the default state.)  |
| <b>down</b>                                   | Sets the state of the interface to down.   |
| <b>output-mac-encapsulation</b><br><MACencap> | The output MAC encapsulation associated with this interface. You can specify one of the following: <ul style="list-style-type: none"><li>– <b>ethernet_ii</b> (the default)</li><li>– <b>ethernet_snap</b></li></ul>   |

|                                       |   |
|---------------------------------------|---|
| <b>mac-addr</b><br><MACaddr-spec>     | <p>Sets the MAC address for this interface. You can specify one of the following:</p> <ul style="list-style-type: none"> <li>– A specific MAC address – specify the entire MAC address as follows: xx:xx:xx:xx:xx:xx</li> <li>– An offset from the base MAC address in the pool – specify the offset. For example, to specify an offset of 10 from the base MAC address, enter “10”. For example, if the base MAC address is 00:E0:63:02:00:00 and you specify an offset of 10, the X-Pedition router assigns MAC address 00:E0:63:02:00:0A to the interface.</li> <li>– The base MAC address – specify the <b>basemac</b> keyword. This is the default.</li> </ul> |
| <b>type broadcast  point-to-point</b> | <p>Sets the type of interface. Specify one of the following:</p> <ul style="list-style-type: none"> <li>– <b>broadcast</b> (the default)</li> <li>– <b>point-to-point</b> (the default for PPP)</li> </ul> <p><b>Note:</b> If you connect the ATM interface to a router that uses a firmware version older than 8.2.0.0, you will need to set the interface type to point-to-point.</p>   |

## Restrictions

You must enter the peer address to set the ATM interface type to point-to-point.

## Example

To create a VLAN called IP3, add ports et.3.1 through et.3.4 to the VLAN, then create an IP interface on the VLAN:

```
xp(config)# vlan create IP3 ip
xp(config)# vlan add ports et.3.1-4 to IP3
xp(config)# interface create ip int3 address-mask 10.20.3.42/24 vlan IP3
```

To create an interface called “int7” with the address 10.50.89.88 and a 16-bit subnet mask, enter the following command. The interface is associated with port et.1.3.

```
xp(config)# interface create ip int7 address-mask 10.50.89.88/16 port et.1.3
```

To create an interface called “int1” with a broadcast address of 10.10.42.255, enter the following command. The interface is associated with the VLAN called “marketing”. The interface is created in the *down* (disabled) state.

```
xp(config)# interface create ip int1 address-mask 10.10.42.17/255.255.255.0 broadcast 10.10.42.255  
vlan marketing down
```

# interface create ipv6

## Purpose

Configure an IPv6 interface directly on a physical port or configure an IPv6-in-IPv4 tunnel interface.

## Format

```
interface create ipv6 <InterfaceName> [address-prefix <address[/prefix-len]> [eui64] [anycast]  
[mtu <num>]{<PortParameters> | <TunnelParameters>} [up | down]
```

## Mode

Configure.

## Description

Use this command to create and configure an IPv6 interface directly on a physical port, using the *PortParameter* options, or to create an IPv6-in-IPv4 tunnel interface, using the *TunnelParameters* options. Secondary addresses can be assigned to interfaces with the **interface add ipv6** command.

Port-related IPv6 interfaces may be configured only on Ethernet ports. An Ethernet port may be configured with both IPv6 and IPv4 interfaces.

An X-Pedition router may have only one tunnel configured between a particular IPv4 address pair, and a particular interface name must uniquely identify a single IPv4 address pair. To fully configure a tunnel between two routers, you must configure it on both routers, using the same IPv4 addresses. That is, on router A, associate an interface name with the address pair (local\_routerA\_IPv4\_address/remote\_routerB\_IPv4\_address) and on router B, associate an interface name with the address pair (local\_routerB\_IPv4\_address/remote\_routerA\_IPv4\_address).

There are no restrictions related to the type of ports on which a tunnel's IPv4 interfaces can be configured. IPv6 tunnel traffic can egress an X-Pedition router via an IPv4 interface configured over a WAN port.

Use the **no** or **negate** command to remove an IPv6 interface.

### Port-Based Interface Address Configuration

When you create a port-based interface and specify a global IPv6 address with the **address-prefix** parameter, a link-local address based on the MAC address of the router is automatically generated and associated with that interface, in addition to the global address.

If you do not explicitly specify a global IPv6 address with the **address-prefix** parameter, only the link-local address is generated when the interface is created.

You can use the **address-prefix** option to manually specify a link-local address, by entering an address with an FE80::/64 prefix. In this case, the system does not automatically generate a link-local address based on the router's MAC address.

Port-based interfaces must be associated with a specific physical port, with the **port** option.

### Tunnel Interface Address Configuration

The autogenerated link-local address for the local end of an IPv6-in-IPv4 tunnel is created from the local IPv4 interface address of the tunnel. You can specify an IPv6 address (global or link-local) for the local end of the tunnel with the **address-prefix** parameter, but if you do, you must also specify the corresponding (global or link-local) IPv6 address for the remote end of the tunnel with the **peer-address** parameter.

If you do not specify an IPv6 address for the tunnel interface with the **address-prefix** parameter, the autogenerated link-local address is used for the IPv6 address of the local end of the tunnel. In addition, the router assumes that the IPv6 address of the remote end of the tunnel is also a link-local address formed from the remote IPv4 interface address entered with the **remotev4** parameter. You cannot use the **peer-address** parameter to specify a remote IPv6 address if you have not used the **address-prefix** option to specify the local IPv6 address. That is, you must use both the **address-prefix** and **peer-address** parameters, or neither parameter, when configuring tunnel interfaces.

## Parameters

The following parameters are common to all IPv6 interfaces:

---

|  |  |
|--|--|
| <i>&lt;InterfaceName&gt;</i>                                 | Name of the IPv6 interface. This name can be used to assign IPv6 routes and access lists and to display configuration parameters and statistics.<br><br><b>Note:</b> Enterasys recommends that you use alphabetic characters when defining interface names—purely numeric interfaces will be interpreted as IP addresses. The X-Pedition router will display interface names up to 32 characters in length.  |
| <b>address-prefix</b><br><i>&lt;address[/prefix-len]&gt;</i> | IPv6 address (global or link-local) and network prefix length of this interface. The default prefix length for port-based interfaces is 64. The default prefix length for tunnel interfaces is 128.<br><br>If you specify a global address, a link-local address is automatically generated for the interface. If no IPv6 address is specified, only the link-local address is generated for the interface.<br><br><b>Note:</b> If you use this parameter when creating a tunnel interface, you must also use the <b>peer-address</b> tunnel parameter to configure the remote IPv6 interface.<br><br>Use the <b>eui64</b> or <b>anycast</b> options below to tailor the behavior of <b>address-prefix</b> . |

---

---

|                               |  |
|-------------------------------|--|
| <b>eui64</b>                  | Automatically fills the specified IPv6 address with an interface identifier in the lower-most 64 bits of the IPv6 address. The given <i>&lt;address[/prefix-len]&gt;</i> should not exceed 64 bits, since the last 64 bits will be filled with the interface identifier. |
| <b>anycast</b>                | Specified address is an anycast address. Anycast addresses will not be used as the source address of any outgoing IPv6 packets.  |
| <b>mtu</b> <i>&lt;num&gt;</i> | Sets the MTU or <i>Maximum Transmission Unit</i> (in bytes) for this interface. By default, this value is 1500 bytes.  |
| <b>up</b>                     | Sets the state of the interface to up. (This is the default state.)  |
| <b>down</b>                   | Sets the state of the interface to down.   |

---

## Port Parameters

The following parameters are used to create a port-based interface:

**port** *<port>* [**mac-addr** *<MACaddr-spec>*] [**vlan-id** *<num>*]

---

|   |   |
|---|---|
| <b>port</b> <i>&lt;port&gt;</i>             | Specifies the physical port associated with this interface.   |
| <b>mac-addr</b> <i>&lt;MACaddr-spec&gt;</i> | <p>Sets the MAC address for a port-based interface. You can specify one of the following:</p> <ul style="list-style-type: none"> <li>– An individual MAC address. Enter the entire MAC address as follows: xx:xx:xx:xx:xx:xx</li> <li>– An offset (0 to 63) from the base MAC address in the pool. For example, to specify an offset of 10 from the base MAC address, enter “10”. For example, if the base MAC address is 00:E0:63:02:00:00 and you specify an offset of 10, the X-Pedition router assigns MAC address 00:E0:63:02:00:0A to the interface.</li> <li>– The base MAC address, by entering the <b>basemac</b> keyword. This is the default.</li> </ul> |
| <b>vlan-id</b> <i>&lt;num&gt;</i>           | <p>Specifies the ID for the VLAN associated with this interface. The number can range from 2 to 4094.</p> <p>If more than one X-Pedition router will be configured with the same VLAN, you must specify the same VLAN ID on each router. If the ID is not specified, the X-Pedition router will assign the smallest ID from 2 – 4094 that has not already been assigned.</p>  |

---

## Tunnel Parameters

The following parameters are used to create an IPv6-in-IPv4 tunnel interface:

**tunnel** [**peer-address** *IPv6addr*] **localv4** *localv4interface* **remotev4** *remotev4Address*

|   |   |
|---|---|
| <b>tunnel</b>                             | Specifies that this interface is an IPv6-in-IPv4 tunnel interface.  |
| <b>peer-address</b> <i>IPv6addr</i>       | <p>Specifies an IPv6 address (with no prefix) for the remote end of the tunnel.</p> <p>If you used the <b>address-prefix</b> parameter to specify an IPv6 address for the local end of the tunnel, you <i>must</i> also use this parameter to specify the remote end's IPv6 address.</p> <p>If you did <i>not</i> use the <b>address-prefix</b> parameter to specify an IPv6 address for the local end of the tunnel, you cannot use this parameter to specify the remote end's IPv6 address.</p> |
| <b>localv4</b><br><i>localv4interface</i> | Specifies the name or address of any previously defined IPv4 interface on the local router (a stable address such as loop back address / router id is recommended). It defines the IPv4 source address of any IPv6-in-IPv4 packets sent over this tunnel to <i>remotev4Address</i> and must be the destination address of any IPv6-in-IPv4 packets received over this tunnel from <i>remotev4Address</i> .  |
| <b>remotev4</b><br><i>remotev4Address</i> | Specifies the IPv4 address of the router interface at the other end of this tunnel. It will be used as the destination address in any IPv6-in-IPv4 packets sent over this tunnel.   |

## Restrictions

An X-Pedition router may have only one tunnel configured between a particular IPv4 address pair, and a particular interface name must uniquely identify a single IPv4 address pair.



## Example

The following example creates a port-based IPv6 interface named “IPv6\_1” on Ethernet port et.5.6 with a global unicast address constructed from the subnet prefix 12AB:34CD:56EF:789A::/64 and the interface identifier for this interface. The **interface show** command is then used to display the results of the **interface create** command.

```
xp(config)# interface create ipv6 IPv6_1 address-prefix 12AB:34CD:56EF:789A::/64
ui64 port et.3.4

xp# interface show ipv6 IPv6_1

Interface IPv6_1:
  Admin State:      up
  Operational State: up
  Capabilities:     <BROADCAST,SIMPLEX,MULTICAST>
  Configuration:
    VLAN:           SYS_L3_IPv6_1
    Ports:          et.5.6
    MTU:            1500
    MAC Encapsulation: ETHERNET_II
    MAC Address:    00:E0:63:13:20:43
    IPv6 Address:   fe80::2e0:63ff:fe13:2043%IPv6_1 (prefixlen 64 scopeid 0x8)
    IPv6 Address:   12ab:34cd:56ef:789a:2e0:63ff:fe13:2043 (prefixlen 64)
    IPv6 Address:   12ab:34cd:56ef:789a:: (prefixlen 64 anycast)
```

The following example creates an IPv6 port-based interface named “IPv6\_2” on Ethernet port et.3.1 and manually assigns a link-local address (but no global address):

```
xp(config)# interface create ipv6 IPv6_2 address-prefix FE80::1234:ABCD:5678:9911/64 port et.3.1
```

The following example creates an IPv6-in-IPv4 tunnel using a local, previously created IPv4 interface named “IPv4\_1”. The remote end of the tunnel is IPv4 address 10.20.30.1. The tunnel interface being created is named “IPv6\_tunnel1”. This tunnel uses autogenerated IPv6 addresses for both the local and remote ends.

```
xp(config)# interface create ipv6 IPv6_tunnel1 tunnel localv4 IPv4_1 remotev4 10.20.30.1
```

The following example creates an IPv6-in-IPv4 tunnel using the IPv4 interface named IPv4\_2. The remote end of the tunnel has the IPv4 address 30.20.10.1. In this example, IPv6 addresses are specified for this point-to-point link.

```
xp(config)# interface create ipv6 IPv6_tunnel2 address-prefix 1234::1 tunnel peer-address 1234::2
localv4 IPv4_2 remotev4 30.20.10.1
```

# interface create ipx

## Purpose

Create an IPX interface.

## Format

```
interface create ipx <InterfaceName> address <IPXaddr> peer-address [<IPXaddr>]  
vlan <name> | port <port> [output-mac-encapsulation <MACencap>] [up|down]  
[mac-addr <MACaddr-spec>] [mtu <num>]
```

## Mode

Configure.

## Description

The **interface create ipx** command creates and configures an IPX interface. Configuration of an IPX interface can include information such as the interface's name, IPX address, VLAN, port, and output MAC encapsulation. You can also create an interface in the disabled (**down**) state instead of the default enabled (**up**) state.

The X-Pedition router is pre-allocated a pool of 64 MAC addresses (the maximum). By default, each new IPX interface is automatically configured with the lowest MAC address in the pool (the "base" MAC address). However, you can assign an interface a different MAC address by using the **mac-addr** option.

## Parameters

|                   |  |
|-------------------|--|
| <InterfaceName>   | Name of the IPX interface; for example, int9.<br><br><b>Note:</b> Enterasys recommends that you use alphabetic characters when defining interface names—purely numeric interfaces will be interpreted as IP addresses. The X-Pedition router will display interface names up to 32 characters in length. |
| address <ipxAddr> | IPX address of this interface.   |
| peer-address      | IPX address of the peer for this port. Primarily used for setting up connection with another WAN port. The <b>peer-address</b> contains the network address, a period (.), then the mac address. This can be illustrated as follows: <b>a1b2c3d4.aa:bb:cc:dd:ee:ff</b><br><br>For WAN ports only.        |

|                                 |  |
|---------------------------------|--|
| <b>vlan</b> <name>              | Name of the VLAN associated with this interface.<br><br><b>Note:</b> The X-Pedition router will display VLAN names up to 32 characters in length.  |
| <b>port</b> <port>              | Port associated with this interface.   |
| <b>up</b>                       | Sets the state of the interface to up. (This is the default state.)  |
| <b>down</b>                     | Sets the state of the interface to down.   |
| <b>output-mac-encapsulation</b> | <p>The output MAC encapsulation associated with this interface. You can specify one of the following:</p> <ul style="list-style-type: none"><li>• <b>ethernet_ii</b> (the default)</li><li>• <b>ethernet_snap</b></li><li>• <b>ethernet_802.2_ipx</b></li></ul> <p><b>Note:</b> When using line cards introduced prior to the “AA” series, SNA/DLC/NetBIOS traffic may not bridge properly. The issue in bridging DLC packets occurs where the length field within an IEEE 802.3 frame indicates less than 46 bytes of data.</p> <p>The X-Pedition router removes the length field information of incoming IEEE 802.3, 802.2, and Ethernet SNAP packets, then recalculates the field prior to re-transmission. Consequently, the calculation is based on the length of the entire data field. A packet entering the X-Pedition router whose length field indicates a data field of less than 46 bytes will exit with the length field recalculated incorrectly. This can be a problem with LLC2 and legacy IPX applications. Typically, such packets exist only in SNA and NetBIOS/NetBEUI environments.</p> |

|                                 |  |
|---------------------------------|--|
| <b>vlan</b> <name>              | Name of the VLAN associated with this interface.<br><br><b>Note:</b> The X-Pedition router will display VLAN names up to 32 characters in length.  |
| <b>port</b> <port>              | Port associated with this interface.   |
| <b>up</b>                       | Sets the state of the interface to up. (This is the default state.)  |
| <b>down</b>                     | Sets the state of the interface to down.   |
| <b>output-mac-encapsulation</b> | <p>The output MAC encapsulation associated with this interface. You can specify one of the following:</p> <ul style="list-style-type: none"> <li>• <b>ethernet_ii</b> (the default)</li> <li>• <b>ethernet_snap</b></li> <li>• <b>ethernet_802.2_ipx</b></li> </ul> <p><b>Note:</b> When using line cards introduced prior to the “AA” series, SNA/DLC/NetBIOS traffic may not bridge properly. The issue in bridging DLC packets occurs where the length field within an IEEE 802.3 frame indicates less than 46 bytes of data.</p> <p>The X-Pedition router removes the length field information of incoming IEEE 802.3, 802.2, and Ethernet SNAP packets, then recalculates the field prior to re-transmission. Consequently, the calculation is based on the length of the entire data field. A packet entering the X-Pedition router whose length field indicates a data field of less than 46 bytes will exit with the length field recalculated incorrectly. This can be a problem with LLC2 and legacy IPX applications. Typically, such packets exist only in SNA and NetBIOS/NetBEUI environments.</p> |

---

|                                   |  |
|-----------------------------------|--|
| <b>mac-addr</b><br><MACaddr-spec> | <p>Sets the MAC address for this interface. You can specify one of the following:</p> <ul style="list-style-type: none"> <li>• A specific MAC address – specify the entire MAC address as follows: xx:xx:xx:xx:xx:xx or xxxxxx:xxxxxx</li> <li>• An offset from the IPX base MAC address (base+2) in the pool – specify the offset. For example, to specify an offset of 10 from the IPX base MAC address, enter “10”. If, for example, the IPX base MAC address is 00:E0:63:02:00:00 and you specify an offset of 10, the X-Pedition router assigns IPX MAC address 00:E0:63:02:00:0A to the interface. You may enter any number between 1 and 61.</li> </ul> <p><b>Note:</b> The X-Pedition router has a pool of 64 MAC addresses (base to base+63); by default, IPX uses (base+2). If you would like to use another of the available MAC addresses, enter a number between 1 and 61; the interface MAC will then become ((IPXbaseMAC) + &lt;number&gt;).</p> <ul style="list-style-type: none"> <li>• The IPX base MAC address – specify the <b>basemac</b> keyword. This is the default, therefore you need only enter the keyword in order to make the selection explicit.</li> </ul> |
| <b>mtu</b>                        | <p>Sets the MTU or <i>Maximum Transmission Unit</i> (in bytes) for this interface. By default, this value is equal to the MTU of the physical port minus some Layer-2 overhead (usually 22 bytes). However, users may set the interface MTU to anything less than the MTU of the physical port minus the Layer-2 overhead. In cases where an interface is assigned to a VLAN or SmartTRUNK, the interface MTU must be less than the MTU of the port in the VLAN or SmartTRUNK with the lowest value. When working with jumbo-frame capable ports, users may first need to use the <b>port set</b> &lt;port&gt; <b>mtu</b> &lt;mtu&gt; command to increase the physical port MTU size.</p>  |

---

## Restrictions

IPX is not supported in partially meshed WAN networks unless each node has a unique network address.

## Example

The following commands create a VLAN called IPX10, add all the ports on the line card in slot 1 to the VLAN, and create an IPX interface called “int10” with the IPX address a98d7c6f, associated with VLAN IPX10.

```
xp(config)# vlan create IPX10 ipx  
xp(config)# vlan add ports et.1.* to IPX10  
xp(config)# interface create ipx int10 address a98d7c6f vlan IPX10
```

The following command creates an interface called “int5” with the IPX address 82af3d57 for port et.1.3. The interface is added in the down (disabled) state.

```
xp(config)# interface create ipx int5 address 82af3d57 port et.1.3 down
```

To create an interface called “int6” with the MAC address 00:01:02:03:04:05 and IPX address 82af3d58 for port et.1.4.

```
xp(config)# interface create ipx int6 address 82af3d58 port et.1.4  
          mac-addr 00:01:02:03:04:05
```

To create an interface called “int7” for a VLAN called “IPX-VLAN” on port et.1.4 with the MAC address at the base of the X-Pedition router’s MAC address pool:

```
xp(config)# interface create ipx int7 address 82af3d59 vlan IPX-VLAN et.1.4 mac-addr basemac
```

The following command creates an interface called “int7” for a VLAN called “IPX-VLAN” on port et.1.4 with a MAC address offset by 10 from the base of the X-Pedition router’s MAC address pool. If the base MAC address in the X-Pedition router’s MAC address pool is 00:E0:63:02:00:00, the offset of 10 gives the interface the MAC address 00:E0:63:02:00:0A.

```
xp(config)# interface create ipx int7 address 82af3d59 vlan IPX-VLAN et.1.4 mac-addr 10
```

The following commands create an ATM virtual channel on an ATM port and associate the port with an IPX interface. This allows IPX routing between two IPX interfaces. As with any IPX interface, IPX routing using RIP (the default) will begin when you configure an IPX interface.

```
xp(config)# atm create vcl port at.3.1.1.100  
xp(config)# interface create ipx finance address 01234567 peer-address 01234567.00:00:1d:a9:8c:a1  
          port at.3.1.1.100  
xp(config)# interface create ipx marketing address 01234569 port et.1.1
```

# interface show appletalk

## Purpose

Displays configuration of all AppleTalk interfaces.

## Format

**interface show appletalk** <InterfaceName> | **all** [**brief**]

## Mode

Enable.

## Description

The **interface show appletalk** command displays configuration information for all AppleTalk/ARE interfaces defined on the system.

## Parameters

---

|                              |   |
|------------------------------|---|
| <InterfaceName>   <b>all</b> | Name of the AppleTalk interface; for example, app4. Specify <b>all</b> to show configuration information about all AppleTalk interfaces on the X-Pedition router. |
|------------------------------|---|

|              |  |
|--------------|--|
| <b>Note:</b> | Enterasys recommends that you use alphabetic characters when defining interface names—purely numeric interfaces will be interpreted as IP addresses. The X-Pedition router will display interface names up to 32 characters in length. |
|--------------|--|

---

|              |   |
|--------------|---|
| <b>brief</b> | Display a brief summary of the interface in tabular form. |
|--------------|---|

---

## Restrictions

None.

## Example

To display configuration information for the AppleTalk interface called “app7”:

```
xp# interface show appletalk app7
```

To display configuration information for all AppleTalk interfaces:

```
xp# interface show appletalk all
```



# interface show ip

## Purpose

Display configuration of an IPv4 interface.

## Format

**interface show ip** <InterfaceName> | **all** [**brief**]

## Mode

Enable.

## Description

The **interface show ip** command displays configuration information for an IPv4 interface. To display information about an IPv6 interface, use the **interface show ipv6** command.

**Note:** You can display exactly the same information from within the ip facility using the **ip show interfaces** command.

## Parameters

|                              |  |
|------------------------------|--|
| <InterfaceName>   <b>all</b> | Name of the IP interface; for example, int4. Specify <b>all</b> to show configuration information about all the IP interfaces on the X-Pedition router.<br><br><b>Note:</b> Enterasys recommends that you use alphabetic characters when defining interface names—purely numeric interfaces will be interpreted as IP addresses. The X-Pedition router will display interface names up to 32 characters in length. |
| <b>brief</b>                 | Displays a brief summary of the interface in tabular form.   |

## Restrictions

None.

## Example

To display configuration information for the IPv4 interface called “IPv4\_1”:

```
xp# interface show ip IPv4_1

Interface IPv4_1:
  Admin State:      up
  Operational State: up
  Capabilities:     <BROADCAST,SIMPLEX,MULTICAST>
  Configuration:
    VLAN:           SYS_L3_IPv4_1
    Ports:          et.1.2
    MTU:            1500
    MAC Encapsulation: ETHERNET_II
    MAC Address:    00:E0:63:13:20:00
    IP Address:     10.10.10.10/24 (broadcast: 10.10.10.255)
```

.To display brief configuration information for all IPv4 interfaces:

```
xp# interface show ip all brief
```

| Interface | Status | Oper. Status | Address        | Broadcast     | Vlan/Port            |
|-----------|--------|--------------|----------------|---------------|----------------------|
| -----     | -----  | -----        | -----          | -----         | -----                |
| lo0       | up     | up           | 127.0.0.1/8    |               |                      |
| en0       | up     | up           | 192.132.1.1/24 | 192.132.1.255 |                      |
| IPv4_1    | up     | up           | 10.10.10.10/24 | 10.10.10.255  | SYS_L3_IPv4_1/et.1.2 |

# interface show ipv6

## Purpose

Display configuration of an IPv6 interface, including IPv6-in-IPv4 tunnels.

## Format

**interface show ipv6** {<InterfaceName> | **all** | **tunnels**} [**brief**]

## Mode

Enable.

## Description

Use this command to display the configuration of a single IPv6 interface, all IPv6 interfaces including IPv6-in-IPv4 tunnels, or just tunnels. The configured address/mask-length and any statistics will be displayed.

**Note:** You can display the exact same information from within the ipv6 facility using the **ipv6 show interfaces** command.

## Parameters

|                              |   |
|------------------------------|---|
| <i>&lt;InterfaceName&gt;</i> | Specifies the name of the IPv6 interface for which to display information.  |
| <b>all</b>                   | Specifies that configuration information should be displayed about all IPv6 interfaces configured on the X-Pedition router, including IPv6-in-IPv4 tunnels. |
| <b>tunnels</b>               | Specifies that configuration information should be displayed about all IPv6-in-IPv4 tunnels configured on the X-Pedition router.                            |
| <b>brief</b>                 | Displays a brief summary of the specified interface(s).   |

## Restrictions

None.

## Example

The following example displays configuration information for the IPv6 interface named “IPv6\_1.”

```
xp# interface show ipv6 IPv6_1

Interface IPv6_1:
  Admin State:      up
  Operational State: up
  Capabilities:     <BROADCAST,SIMPLEX,MULTICAST>
  Configuration:
    VLAN:           SYS_L3_IPv6_1
    Ports:          et.5.6
    MTU:            1500
    MAC Encapsulation: ETHERNET_II
    MAC Address:    00:E0:63:13:20:43
    IPv6 Address:   fe80::2e0:63ff:fe13:2043%IPv6_1 (prefixlen 64 scopeid 0x8)
    IPv6 Address:   12ab:34cd:56ef:789a:2e0:63ff:fe13:2043 (prefixlen 64)
    IPv6 Address:   12ab:34cd:56ef:789a:: (prefixlen 64 anycast)
```

The following example illustrates the **brief** option.

```
xp# interface show ipv6 all brief

Interface      Status Oper. Status      Address                                     Vlan/Port
-----
lo1            up      up                ::1/128
intf1          up      up                fe80::2e0:63ff:fe13:2043%intf1/64  SYS_L3_intf1/et.5.1
                20::2/64
                20::/64
intf3          up      up                fe80::2e0:63ff:fe13:2043%intf3/64  SYS_L3_intf3/et.5.7
                23::1/64
                23::/64
tunnell1       up      up                fe80::1401:102:tunnell1 --> fe80::1401:101:tunnell1
                abcd::1 --> abcd::2
IPv6_1         up      up                fe80::2e0:63ff:fe13:2043%IPv6_1/64  SYS_L3_IPv6_1/et.5.6
                12ab:34cd:56ef:789a:2e0:63ff:fe13:
                12ab:34cd:56ef:789a::/64
```

# interface show ipx

## Purpose

Display configuration of an IPX interface.

## Format

**interface show ipx** <InterfaceName> | **all** [**brief**]

## Mode

Enable.

## Description

The **interface show ipx** command displays configuration information for an IPX interface.

**Note:** You can display exactly the same information from within the ipx facility using the **ipx show interfaces** command.

## Parameters

|                              |   |
|------------------------------|---|
| <InterfaceName>   <b>all</b> | Name of the IPX interface; for example, int9. Specify <b>all</b> to show configuration information about all the IPX interfaces on the router.<br><br><b>Note:</b> Enterasys recommends that you use alphabetic characters when defining interface names—purely numeric interfaces will be interpreted as IP addresses. The X-Pedition router will display interface names up to 32 characters in length. |
| <b>brief</b>                 | Shows a brief summary of the interface in tabular form.   |

## Restrictions

None.

## Example

To display configuration information for the IPX interface called “int8”:

```
xp# interface show ipx int8
```

To display configuration information for all IPX interfaces:

```
xp# interface show ipx all
```

# Chapter 29

## ip Commands

The **ip** commands let you display and configure route table entries and various IP related tables.

### Command Summary

[Table 24](#) lists the **ip** commands. The sections following the table describe the command syntax.

**Table 24. ip Commands**

|  |
|--|
| <b>ip add route</b> <ipAddr-mask>  <b>default gateway</b> <hostname-or-IPaddr> [ <b>host</b> ]<br>[ <b>interface</b> <hostname-or-IPaddr>] [ <b>intf-list</b> <IPaddr-list>] [ <b>preference</b> <num>] [ <b>retain</b> ]<br>[ <b>reject</b> ] [ <b>no-install</b> ] [ <b>blackhole</b> ] [ <b>gate-list</b> <gateway list>] [ <b>unicast-rib</b> ] [ <b>multicast-rib</b> ] |
| <b>ip clear reverse-flows</b>  |
| <b>ip disable</b> dns-lookup forwarding icmp-redirect { <b>interface</b> <name>  <b>all</b> }   <b>proxy-arp</b><br>{ <b>interface</b> <name>  <b>all</b> }   <b>source-routing</b>  icmp-message { <b>echo-reply</b> <b>timestamp-reply</b><br><b>time-exceeded</b> <b>destination-unreachables</b> }   <b>default-route-check</b>  |
| <b>ip dos disable</b> port-attack-protection directed-broadcast-protection   |
| <b>ip enable</b> { <b>directed-broadcast</b> <b>interface</b> <interface name>  <b>all</b> }   { <b>reverse-flow</b> <b>all</b>   <b>policy</b>  <br><b>NAT</b>   <b>load-balance</b>   <b>normal</b> }   { <b>local-proxy-arp</b> <b>interface</b> <interface name>   <b>all</b> }  <br><b>limit-ip-option-pkts</b> <b>rate-threshold</b> <num>                             |
| <b>ip helper-address</b> <b>interface</b> <interface-name> <helper-address>   <b>all-interfaces</b><br>[<udp-port#>]   |
| <b>ip l3-hash module</b> <num>  <b>all</b> <b>variant</b> <num>  |
| <b>ip set port</b> <port-list> <b>forwarding-mode</b> <b>destination-based</b>   <b>host-flow-based</b>  |
| <b>ip show connections</b> [ <b>no-lookup</b> ]  |
| <b>ip show hash-variant</b> <num>  <b>all</b>  |

**Table 24. ip Commands (Continued)**

|  |
|--|
| <b>ip show helper-address</b>  |
| <b>ip show interfaces</b> [ <i>&lt;interface-name&gt;</i> ] [ <b>brief</b> ]   |
| <b>ip show reverse-flows</b>   |
| <b>ip show routes</b> [ <b>show-protocol</b> <b>direct default ospf ospf-ase ospf-nssa rip bgp static</b> ]<br>[ <b>show-arps</b> ] [ <b>show-multicast</b> ] [ <b>show-summary</b> ] [ <b>verbose</b> ] |



# ip add route

## Purpose

Configure a static route.

## Format

```
ip add route <ipAddr-mask>|default gateway <hostname-or-IPaddr> [host]
[interface <hostname-or-IPaddr>] [intf-list <IPaddr-list>] [preference <num>] [retain] [reject]
[no-install] [blackhole] [gate-list <gateway list>] [unicast-rib] [multicast-rib]
```

## Mode

Configure.

## Description

The **ip add route** command creates a static route entry in the route table. The static route can be a default route, a route to a network, or a route to a specific host.

## Parameters

|                                       |  |
|---------------------------------------|--|
| <b>&lt;ipAddr-mask&gt;</b>            | IP address and netmask of the destination. You can specify the address and mask information using the traditional format (example: 10.1.2.3/255.255.0.0) or the CIDR format (example: 10.1.2.3/16). If you specify an address without mask information, the X-Pedition router uses the natural mask for the address ( /8 for Class A, /16 for Class B or /24 for Class C). |
| <b>gateway</b> <hostname-or-IPaddr>   | IP address or hostname of the next hop gateway for this route. If a static route has several next hop gateways, use the <b>gate-list</b> option instead. This option cannot be used with <b>gate-list</b> or <b>intf-list</b> .  |
| <b>host</b>                           | Specifies that this route is a route to a host.  |
| <b>interface</b> <hostname-or-IPaddr> | The next hop interface associated with this route. When this option is specified, gateway is only considered valid when it is on this interface. If the next hop gateway can be reachable over more than one interface, use <b>intf-list</b> . This option cannot be used with <b>gate-list</b> or <b>intf-list</b> .  |
| <b>intf-list</b> <IPaddr-list>        | The next hop interfaces associated with this route. When you specify this option, the only gateways considered valid are those identified on the list of interfaces. This option cannot be used with <b>gateway</b> or <b>interface</b> .  |

|                                    |  |
|------------------------------------|--|
| <b>preference</b>                  | The preference of this static route. The preference controls how this route competes with routes from other protocols. The parameter takes a value between 0-255. The default preference is 60.  |
| <b>retain</b>                      | If specified, this option prevents this static route from being removed from the forwarding table when the routing service (GateD) is gracefully shut down. Normally gated removes all routes except interface routes during a graceful shutdown. The retain option can be used to insure that some routing is available even when GateD is not running. |
| <b>reject</b>                      | If specified, install this route as a reject route. Instead of forwarding a packet like a normal route, reject routes cause packets to be dropped and unreachable messages to be sent to the originator of the packet.   |
| <b>no-install</b>                  | If specified, the route will not be installed in the forwarding table when it is active but will be eligible for exporting to other protocols.   |
| <b>blackhole</b>                   | This option is the same as the reject option with the exception that unreachable messages are not sent.  |
| <b>gate-list</b><br><gateway list> | The next hop gateway associated with this route. Allows you to specify up to four gateways for a particular destination host or network. Static routes are installed when one or more gateways listed are available on directly attached interfaces. This option cannot be used with <b>gateway</b> or <b>interface</b> .                                |
| <b>unicast-rib</b>                 | Install this route in the Unicast Routing Information Base (RIB). This is enabled by default unless multicast-rib is specified. If both options are specified, the route will be installed in both RIBs.   |
| <b>multicast-rib</b>               | Install this route in the Multicast Routing Information Base (RIB). If this option is specified with the <b>unicast-rib</b> , the route will be installed in both RIBs.  |

## Restrictions

None.

## Examples

To configure the router 10.4.1.1 as the default gateway for this X-Pedition router:

```
xp(config)# ip add route default gateway 10.4.1.1
```

To configure the gateway 10.4.78.11 as the gateway for any packet destined for the subnet 10.4.14.0/24:

```
xp(config)# ip add route 10.4.14.0/24 gateway 10.4.78.11
```

To configure the gateway 10.4.78.11 as the gateway for any packet destined for the subnet 10.4.14.0/24:

```
xp(config)# ip add route 10.4.14.0/24 gateway 10.4.78.11
```

To configure the gateway 10.4.16.99 as the gateway to the host 10.4.15.2:

```
xp(config)# ip add route 10.4.15.2 host gateway 10.4.16.99
```

To configure a reject route entry for packets destined for the subnet 10.14.3.0/24:

```
xp(config)# ip add route 10.14.3.0/24 gateway 10.1.16.99 reject
```

## **ip clear reverse-flows**

### **Purpose**

Clears reverse flow statistics.

### **Format**

**ip clear reverse-flows**

### **Mode**

Enable.

### **Description**

The **ip clear reverse-flows** command deletes all reverse flow statistics. Reverse flows are IP traffic flows in the opposite direction, where source information becomes destination information and vice versa.

### **Parameters**

None.

### **Restrictions**

None.

### **Example**

To clear the reverse flow statistics:

```
xp# ip clear reverse-flows
```

# ip disable

## Purpose

Disables IP options on the X-Pedition router.

## Format

```
ip disable dns-lookup | forwarding | icmp-redirect {interface <name>|all} |  
proxy-arp {interface <name>|all} | source-routing | icmp-message  
{echo-reply timestamp-reply time-exceeded destination-unreachables} | default-route-check
```

## Mode

Configure.

## Description

The **ip disable** command allows you to disable features that are enabled by default on the X-Pedition router.

## Parameters

|  |   |
|--|---|
| <b>dns-lookup</b>  | Disables DNS name lookup for all commands. Sometimes a DNS server is too slow to respond and this can cause a command that displays information about many hosts to take a long time to finish. Disabling DNS lookup displays all host addresses as IP addresses instead of host names.   |
| <b>forwarding</b>  | Disables the router's ability to forward IP packets. No IP packets will be forwarded to any IP interface if this command is used.   |
| <b>icmp-redirect</b><br><b>{interface</b><br><i>&lt;interface-</i><br><i>name&gt; all</i> <b>}</b> | <p>Disables ICMP redirection on the specified IP interface. If you specify the all keyword, ICMP redirection is disabled for all network interfaces.</p> <p><b>Note:</b> Enterasys recommends that you use alphabetic characters when defining interface names—purely numeric interfaces will be interpreted as IP addresses. The X-Pedition router will display interface names up to 32 characters in length.</p> |

|   |   |
|---|---|
| <b>proxy-arp {interface &lt;name&gt; all}</b>   | <p>Disables the proxy ARP feature on the specified IP interface. By default, the router acts as a proxy for ARP requests with destination addresses of hosts to which the router can route traffic. Unless you require the use of proxy ARP, it is advisable to disable it on the router. If you specify the all keyword, the proxy ARP feature is disabled for all network interfaces.</p> <p><b>Note:</b> If you remove an interface on which you used the <b>ip disable proxy-arp interface</b> command to disable the proxy ARP feature, you disable proxy-arp for the entire system. Any unrouted Layer-2 packets will be lost—they will not know to route to another port.</p> <p><b>Note:</b> Enterasys recommends that you use alphabetic characters when defining interface names—purely numeric interfaces will be interpreted as IP addresses. The X-Pedition router will display interface names up to 32 characters in length.</p> |
| <b>source-routing</b>   | Causes the router to drop packets that have the SOURCE_ROUTE option set in the IP header. By default, packets that have the SOURCE_ROUTE option set are forwarded using the next-hop address in the IP packet.  |
| <b>icmp-message {echo-reply timestamp-reply time-exceeded destination-unreachables}</b> | Disables the ability to send out ICMP messages. ICMP messages are used to communicate errors in packet traffic to other X-Pedition routers. You can disable the following ICMP response messages: <b>echo-reply</b> , <b>timestamp-reply</b> , <b>time-exceeded</b> , and <b>destination-unreachables</b> .   |
| <b>default-route-check</b>  | Allows a default route to be set through the management (en0) interface.  |

**Note:** The **fast-icmp** option from previous releases has been deprecated and should not be used.

## Restrictions

None.

## Examples

To disable ICMP redirection on the “int4” network interface:

```
xp(config)# ip disable icmp-redirect int4
```

To disable DNS name lookup for all commands:

```
xp(config)# ip disable icmp-redirect dns-lookup
```

To prevent the X-Pedition router from acting as a proxy for ARP requests with destination addresses of hosts to which the router can route traffic:

```
xp(config)# ip disable proxy-arp interface all
```

# ip dos disable

## Purpose

Disables denial of service (DOS) features on the X-Pedition router.

## Format

**ip dos disable directed-broadcast-protection|port-attack-protection**

## Mode

Configure.

## Description

By default, the X-Pedition router installs flows in the hardware so that packets sent as directed broadcasts are dropped in hardware if directed broadcast is not enabled on the interface where the packet is received. You can disable this behavior with the **ip dos disable directed-broadcast-protection** command.

Similarly, the X-Pedition router installs flows to drop packets destined for the router for which service is not provided by the router. This prevents packets for unknown services from slowing the CPU. You can disable this behavior with the **ip dos disable port-attack-protection** command, causing these packets to be processed by the CPU.

## Parameters

|                                      |   |
|--------------------------------------|---|
| <b>directed-broadcast-protection</b> | Disables the directed-broadcast-protection feature of the X-Pedition router. By default the router drops packets sent as directed broadcasts if directed broadcast is not enabled on the interface where the packet is received. This command causes directed broadcast packets to be processed on the router even if directed broadcast is not enabled on the interface receiving the packet.  |
| <b>port-attack-protection</b>        | Disables the port-attack-protection feature of the X-Pedition router. By default, packets that are destined for the router, but do not have a service defined for them on the router, are dropped. This prevents packets for unknown services from slowing the router's CPU. This command disables this behavior, allowing packets destined for the router that do not have a service defined for them on the router to be processed by the router's CPU. |

## Restrictions

None.

## Examples

To cause directed broadcast packets to be processed on the X-Pedition router, even if directed broadcast is not enabled on the interface receiving the packet:

```
xp(config)# ip dos disable directed-broadcast-protection
```

To allow packets destined for the X-Pedition router, but do not have a service defined for them on the router, to be processed by the router's CPU:

```
xp(config)# ip dos disable port-attack-protection
```



# ip enable

## Purpose

Enables IP options on the X-Pedition router.

## Format

**ip enable** { **directed-broadcast interface** <interface name> | **all** } | { **reverse-flow all** | **policy** | **NAT** | **load-balance** | **normal** } | { **local-proxy-arp interface** <interface name> | **all** } | **limit-ip-option-pkts rate-threshold** <num>

## Mode

Configure.

## Description

The **ip enable** command allows you to configure the router to forward directed broadcast packets received on an interface, to set up reverse flows, and to limit the number of IP packets containing the option field that the Control Module will process per second.

Directed broadcast packets are network or subnet broadcast packets which are sent to a router to be forwarded as broadcast packets. They can be misused to create Denial Of Service attacks. The X-Pedition router protects against this possibility by *not* forwarding directed broadcasts, by default. To enable the forwarding of directed broadcasts, use the **ip enable directed-broadcast** command.

Reverse flows in this case are Layer-3 flows heading in the opposite direction to the corresponding IP flows. IP flows are defined by the source and destination IP addresses, source and destination TCP/UDP port, Type of Service and transport protocol.

When an IP packet includes the option field in its IP header, the packet routes to the Control Module for further processing—even if the packet does not match any hardware flow. This can significantly degrade Control Module performance when several of these packets arrive over a short time. The **rate-threshold** option allows you to limit the rate of IP-option packets— if the rate exceeds this limit, the X-Pedition router drops the packets. This feature is disabled by default.

## Parameters

|  |   |
|--|---|
| <b>directed-broadcast interface</b> <interface name>  <b>all</b> | <p>This is the name of the specified IP interface. If you specify the <b>all</b> keyword, directed broadcast forwarding is enabled for all network interfaces.</p> <p><b>Note:</b> Enterasys recommends that you use alphabetic characters when defining interface names—purely numeric interfaces will be interpreted as IP addresses. The X-Pedition router will display interface names up to 32 characters in length.</p>   |
| <b>reverse-flow all  policy  NAT  load-balance  normal</b>       | <p>Enables the ability to set up reverse flows. Specify <b>all</b> to disable any type of reverse flow to be set up. Specify <b>policy</b> to disable setting up reverse flows for policy routed packets. Specify <b>NAT</b> to disable setting up reverse flows for NAT packets. Specify <b>load-balance</b> to disable setting up reverse flows for load balance packets. Specify <b>normal</b> to disable setting up reverse flows for normally routed packets.</p>  |
| <b>local-proxy-arp interface</b> <interface name>   <b>all</b>   | <p>The local-proxy-arp parameter allows you to configure the X-Pedition router to respond to all ARP requests it processes with its own MAC address, regardless of whether it is the owner of the IP address being requested. Implement this option only after carefully considering the network implications.</p>  |
| <b>limit-ip-option-pkts rate-threshold</b> <num>                 | <p>The number of packets per second (0-3000) to use as the rate limit for IP option packets (enter 0 to drop every packet). Each time the X-Pedition router receives a packet without an ip-option field defined, the router establishes a flow—L3-Aging removes the flow if it sits unused for a specific amount of time. Packets with an IP-option field defined do not use a standard flow; rather, they route directly to the CM. The X-Pedition router collects statistics every second on the rate of IP option packets flowing to the CM—if the packet rate exceeds the limit specified, all IP option packets received in the same one-second period will be dropped and the router will increment the drop-flow count. The X-Pedition router clears all dropped flows and begins processing IP option packets (if their rate falls below the threshold limit) each time half of the L3 aging period lapses—by default this period is 15 seconds.</p> |

## Restrictions

The **limit-ip-option-pkts rate-threshold** <num> option will not work if L3 aging is disabled.

## Examples

To enable directed broadcast forwarding on the “int4” network interface:

```
xp(config)# ip enable directed-broadcast interface int4
```

To enable directed broadcast forwarding for all network interfaces:

```
xp(config)# ip enable directed-broadcast interface all
```

To enable reverse flows for policy routed packets:

```
xp(config)# ip enable reverse-flow policy
```

To set the limit on the rate of IP option packets to 100 packets/seconds:

```
xp(config)# ip enable limit-ip-option-pkts rate-threshold 100
```

# ip helper-address

## Purpose

Configure the router to forward specific UDP broadcast packets across interfaces.

## Format

**ip helper-address interface** <interface-name> <helper-address>/**all-interfaces** [<udp-port#>]

## Mode

Configure.

## Description

The **ip helper-address** command allows the user to forward specific UDP broadcast from one interface to another. Typically, broadcast packets from one interface are not forwarded (routed) to another interface. However, some applications use UDP broadcast to detect the availability of a service. Other services, for example BOOTP/DHCP require broadcast packets to be routed so that they can provide services to clients on another subnet. An IP helper can be configured on each interface to have UDP broadcast packets forwarded to a specific host for a specific service or forwarded to all other interfaces.

The **ip helper-address** command allows the user to specify a UDP port number for which UDP broadcast packets with that destination port number will be forwarded. By default, if no UDP port number is specified, the X-Pedition router will forward UDP broadcast packets for the following services:

- BOOTP/DHCP (port 67 and 68)
- DNS (port 53)
- NetBIOS Name Server (port 137)
- NetBIOS Datagram Server (port 138)
- Time Service (port 37)

## Parameters

|   |   |
|---|---|
| <code>&lt;interface-name&gt;</code>                                 | Name of the IP interface where UDP broadcast is to be forwarded to the helper address.<br><br><b>Note:</b> Enterasys recommends that you use alphabetic characters when defining interface names—purely numeric interfaces will be interpreted as IP addresses. The X-Pedition router will display interface names up to 32 characters in length. |
| <code>&lt;helper-address&gt;</code><br><code>/all-interfaces</code> | Address of the host where UDP broadcast packets should be forwarded. If <b>all-interfaces</b> is specified, UDP broadcast packets are forwarded to all interfaces except the interface on which the broadcast packet was received.  |
| <code>&lt;udp-port&gt;</code>                                       | Destination UDP port number of the broadcast packets to forward. If not specified, packets for the six default services will be forwarded to the helper address.  |

## Restrictions

If you specify an interface name, the name must belong to an existing IP interface.

## Examples

To forward UDP broadcast packets received on interface int1 to the host 10.1.4.5 for the six default UDP services:

```
xp(config)# ip helper-address interface int1 10.1.4.5
```

To forward UDP broadcast packets received on interface int2 to the host 10.2.48.8 for packets with the destination port 111 (port mapper):

```
xp(config)# ip helper-address interface int2 10.2.48.8 111
```

To forward UDP broadcast packets received on interface int3 to all other interfaces:

```
xp(config)# ip helper-address interface int3 all-interfaces
```

## ip l3-hash

### Purpose

Changes the hashing algorithm used for the L3 lookup table.

### Format

**ip l3-hash module** <num>|**all variant** <num>

### Mode

Configure.

### Description

The X-Pedition router's L3 Lookup table is organized as a hash table. The hash function reduces the destination and source MAC addresses to 16-bit quantities each. The hashing algorithm generates a uniform distribution within the MAC address space. However, given a particular set of addresses, the distribution may cause addresses to clump together in the table. To minimize the risk of thrashing in the tables, three variations to the basic hashing algorithm are defined. Only one variation is in effect on a line card at any given time. You can use the **ip l3-hash** command to set which variation is in effect for a line card.

Swizzling shifts the hash value by a certain amount of bits, producing more random distribution across the L3 lookup table.

Auto-hashing periodically queries the L3 table for hash bucket overflow on a port. If there are more overflows than a certain threshold level, auto-hashing will automatically change the hash mode for that port. Eventually a 'best' hash mode for the particular traffic will be found, which will provide a more even distribution across the L3 lookup table.

**Note:** This command is subject to merging. If you enter one command for a module setting the variant to 8 (enabling autohashing) and then enter another command for the same module setting it to another variant, the commands will merge. The second command will become activated and overwrite the first one, in this case disabling autohashing on the module.

**Note:** Setting a variant on an ER-16 module will set it on both channels on that module.

## Parameters

|                                 |   |
|---------------------------------|---|
| <b>module</b> <num>  <b>all</b> | Slot number on the X-Pedition router. Specify any number between 1 and 16. The hashing algorithm change affects all ports on the line card in the slot. The <b>all</b> option causes the hashing algorithm to change on all ports on all slots. |
| <b>variant</b> <num>            | Creates a variation to the basic hashing algorithm. Variant numbers are: 0-3, 4-7 (swizzled), and 8 (enables autohashing). Specify 0 to use the default hashing algorithm.  |

## Restrictions

None.

## Example

To change the default hashing algorithm used for the L3 lookup table on all ports on slot 7:

```
xp(config)# ip l3-hash module 7 variant 1
```

# ip set port forwarding-mode

## Purpose

Causes the X-Pedition router, when processing an IP packet, to extract only certain fields from a layer-4 flow, rather than the entire flow.

## Format

**ip set port** <port-list> **forwarding-mode destination-based|host-flow-based**

## Mode

Configure.

## Description

The X-Pedition router's flow identifying logic normally extracts the complete application (layer-4) flow from an IP packet. The **ip set port forwarding-mode** command causes the X-Pedition router to extract only certain flow-related fields from the packet's L3 header, rather than the full layer-4 flow. This allows ports to route packets based on destination address alone, or on destination and source address only. As a result, in environments that do not have any filtering or RSVP requirements, the flow table can be used much more efficiently.

## Parameters

|                          |   |
|--------------------------|---|
| <b>port</b> <port-list>  | Modifies the flow extraction behavior on the specified ports. All ports must have an IP interface configured for them.  |
| <b>destination-based</b> | <p>All ports must have an IP interface configured for them.If the packet is a unicast packet, causes the <i>destination IP address</i>, <i>TOS</i> and <i>L4 protocol</i> fields to be the only fields extracted from the IP packet. These fields and the <i>port of entry</i> field are set into the flow block being constructed. All of the other fields are set to zero.</p> <p>For L3 multicast packets, the <i>destination IP address</i>, <i>source IP address</i>, <i>TOS</i> and <i>L4 protocol</i> fields are the only fields extracted from the IP packet. These along with the <i>port of entry</i> are the only fields set in the flow block. The remaining fields are set to zero. The flow lookup then proceeds as normal.</p> |
| <b>host-flow-based</b>   | For both unicast and multicast packets, the <i>destination IP address</i> , <i>source IP address</i> , <i>TOS</i> and the <i>L4 protocol</i> are the only fields extracted from the IP packet. These along with the <i>port of entry</i> are set in the flow block. The remaining flow block fields are set to zero. The flow lookup then proceeds as normal.   |



## Restrictions

None.

## Example

To cause the X-Pedition router to extract only the *destination IP address*, *TOS*, and *L4 protocol* fields from a layer-4 flow when processing an IP packet on port et.1.1:

```
xp(config)# ip set port et.1.1 forwarding-mode destination-based
```

To cause the X-Pedition router to extract only the *destination IP address*, *source IP address*, *TOS*, and *L4 protocol* type from a layer-4 flow when processing an IP packet on port et.1.1:

```
xp(config)# ip set port et.1.1 forwarding-mode host-flow-based
```

## ip show connections

### Purpose

Show all TCP/UDP connections and services.

### Format

**ip show connections [no-lookup]**

### Mode

Enable.

### Description

The **ip show connections** command displays all existing TCP and UDP connections to the X-Pedition router as well as TCP/UDP services available on the router.

### Parameters

---

|                  |  |
|------------------|--|
| <b>no-lookup</b> | By default, when displaying an IP address, this command attempts to do a reverse DNS lookup to look for the hostname associated with the IP address and display the hostname instead. If you do not want the reverse DNS lookup to occur, specify the <b>no-lookup</b> option. |
|------------------|--|

---

### Restrictions

None.

## Example

The following example displays all established connections and services of the X-Pedition router.

| xp# <b>ip show connections</b>                  |        |        |                |                 |         |
|---|--------|--------|----------------|-----------------|---------|
| Active Internet connections (including servers) |        |        |                |                 |         |
| Proto   | Recv-Q | Send-Q | Local Address  | Foreign Address | (state) |
| tcp   | 0      | 0      | *:gated-gii    | *:*             | LISTEN  |
| tcp   | 0      | 0      | *:http         | *:*             | LISTEN  |
| tcp   | 0      | 0      | *:telnet       | *:*             | LISTEN  |
| udp   | 0      | 0      | 127.0.0.1:1025 | 127.0.0.1:162   |         |
| udp   | 0      | 0      | *:snmp         | *:*             |         |
| udp   | 0      | 0      | *:snmp-trap    | *:*             |         |
| udp   | 0      | 0      | *:bootp-relay  | *:*             |         |
| udp   | 0      | 0      | *:route        | *:*             |         |
| udp   | 0      | 0      | *:*            | *:*             |         |

# ip show hash-variant

## Purpose

Display IP hash variant per module.

## Format

**ip show hash-variant** <num>|all

## Mode

Enable.

## Description

The **ip show hash-variant** command displays hash variant information. There are a total of 16 modules using the hash variant feature (1-16).

Enabling hash variant causes a variation to the basic hashing algorithm. This variation will prevent clustering of hash values and will provide a more even distribution across the L3 lookup table. Valid variant numbers are: 0-3, 4-7 (swizzled), and 8 (auto-hashed). The default hashing algorithm is 0.

Swizzling shifts the hash value by a certain amount of bits, causing a more random distribution across the L3 lookup table. Auto-hashing allows the X-Pedition router to auto-select a hashing algorithm optimized for 'best case' L3 table distribution.

## Parameters

|       |   |
|-------|---|
| <num> | Specifies the module. Specify any number between 1-16.                  |
| all   | Specify <b>all</b> to display hash variant information for all modules. |

## Restrictions

None.

## Example

To display IP hash variant information on all 16 modules:

```
xp# ip show hash-variant all
IP Module      Hash Variant
-----
Module 2       variant-0
Module 3       variant-0
Module 4       variant-0
Module 5       variant-1
Module 6       variant-0
Module 7       variant-0
Module 8       variant-2
Module 9       variant-0
Module 10      variant-7
Module 11      variant-0
Module 12      variant-6
Module 13      variant-0
Module 14      variant-0
Module 15      variant-0
```

## ip show helper-address

### Purpose

Display the configuration of IP helper addresses.

### Format

**ip show helper-address** [*<interface-name>*]

### Mode

Enable.

### Description

The **ip show helper-address** command displays the configuration of IP helper addresses configured on the system. One can specify the optional parameter, *interface-name*, to show only the IP helper addresses configured for that interface. If the command is executed without specifying an interface name then the IP helper address configuration of all interfaces are shown.

### Parameters

|                               |  |
|-------------------------------|--|
| <i>&lt;interface-name&gt;</i> | Name of the IP interface to display any configured IP helper addresses.  |
| <b>Note:</b>                  | Enterasys recommends that you use alphabetic characters when defining interface names—purely numeric interfaces will be interpreted as IP addresses. The X-Pedition router will display interface names up to 32 characters in length. |

### Restrictions

If you specify an interface name, the name must belong to an existing IP interface.

## Example

The following example shows that interface int4 has one helper address configured while interface int3 has one helper address configured for the port mapper service (port 111).

| xp# ip show helper-address |            |                  |
|----------------------------|------------|------------------|
| Interface                  | IP address | Helper Address   |
| -----                      | -----      | -----            |
| int6                       | 10.1.17.1  | none             |
| int5                       | 10.1.16.1  | none             |
| int4                       | 10.1.15.1  | 10.4.1.45        |
| int1                       | 10.1.12.1  | none             |
| int0                       | 10.1.11.1  | none             |
| int3                       | 10.1.14.1  | 10.5.78.122(111) |

# ip show interfaces

## Purpose

Display the configuration of IP interfaces.

## Format

**ip show interfaces** [<interface-name>] [**brief**] | **all**

## Mode

Enable.

## Description

The **ip show interfaces** command displays the configuration of an IP interface. If you issue the command without specifying an interface name the configuration of all IP interfaces is displayed. This command displays the same information as the **interface show ip** command.

## Parameters

|                  |   |
|------------------|---|
| <interface-name> | Name of the IP interface; for example, xp4. If you do not specify an interface name, the X-Pedition router displays all the IP interfaces.<br><br><b>Note:</b> Enterasys recommends that you use alphabetic characters when defining interface names—purely numeric interfaces will be interpreted as IP addresses. The X-Pedition router will display interface names up to 32 characters in length. |
| <b>brief</b>     | Shows a brief summary of the interface in tabular form.   |

## Restrictions

If you specify an interface name, the name must belong to an existing IP interface.



## Example

To display the configuration of the IP interface “int1”:

```
xp# ip show interfaces int1  
int1: flags=9862<BROADCAST,NOTRAILERS,RUNNING,SIMPLEX,LINK0,MULTICAST>  
      VLAN: IP2  
      Ports:  
      inet 10.1.12.1/24 broadcast 10.1.12.255
```

## ip show reverse-flows

### Purpose

Display reverse flow statistics.

### Format

**ip show reverse-flows**

### Mode

Enable.

### Description

The **ip show reverse-flows** command displays the reverse flow statistics. Reverse flows are IP traffic flows in the opposite direction, where source information becomes destination information and vice versa. This command shows the number of reverse flow packets.

### Parameters

None.

### Restrictions

None.

### Example

To display the reverse flow statistics:

```
xp# ip show reverse-flows
IP Reverse Flow Statistics :
Total reverse-flow packets      : 0
Successful reverse-flow packets : 0
Unsuccessful reverse-flow packets : 0
Arphold packets                 : 0
Find Flow entry success packets : 0
Sum of arp hold and flow entry success packets : 0
```

# ip show routes

## Purpose

Display the IP routing table.

## Format

```
ip show routes [show-protocol direct|default|ospf|ospf-ase|ospf-nssa|rip|bgp|static]
[show-arps] [show-multicast] [show-summary] [verbose]
```

## Mode

Enable.

## Description

The **ip show routes** command displays the IP routing table. Different command options can be used to show different aspects of the routing table.

## Parameters

|                       |   |
|-----------------------|---|
| <b>show-protocol</b>  | Shows only the IP routes that belong to one of these specified protocols:   |
| <b>direct</b>         | Shows all direct routes.  |
| <b>default</b>        | Shows all default routes.   |
| <b>ospf</b>           | Shows all OSPF (Open Shortest Path First) routes.   |
| <b>ospf-ase</b>       | Shows all OSPF (Open Shortest Path First) Autonomous System-External routes.  |
| <b>ospf-nssa</b>      | Shows all OSPF (Open Shortest Path First) Not-So-Stubby Area (NSSA) routes.   |
| <b>rip</b>            | Shows all RIP (Routing Information Protocol) routes.  |
| <b>bgp</b>            | Shows all BGP (Border Gateway Protocol) routes.   |
| <b>static</b>         | Shows all manually defined routes.  |
| <b>show-arps</b>      | By default, ARP entries are not shown. To show ARP entries (if any are present), specify the <b>show-arps</b> option.                           |
| <b>show-multicast</b> | By default, routes to multicast destinations are not shown. To show routes to multicast destinations, specify the <b>show-multicast</b> option. |
| <b>show-summary</b>   | Shows a summary of all route entries.   |

---

|                      |   |
|----------------------|---|
| <b>verbose</b>       | Show the routing table in verbose mode (the additional information is useful for debugging). A list of definitions for the verbose command follows.                   |
| <b>U: Up</b>         | Interface is up.  |
| <b>G: Gateway</b>    | This is a route to another network through the gateway specified.   |
| <b>H: Host</b>       | This is a route to a host through the gateway specified.  |
| <b>R: Reject</b>     | The router will return a “host unreachable” message upon receipt of a packet destined for this network and drop the packet.   |
| <b>D: Dynamic</b>    | The router received an ICMP redirect message for this route and installed it.   |
| <b>M: Modified</b>   | The router has changed an existing route because of an ICMP redirect.   |
| <b>C: Cloning</b>    | A directly connected interface route that may have more specific routes generated from it (e.g., ARP entries). Cloned routes may not be on point-to-point interfaces. |
| <b>S: Static</b>     | This is a manually configured route.  |
| <b>W: Cloned</b>     | A route was “cloned” from another route that was “C” or “c”.  |
| <b>c: Pr Cloning</b> | A route learned from a routing protocol may be “cloned.” Cloned routes may not be on point-to-point interfaces.   |
| <b>B: Blackhole</b>  | The router quietly drops any packets received on this interface destined for this network. A “host unreachable” message is not sent.                                  |

---

## Restrictions

None.

## Example

The following example displays the contents of the routing table. It shows that some of the route entries are for locally connected interfaces (“directly connected”), while some of the other routes are learned from RIP.

| xp# ip show routes |                    |        |           |
|--------------------|--------------------|--------|-----------|
| Destination        | Gateway            | Owner  | Netif     |
| -----              | -----              | -----  | -----     |
| 10.1.0.0/16        | 50.1.1.2           | RIP    | to-linux2 |
| 10.2.0.0/16        | 50.1.1.2           | RIP    | to-linux2 |
| 10.3.0.0/16        | 50.1.1.2           | RIP    | to-linux2 |
| 10.4.0.0/16        | 50.1.1.2           | RIP    | to-linux2 |
| 14.3.2.1           | 61.1.4.32          | Static | int61     |
| 21.0.0.0/8         | 50.1.1.2           | RIP    | to-linux2 |
| 30.1.0.0/16        | directly connected | -      | to-goya   |
| 50.1.0.0/16        | directly connected | -      | to-linux2 |
| 61.1.0.0/16        | directly connected | -      | int61     |
| 62.1.0.0/16        | 50.1.1.2           | RIP    | to-linux2 |
| 68.1.0.0/16        | directly connected | -      | int68     |
| 69.1.0.0/16        | 50.1.1.2           | RIP    | to-linux2 |
| 127.0.0.0/8        | 127.0.0.1          | Static | lo        |
| 127.0.0.1          | 127.0.0.1          | -      | lo        |
| 210.11.99.0/24     | directly connected | -      | int41     |



# Chapter 30

## ipv6 Commands

The **ipv6** commands let you configure static IPv6 routes, display the IPv6 routing table, display IPv6 interface information, and configure ICMPv6 parameters.

### Command Summary

[Table 25](#) lists the **ipv6** commands. The sections following the table describe the command syntax.

**Table 25. ipv6 commands**

|  |
|--|
| <b>ipv6 add route</b> {<IPv6addr/prefixlen>   <b>default</b> } { <b>gateway</b> <hostname-or-IPv6addr>} [ <b>host</b> ] [ <b>interface</b> <name-or-IPv6addr>] [ <b>preference</b> <num>] [ <b>retain</b> ] [ <b>reject</b> ] [ <b>no-install</b> ] [ <b>blackhole</b> ] |
| <b>ipv6 set icmp-rate-limit</b> <integer>  |
| <b>ipv6 disable icmp-redirect</b>  |
| <b>ipv6 show interfaces</b> {<interface-name>   <b>all</b>   <b>tunnels</b> } [ <b>brief</b> ]   |
| <b>ipv6 show routes</b> [ <b>show-protocol</b> { <b>direct</b>   <b>default</b>   <b>ripng</b>   <b>static</b> }   <b>show-summary</b> ] [ <b>verbose</b> ]  |

# **ipv6 add route**

## **Purpose**

Configure a static IPv6 route.

## **Format**

**ipv6 add route** { <IPv6addr/prefixlen> | **default** } { **gateway** <name-or-IPv6addr> } [**host**]  
 [**interface** <name-or-IPv6addr>] [**preference** <num>] [**retain**] [**reject**] [**no-install**] [**blackhole**]

## **Mode**

Configure.

## **Description**

The **ipv6 add route** command creates a static route entry in the unicast IPv6 route table. The static route can be a default route, a route to a network, or a route to a specific host.

## **Parameters**

|   |  |
|---|--|
| <b>&lt;ipv6addr/prefixlen&gt; / default</b> | Specify either the IPv6 address and prefix length associated with a route, or a default route. Specify the address and mask information using the CIDR format (example: 1234:5678:90ab::/64).  |
| <b>gateway &lt;name-or-IPv6addr&gt;</b>     | Use <b>gateway</b> to specify a single IPv6 address or hostname of the next hop router for this route<br><br>If a link-local address is specified as a gateway address, either the interface to use must be specified with the <b>interface</b> option, or the gateway address must be qualified with a zone id (interface name). If the interface corresponds to a 6-in-4 tunnel, the gateway address must match a remote peer address of the tunnel. |
| <b>host</b>                                 | Specifies that this route is a route to a host.  |



|                                     |  |
|-------------------------------------|--|
| <b>interface</b> <name-or-IPv6addr> | <p>Use <b>interface</b> to specify the next hop interface associated with this route. Interface specified may be an IPv6 address, IPv6 interface name, or IPv6-in-IPv4 tunnel name. When this option is specified, a gateway is only considered valid when it is on this interface.</p> <p>If a link-local address is specified as a gateway address (using the <b>gateway</b> option), either the interface to use must be specified with the <b>interface</b> option, or the gateway address must be qualified with a zone id (interface name). If the interface corresponds to a 6-in-4 tunnel, the gateway address must match a remote peer address of the tunnel.</p> |
| <b>preference</b>                   | <p>The preference of this static route. The preference controls how this route competes with routes from other protocols. The parameter takes a value between 0-255. The default preference is 60.</p>   |
| <b>retain</b>                       | <p>If specified, this option prevents this static route from being removed from the forwarding table when the routing service (GateD) is gracefully shut down. Normally GateD removes all routes except interface routes during a graceful shutdown. The <b>retain</b> option can be used to insure that some routing is available even when GateD is not running.</p>   |
| <b>reject</b>                       | <p>If specified, install this route as a reject route. Instead of forwarding a packet like a normal route, reject routes cause packets to be dropped and unreachable messages to be sent to the originator of the packet.</p>  |
| <b>no-install</b>                   | <p>If specified, the route will not be installed in the forwarding table when it is active but will be eligible for exporting to other protocols.</p>  |
| <b>blackhole</b>                    | <p>This option is the same as the reject option with the exception that unreachable messages are not sent.</p>   |

## Restrictions

If a link-local address is specified as a gateway address, either the interface to use must be specified with the **interface** option, or the address must be qualified with a zone id (interface name). If the interface corresponds to a 6-in-4 tunnel, the gateway address must match a remote peer address of the tunnel.

## Examples

To configure the router 4fde::2 as the default gateway for this X-Pedition router:

```
xp(config)# ipv6 add route default gateway 4fde::2
```

To configure the gateway 4fde::2 as the gateway for any packet destined for the subnet 1234::/64:

```
xp(config)# ipv6 add route 1234::/64 gateway 4fde::2
```

To configure a reject route entry for packets destined for the subnet 1234::/64:

```
xp(config)# ipv6 add route route 1234::/64 gateway 5678::2 reject
```

# **ipv6 set icmp-rate-limit**

## **Purpose**

Configures the maximum rate at which ICMPv6 error messages are sent to other nodes from this router.

## **Format**

**ipv6 set icmp-rate-limit** *<integer>*

## **Mode**

Configure.

## **Description**

This command lets you limit the rate at which ICMPv6 error messages are generated by this router to a maximum value specified in units of packets per second. The default maximum rate is 100 packets per second.

The **no** form of the command is used to delete the configuration previously specified by a matching command that did not include the **no** keyword.

## **Parameters**

*<integer>*

Specifies the maximum rate at which ICMPv6 error messages should be generated by this node, in units of packets per second. This value may be specified in the range from 1 to 100.

The default value is 100 packets per second.

## **Restrictions**

None.

## **Example**

To change the retransmission rate to 10 packets per second:

```
xp(config)# ipv6 set icmp-rate-limit 10
```

# ipv6 disable icmp-redirect

## Purpose

Disable the generation of ICMPv6 redirect messages when a packet is forwarded through the same interface on which it was received.

## Format

**ipv6 disable icmp-redirect**

## Mode

Configure.

## Description

This command lets you disable the generation of ICMPv6 redirect messages when a packet is forwarded through the same interface on which it was received. Sending of redirects is enabled by default.

The **no** form of the command is used to delete the configuration previously specified by a matching command that did not include the **no** keyword.

## Parameters

None.

## Restrictions

None.

## Example

To disable ICMPv6 redirects:

```
xp(config)# ipv6 disable icmp-redirect
```

# **ipv6 show interfaces**

## **Purpose**

Display the configuration of IPv6 interfaces.

## **Format**

**ipv6 show interfaces** { *<interface-name>* | **all** | **tunnels** } [**brief**]

## **Mode**

Enable.

## **Description**

The **ipv6 show interfaces** command displays the configuration of one or multiple IPv6 interfaces, including IPv6-in-IPv4 tunnels. The configured address/mask-length and any statistics will be displayed. This command displays the same information as the **interface show ipv6** command.

## **Parameters**

*<interface-name>* | **all** | **tunnels** To display the configuration of a single interface, specify the name of the IPv6 interface; for example, xp6. To display all the IPv6 interfaces, including IPv6-in-IPv4 tunnels, enter the **all** option. To display information about only the IPv6-in-IPv4 tunnels, enter the **tunnel** option.

**Note:** Enterasys recommends that you use alphabetic characters when defining interface names—purely numeric interfaces will be interpreted as IP addresses. The X-Pedition router will display interface names up to 32 characters in length.

**brief** Shows a brief summary of the interface in tabular form.

## **Restrictions**

If you specify an interface name, the name must belong to an existing IPv6 interface.

## Example

To display the configuration of the IPv6 interface “int1”:

```
xp# ipv6 show interfaces intf3

Interface intf3:
  Admin State:      up
  Operational State: up
  Capabilities:     <BROADCAST,SIMPLEX,MULTICAST>
  Configuration:
    VLAN:           SYS_L3_intf3
    Ports:          et.1.3
    MTU:            1500
    MAC Encapsulation: ETHERNET_II
    MAC Address:    00:E0:63:13:20:43
    IPv6 Address:   fe80::2e0:63ff:fe13:2043%intf3 (prefixlen 64 scopeid 0x4)
    IPv6 Address:   23::2e0:63ff:fe13:2043 (prefixlen 64)
    IPv6 Address:   23:: (prefixlen 64 anycast)
```

The following example illustrates the use of the brief option:

```
xp# ipv6 show interfaces all brief
```

| Interface | Status | Oper. Status | Address   | Vlan/Port           |
|-----------|--------|--------------|---|---------------------|
| -----     | -----  | -----        | -----   | -----               |
| lo1       | up     | up           | ::1/128   |                     |
| intf1     | up     | up           | fe80::2e0:63ff:fe13:2003%intf1/64                 | SYS_L3_intf1/et.1.1 |
|           |        |              | 20::1/64  |                     |
|           |        |              | 20::/64   |                     |
| intf3     | up     | up           | fe80::2e0:63ff:fe13:2003%intf3/64                 | SYS_L3_intf3/et.1.3 |
|           |        |              | 22::1/64  |                     |
|           |        |              | 22::/64   |                     |
| tunnel1   | up     | up           | fe80::1401:101%tunnel1 --> fe80::1401:102%tunnel1 |                     |
|           |        |              | abcd::1 --> abcd::2                               |                     |

# **ipv6 show routes**

## **Purpose**

Display the IPv6 routing table.

## **Format**

**ipv6 show routes** [**show-protocol** { **direct** | **default** | **ripng** | **static** } | **show-summary**] [**verbose**]

## **Mode**

Enable.

## **Description**

The **ipv6 show routes** command displays the IPv6 routing table. Different command options can be used to show different aspects of the routing table.

## **Parameters**

|                      |   |
|----------------------|---|
| <b>show-protocol</b> | Shows only the IP routes that belong to one of these specified protocols: |
| <b>direct</b>        | Shows all direct routes.  |
| <b>default</b>       | Shows all default routes.   |
| <b>ripng</b>         | Shows all RIPng (Routing Information Protocol Next Generation) routes.    |
| <b>static</b>        | Shows all manually defined routes.  |
| <b>show-summary</b>  | Shows a summary of all route entries.                                     |

**verbose**

Show the routing table in verbose mode (the additional information is useful for debugging). The following list describes the meaning of the flags shown in the Flags column in verbose mode:

**U: Up**—Interface is up.

**G: Gateway**—This is a route to another network through the gateway specified

**H: Host**—This is a route to a host through the gateway specified.

**R: Reject**—The router will return a “host unreachable” message upon receipt of a packet destined for this network and drop the packet.

**D: Dynamic**—The router received an ICMP redirect message for this route and installed it.

**M: Modified**—The router has changed an existing route because of an ICMP redirect.

**C: Cloning**—A directly connected interface route that may have more specific routes generated from it. Cloned routes may not be on point-to-point interfaces.

**S: Static**—This is a manually configured route.

**W: Cloned**—A route was “cloned” from another route that was “C” or “c”

**c: Pr Cloning**—A route learned from a routing protocol may be “cloned.” Cloned routes may not be on point-to-point interfaces.

**B: Blackhole**—The router will drop—quietly—any packets received on this interface destined for this network. A “host unreachable” message will *not* be sent.

**L: Local Route**—The destination of this route is one of the addresses of this router.

## Restrictions

None.



## Examples

The following example illustrates output using the verbose parameter. The “=>” symbol indicates that routes are sharing a duplicate key in the routing table. For example, the => on the second line indicates that the route is sharing a duplicate key with the route below it and that it is the preferred route.

```

xp# ipv6 show routes verbose

```

| Destination                    | Gateway                        | Owner | Flags | Refcnt | Netif  |
|--------------------------------|--------------------------------|-------|-------|--------|--------|
| -----                          | -----                          | ----  | ----  | -----  | ----   |
| ::1                            | directly connected             | -     | UHL   | 0      | lo1    |
| 20::                           | directly connected             | -     | UHL   | 0      | lo1 => |
| 20::/64                        | directly connected             | -     | UC    | 0      | intf1  |
| 20::2                          | directly connected             | -     | UHL   | 0      | lo1    |
| 22::/64                        | fe80::2e0:63ff:fe13:2003%intf1 | RIPNG | UG    | 0      | intf1  |
| 23::                           | directly connected             | -     | UHL   | 0      | lo1 => |
| 23::/64                        | directly connected             | -     | UC    | 0      | intf3  |
| 23::1                          | directly connected             | -     | UHL   | 0      | lo1    |
| fe80::%intf1/64                | directly connected             | -     | UC    | 1      | intf1  |
| fe80::2e0:63ff:fe13:2003%intf1 | directly connected             | -     | UHLW  | 1      | intf1  |
| fe80::2e0:63ff:fe13:2043%intf1 | directly connected             | -     | UHL   | 1      | lo1    |
| fe80::%intf3/64                | directly connected             | -     | UC    | 0      | intf3  |
| fe80::2e0:63ff:fe13:2043%intf3 | directly connected             | -     | UHL   | 0      | lo1    |
| ff01::%lo1/32                  | ::1                            | -     | UC    | 0      | lo1    |
| ff01::%intf1/32                | directly connected             | -     | UC    | 0      | intf1  |
| ff01::%intf3/32                | directly connected             | -     | UC    | 0      | intf3  |
| ff02::%lo1/32                  | ::1                            | -     | UC    | 0      | lo1    |
| ff02::%intf1/32                | directly connected             | -     | UC    | 0      | intf1  |
| ff02::%intf3/32                | directly connected             | -     | UC    | 0      | intf3  |

The following example displays the contents of the routing table. It shows that some of the route entries are for locally connected interfaces ("directly connected"), while some of the other routes are learned from RIPng. The route on the second line shares a duplicate key in the routing table with the route below it, and is the preferred route because of higher preference for static routes.

```

xp# ipv6 show routes

```

| Destination                    | Gateway            | Owner  | Netif    |
|--------------------------------|--------------------|--------|----------|
| -----                          | -----              | ----   | ----     |
| ::1                            | directly connected | -      | lo1      |
| 2700::                         | 2130::2            | Static | intf3 => |
| 2700::/64                      | fe80::2%intf3      | RIPNG  | intf3    |
| fe80::2e0:63ff:fe11:6043%intf2 | directly connected | -      | lo1      |
| fe80::%intf3/64                | directly connected | -      | intf3    |
| ff01::%lo1/32                  | ::1                | -      | lo1      |
| ff01::%intf3/32                | directly connected | -      | intf3    |
| ff02::%lo1/32                  | ::1                | -      | lo1      |
| ff02::%intf3/32                | directly connected | -      | intf3    |



# Chapter 31

## ip-policy Commands

The **ip-policy** commands let you set up policies that cause the X-Pedition router to forward packets to a specified IP address based on information in a packet's L3/L4 IP header fields.

### Command Summary

[Table 26](#) lists the **ip-policy** commands. The sections following the table describe the command syntax.

**Table 26. ip-policy Commands**

|  |
|--|
| <b>ip-policy</b> <name> <b>apply</b> local interface <name> all  |
| <b>ip-policy</b> <b>clear</b> all policy-name <name> all   |
| <b>ip-policy</b> <name> <b>deny</b> acl <aclname> everything-else [sequence <num>]   |
| <b>ip-policy</b> <name> <b>permit</b> acl <aclname> everything-else [sequence <num>]<br><b>next-hop-list</b> <ip-addr-list> <b>action</b> policy-first policy-last policy-only |
| <b>ip-policy</b> <name> <b>set</b> [pinger on] [load-policy round-robin   ip-hash sip dip both]  |
| <b>ip-policy</b> <b>show</b> [all] [policy-name <name> all] [interface <name> all]   |

# ip-policy apply

## Purpose

Applies an IP policy to an interface.

## Format

**ip-policy** <name> **apply local|interface** <InterfaceName>|**all**

## Mode

Configure.

## Description

Once you have defined an IP policy, you use the **ip-policy apply** command to apply the IP policy to an interface. Once the IP policy is applied to the interface, packets start being forwarded using the policy.

## Parameters

|                 |  |
|-----------------|--|
| <name>          | Is the name of a previously defined IP policy.   |
| <InterfaceName> | Is the name of the inbound interface to which you are applying the IP policy. The interface name must be less than 32 characters.<br><br><b>Note:</b> Enterasys recommends that you use alphabetic characters when defining interface names—purely numeric interfaces will be interpreted as IP addresses. The X-Pedition router will display interface names up to 32 characters in length. |
| <b>local</b>    | Causes packets generated by the X-Pedition router to be forwarded according to the IP policy.  |
| <b>all</b>      | Causes the IP policy to be applied to all IP interfaces.   |

## Restrictions

IP policies can be applied to IP interfaces only.

## Examples

To apply IP policy p1 to interface int4:

```
xp(config)# ip-policy p1 apply interface int4
```

To apply IP policy p2 to all IP packets generated on the X-Pedition router:

```
xp(config)# ip-policy p2 apply local
```

# ip-policy clear

## Purpose

Clears IP policy statistics.

## Format

**ip-policy clear all|policy-name <name>|all**

## Mode

Enable.

## Description

The **ip-policy clear** command is used in conjunction with the **ip-policy show** command, which gathers statistics about IP policies. The **ip-policy clear** command lets you reset IP policy statistics to zero.

## Parameters

|            |  |
|------------|--|
| <name>     | Is the name of an active IP policy.                  |
| <b>all</b> | Causes statistics to be cleared for all IP policies. |

## Restrictions

None.

## Examples

To clear statistics for IP policy p1:

```
xp# ip-policy clear policy-name p1
```

To clear statistics for all IP policies:

```
xp(config)# ip-policy clear all
```

# ip-policy deny

## Purpose

Specifies which packets cannot be subject to policy-based routing.

## Format

**ip-policy** <name> **deny acl** <aclname>|**everything-else** [sequence <num>]

## Mode

Configure.

## Description

The **ip-policy deny** command allows you to specifically prevent packets matching a profile from being forwarded with an IP policy. These packets are routed using dynamic routes instead.

**Note:** Since there is an implicit deny rule at the end of all IP policies, all packets that do not match any policy are forwarded using dynamic routes.

## Parameters

|                        |   |
|------------------------|---|
| <name>                 | Is the name of an IP policy.  |
| <b>acl</b> <aclname>   | Is the name of the ACL profile of the packets to be excluded from IP policy-based forwarding. Profiles are defined with the <b>acl</b> command. The ACL may contain either <b>permit</b> or <b>deny</b> keywords. The <b>ip-policy deny</b> command only looks at the following ACL rule parameter values: protocol, source IP address, destination IP address, source port, destination port, and TOS. |
| <b>everything-else</b> | Keyword that specifies an action to be performed for packets that do not match any of the previously-defined ACLs. Specifies that packets that are not <i>specifically</i> permitted to use policy-based routing are forwarded using dynamic routes.  |
| <b>sequence</b> <num>  | If an IP policy is composed of more than one <b>ip-policy</b> statement, specifies the order in which the statement is evaluated. Possible values are 1-65535. The <b>ip-policy</b> statement with the lowest sequence number is evaluated first.   |

## Restrictions

ACLs for non -IP protocols cannot be used for IP policy routing.

## Examples

To create a profile called “prof1” for telnet packets from 9.1.1.5 to 15.1.1.2:

```
xp(config)# acl prof1 permit ip 9.1.1.5 15.1.1.2 any any telnet 0
```

**Note:** See [acl permit/deny ip on page 29](#) for more information on creating profiles for IP policy routing.

To create an IP policy called “p3” that prevents packets matching prof1 (that is, telnet packets from 9.1.1.5 to 15.1.1.2) from being forwarded using an IP policy:

```
xp(config)# ip-policy p3 deny acl prof1
```

To create a policy called “p4” that prevents all packets that have not been specifically permitted to use policy-based routing (using the **ip-policy permit** command) from being forwarded using an IP policy:

```
xp(config)# ip-policy p4 deny acl everything-else
```



# ip-policy permit

## Purpose

Specifies gateways and actions for IP policies

## Format

```
ip-policy <name> permit acl <aclname>|everything-else [sequence <num>]
[next-hop-list <ip-addr-list>|null] [action policy-first|policy-last|policy-only]
```

## Mode

Configure.

## Description

The **ip-policy permit** command allows you to specify the next-hop gateway where packets matching a given profile should be forwarded. You can specify up to four next-hop gateways for an IP policy. Packets matching a profile you defined with an **acl** command are forwarded to the next-hop gateway.

You can specify when to apply the IP policy route with respect to dynamic or statically configured routes. You can cause packets to use the IP policy route first, then the dynamic route if the next-hop gateway is unavailable; use the dynamic route first, then the IP policy route; or drop the packets if the next-hop gateway is unavailable.

## Parameters

|                        |   |
|------------------------|---|
| <name>                 | Is the name of an IP policy.  |
| <b>acl</b> <aclname>   | Is the name of the ACL profile of the packets to be forwarded using an IP policy. Profiles are created with the <b>acl</b> command. The ACL may contain either <b>permit</b> or <b>deny</b> keywords. The <b>ip-policy permit</b> command only looks at the following ACL rule parameter values: protocol, source IP address, destination IP address, source port, destination port, and TOS. |
| <b>everything-else</b> | Specifies that all packets not <i>specified</i> using policy-based routing (i.e., with the <b>ip-policy deny</b> command) are forwarded to the next-hop gateway.  |
| <b>sequence</b> <num>  | If an IP policy is composed of more than one <b>ip-policy</b> statement, specifies the order in which the statement is evaluated. Possible values are 1-65536. The <b>ip-policy</b> statement with the lowest sequence number is evaluated first.   |

|   |  |
|---|--|
| <b>next-hop-list</b><br><ip-addr-list>  <b>null</b> | <p>Is the IP address of one or more next-hop gateways. Packets matching the profile specified in &lt;aclname&gt; are forwarded to one of the gateways specified here. You can specify up to four gateways for each profile. If you specify more than one gateway, enclose the list of IP addresses in quotes. You can define how the packet load is distributed among multiple gateways with the <b>ip-policy set load-policy</b> command.</p> <p>To drop packets that match the profile, use the <b>null</b> keyword.</p>   |
| <b>action policy-first policy-last policy-only</b>  | <p>Specifies how IP policies are applied with respect to dynamic or statically configured routes. The following options are available:</p> <p><b>policy-first</b> Causes packets matching the specified profile to use the IP policy route first. If the next-hop gateway specified in the IP policy is not reachable, the dynamic route is used instead.</p> <p><b>policy-last</b> Causes packets matching the specified profile to be routed using dynamic routes first. If a dynamic route is not available, then all packets matching the profile are routed using the IP policy gateway.</p> <p><b>policy-only</b> Causes packets matching the specified profile to use the IP policy route. If the next-hop gateway specified in the IP policy is not reachable, then the packets are dropped.</p> |

## Restrictions

ACLs for non IP protocols cannot be used for IP policy routing.

## Examples

To create a profile called “prof1” for telnet packets from 9.1.1.5 to 15.1.1.2:

```
xp(config)# acl prof1 permit ip 9.1.1.5 15.1.1.2 any any telnet 0
```

**Note:** See [acl permit/deny ip on page 29](#) for more information on creating profiles for IP policy routing.

To cause packets matching prof1 (that is, telnet packets from 9.1.1.5 to 15.1.1.2) to be forwarded to 10.10.10.10:

```
xp(config)# ip-policy p5 permit acl prof1 next-hop-list 10.10.10.10
```

To cause all packets that have not been specified using policy-based routing (using the **ip-policy deny** command) to be forwarded to 10.10.10.10:

```
xp(config)# ip-policy p5 permit acl everything-else next-hop-list 10.10.10.10
```

To cause packets matching prof1 to use dynamic routes if 10.10.10.10 is not available:

```
xp(config)# ip-policy p5 permit acl prof1 next-hop-list 10.10.10.10 action policy-first
```

To cause packets matching prof1 to be dropped if 10.10.10.10 is not available:

```
xp(config)# ip-policy p5 permit acl prof1 next-hop-list 10.10.10.10 action policy-only
```

# ip-policy set

## Purpose

Controls how packets are distributed among the next hop gateways in an IP policy and queries the availability of next-hop gateways.

## Format

**ip-policy** *<name>* **set** [**pinger on**] [**load-policy round-robin**| **ip-hash sip**|**dip**|**both**]

## Mode

Configure.

## Description

If you specify more than one next-hop gateway in an IP policy, you can use the **ip-policy set** command to control how the load is distributed among the next-hop gateways. You can cause each new flow to use the first available next-hop gateway in the **ip-policy permit** statement, or you can cause flows to use all the next-hop gateways in the **ip-policy permit** statement sequentially. You can also control which information in the IP packet to use to determine the next-hop gateway.

In addition, you can use the **ip-policy set** command to have the X-Pedition router query the availability of the next-hop gateways specified in an IP policy. When this option is active, the X-Pedition router periodically queries the next-hop gateways via ICMP\_ECHO\_REQUESTS. Only gateways that respond to these requests are used for forwarding packets.

## Parameters

|                     |  |
|---------------------|--|
| <i>&lt;name&gt;</i> | Is the name of an IP policy.   |
| <b>pinger on</b>    | Causes the X-Pedition router to check the availability of next-hop gateways by querying them with ICMP_ECHO_REQUESTS. Only gateways that respond to these requests are used for forwarding packets. Some hosts may have disabled responding to ICMP_ECHO packets. Make sure each next-hop gateway can respond to ICMP_ECHO packets before using this option. |

|                    |  |  |
|--------------------|--|--|
| <b>load-policy</b> | If an IP policy has more than one next-hop gateway, specifies how the packets are distributed among the gateways. Two options are available: |  |
| <b>round-robin</b> | <b>round-robin</b>   | Uses a sequential order to pick the next gateway in the list for each new flow.    |
|                    | <b>ip-hash</b>   | Uses the following information in the IP packet to determine the next hop gateway. |
|                    | <b>sip</b>   | Uses the source IP based selection.  |
|                    | <b>dip</b>   | Uses the destination IP based selection.   |
|                    | <b>both</b>  | Uses both source IP and destination IP for selection.                              |

## Restrictions

None.

## Examples

To set up 10.10.10.10 and 10.10.10.5 as next-hop gateways for IP policy p6:

```
xp(config)# ip-policy p6 permit profile prof1 next-hop-list '10.10.10.10 10.10.10.5'
```

To distribute flows among these two next-hop gateways in a sequential manner:

```
xp(config)# ip-policy p6 set load-policy round-robin
```

# ip-policy show

## Purpose

Displays information about active IP policies.

## Format

**ip-policy show** [**all**] [**policy-name** <name>|**all**] [**interface** <name>|**all**]

## Mode

Enable.

## Description

The **ip-policy show** command displays information about active IP policies, including profile definitions, policy configuration settings, and next-hop gateways. The command also displays statistics about packets that have matched an IP policy statement as well as the number of packets that have been forwarded to each next-hop gateway.

## Parameters

|  |  |
|--|--|
| <b>policy-name</b><br><name>  <b>all</b> | Is the name of an IP policy. Use the <b>all</b> keyword to display all active policies.<br><br><b>Note:</b> The <b>ip-policy show all</b> command works identically to the <b>ip-policy show policy-name all</b> command   |
| <b>interface</b> <name>  <b>all</b>      | Displays information about IP policies applied to a specified interface. When you use the <b>all</b> keyword, the command displays information about IP policies applied to all interfaces (i.e., an IP policy used by all interfaces). If no IP policy is shared by all interfaces, the following error message will appear:%PBR-I-NOALL, No policy applied to all IP interfaces<br><br><b>Note:</b> Enterasys recommends that you use alphabetic characters when defining interface names—purely numeric interfaces will be interpreted as IP addresses. The X-Pedition router will display interface names up to 32 characters in length. |

## Restrictions

None.

## Example

To display information about IP policy p1:

```
xp# ip-policy show policy-name p1
```

---

IP Policy name : p1 ❶  
Applied Interfaces : int1 ❷  
Load Policy : first available ❸

| ❹          | ❺              | ❻             | ❼       | ❽       | ❾   | ❿    |
|------------|----------------|---------------|---------|---------|-----|------|
| ACL        | Source IP/Mask | Dest. IP/Mask | SrcPort | DstPort | TOS | Prot |
| prof1      | 9.1.1.5/32     | 15.1.1.2      | any     | any     | 0   | IP   |
| prof2      | 2.2.2.2/32     | anywhere      | any     | any     | 0   | IP   |
| everything | anywhere       | anywhere      | any     | any     | 0   | IP   |

Next Hop Information

---

| ❾     | ❿      | ⓫          | ⓬   | ⓭           | ⓮          | ⓯   | ⓰    |
|-------|--------|------------|-----|-------------|------------|-----|------|
| Seq   | Rule   | ACL        | Cnt | Action      | Next Hop   | Cnt | Last |
| 10    | permit | prof1      | 0   | Policy Only | 11.1.1.2   | 0   | Dwn  |
| 20    | permit | prof2      | 0   | Policy Last | 1.1.1.1    | 0   | Dwn  |
|       |        |            |     |             | 2.2.2.2    | 0   | Dwn  |
|       |        |            |     |             | 3.3.3.3    | 0   | Dwn  |
| 999   | permit | everything | 0   | Policy Only | drop       | N/A | N/A  |
| 65536 | deny   | deny       | 0   | N/A         | normal fwd | N/A | N/A  |

### Legend:

1. The name of the IP policy.
2. The interface where the IP policy was applied.
3. The load distribution setting for IP-policy statements that have more than one next-hop gateway; either first available (the default) or round-robin.
4. The names of the profiles (created with an **acl** statement) associated with this IP policy.
5. The source address and filtering mask of this flow.
6. The destination address and filtering mask of this flow.
7. For TCP or UDP, the number of the source TCP or UDP port.
8. For TCP or UDP, the number of the destination TCP or UDP port.
9. The TOS value in the packet.
10. IP protocol (ICMP, TCP UDP).

11. The sequence in which the statement is evaluated. IP policy statements are listed in the order they are evaluated (lowest sequence number to highest).
12. The rule to apply to the packets matching the profile: either permit or deny
13. The name of the profile (ACL) of the packets to be forwarded using an IP policy.
14. The number of packets that have matched the profile since the IP policy was applied (or since the **ip-policy clear** command was last used)
15. The method by which IP policies are applied with respect to dynamic or statically configured routes; possible values are Policy First, Policy Only, or Policy Last.
16. The list of next-hop gateways in effect for the policy statement.
17. The number of packets that have been forwarded to this next-hop gateway.
18. The state of the link the last time an attempt was made to forward a packet; possible values are up, dwn, or N/A.
19. Implicit deny rule that is always evaluated last, causing all packets that do not match one of the profiles to be forwarded normally (with dynamic routes).



# Chapter 32

## ip-redundancy (vrrp) Commands

The **ip-redundancy** commands let you display and configure the Virtual Router Redundancy Protocol (VRRP) on the X-Pedition router. VRRP is defined in RFC 2338.

### Notes:

- Do not use an IP address for load-balancing that is already configured for VRRP.
- Interfaces configured with PVCs do not support VRRP.
- The X-Pedition router supports only 512 instances of VRRP. An instance is defined as one virtual router running on one interface. Running a single virtual router on four interfaces is considered four instances of VRRP, as is running four virtual routers on a single interface.

## Command Summary

[Table 27](#) lists the **ip-redundancy** commands. The sections following the table describe the command syntax.

**Table 27. ip-redundancy Commands**

|  |
|--|
| <b>ip-redundancy associate vrrp</b> <vrid> <b>interface</b> <interface> <b>id</b> <vrid><br><b>address</b> <ip address/mask> |
| <b>ip-redundancy clear vrrp-stats interface</b> <interface> <b>id</b> <vrid>   |
| <b>ip-redundancy create vrrp</b> <vrid> <b>interface</b> <interface>   |

**Table 27. ip-redundancy Commands (Continued)**

|  |
|--|
| <b>ip-redundancy set vrrp</b> <vrid> <b>interface</b> <interface> [ <b>priority</b> <num>] [ <b>adv-interval</b> <num>] [ <b>preempt-mode</b> enabled disabled owner-disabled] [ <b>auth-type</b> none text] [ <b>auth-key</b> <key>] [ <b>warmup-period</b> <num>] [ <b>icmp-response</b> ] |
| <b>ip-redundancy show vrrp interface</b> <interface> [ <b>id</b> <vrid>] [ <b>verbose</b> ] [ <b>summary</b> ]   |
| <b>ip-redundancy start vrrp</b> <vrid> <b>interface</b> <interface>  |
| <b>ip-redundancy trace vrrp</b> [ <b>events</b> [enabled   disabled]] [ <b>state-transitions</b> [enabled   disabled]] [ <b>packet-errors</b> [enabled   disabled]] [ <b>all</b> [enabled   disabled]]   |

# ip-redundancy associate

## Purpose

Associates an IP address with a virtual router.

## Format

**ip-redundancy associate vrrp** <vrid> **interface** <interface> **address** <ipaddr/mask>

## Mode

Configure.

## Description

The **ip-redundancy associate** command adds an IP address to the list of IP addresses associated with a virtual router.

## Parameters

|               |   |
|---------------|---|
| <vrid>        | Is the identifier of a virtual router. Specify a number between 1-255   |
| <interface>   | Is the name of the interface where the virtual router resides.<br><br><b>Note:</b> Enterasys recommends that you use alphabetic characters when defining interface names—purely numeric interfaces will be interpreted as IP addresses. The X-Pedition router will display VLAN and interface names up to 32 characters in length.<br><br><b>Note:</b> Do not use an IP address for VRRP that is already configured for load-balancing. |
| <ipaddr/mask> | Is the IP address and subnet mask to be associated with the virtual router.   |

## Restrictions

- Interfaces configured with PVCs do not support VRRP.
- Do not use an IP address for VRRP that is already configured for load-balancing.

## Example

To add IP address/mask 1.2.3.4/16 to the list of IP addresses associated with virtual router 1 on interface int1:

```
xp(config)# ip-redundancy associate vrrp 1 interface int1 address 1.2.3.4/16
```

# ip-redundancy clear vrrp-stats

## Purpose

Clears statistics gathered for VRRP.

## Format

**ip-redundancy clear vrrp-stats interface** <interface> [**id** <vrid>]

## Mode

Enable.

## Description

The **ip-redundancy clear vrrp-stats** command is used in conjunction with the **ip-redundancy show vrrp** command, which displays information about the virtual routers associated with an interface. When you specify the **verbose** option with the **ip-redundancy show vrrp** command, additional statistics are shown, including the number of times a Backup router became the Master, the number of VRRP advertisements received, and counts of VRRP packets that contain errors. When you run the **ip-redundancy clear vrrp-stats** command, these statistics are reset to zero.

## Parameters

|             |  |
|-------------|--|
| <interface> | Causes VRRP statistics to be cleared for all virtual routers on the specified interface.                           |
| <vrid>      | Causes VRRP statistics to be cleared for the virtual router with the specified VRID. Enter a number between 1-255. |

## Restrictions

Interfaces configured with PVCs do not support VRRP.

## Example

To clear statistics for virtual router 1 on interface int1:

```
xp# ip-redundancy clear vrrp-stats interface int1 id 1
```

# ip-redundancy create

## Purpose

Creates a virtual router.

## Format

**ip-redundancy create vrrp** <vrid> **interface** <interface>

## Mode

Configure.

## Description

The **ip-redundancy create** command creates a virtual router on a specified interface.

## Parameters

|             |  |
|-------------|--|
| <vrid>      | Is the identifier of the virtual router to create. Specify a number between 1-255. |
| <interface> | Is the interface on which to create the virtual router.                            |

## Restrictions

- Interfaces configured with PVCs do not support VRRP.
- The X-Pedition router supports only 512 instances of VRRP. An instance is defined as one virtual router running on one interface. Running a single virtual router on four interfaces is considered four instances of VRRP, as is running four virtual routers on a single interface.

## Example

To create a virtual router with an identifier (VRID) of 1 on interface int1:

```
xp(config)# ip-redundancy create vrrp 1 interface int1
```

# ip-redundancy set

## Purpose

Sets parameters for a virtual router.

## Format

```
ip-redundancy set vrrp <vrid> interface <interface> [priority <num>] [adv-interval <num>]
[preempt-mode enabled|disabled|owner-disabled] [auth-type none|text] [auth-key <key>]
[warmup-period <num>] [icmp-response]
```

## Mode

Configure.

## Description

The **ip-redundancy set** command lets you specify parameters for a virtual router, including backup priority, advertisement interval, whether the router can preempt a Master router that has a lower priority, the type of authentication used, and warm up time.

## Parameters

|                           |   |
|---------------------------|---|
| <vrid>                    | Is the identifier of a virtual router. Specify a number between 1-255.  |
| <interface>               | Is the name of the interface where the virtual router resides.  |
|                           | <b>Note:</b> Enterasys recommends that you use alphabetic characters when defining interface names—purely numeric interfaces will be interpreted as IP addresses. The X-Pedition router will display interface names up to 32 characters in length.                                   |
| <b>priority</b> <num>     | Specifies the backup priority to be used by this virtual router. This number must be between 1-254. The default is 100. The priority number applies only if the virtual router is not the IP address owner. The priority of the IP address owner is always 255 and cannot be changed. |
| <b>adv-interval</b> <num> | Is the interval between VRRP advertisements in seconds. The default is 1 second.  |

|                               |   |   |
|-------------------------------|---|---|
| <b>preempt-mode</b>           | Specifies whether a backup router can preempt a Master router with a lower priority. Use one of the following keywords:   |   |
|                               | <b>enabled</b>  | Preempt mode is enabled. A backup router can preempt a lower-priority Master router.                                |
|                               | <b>disabled</b>   | Pre-empt mode is disabled. A backup router cannot pre-empt a lower-priority Master router.                          |
|                               | <b>owner-disabled</b>   | Pre-empt mode is disabled. A backup router cannot pre-empt a lower-priority Master router, even if it is the Owner. |
| <b>auth-type</b>              | Specifies the type of authentication used for VRRP exchanges between routers. Use one of the following keywords:  |   |
|                               | <b>none</b>   | VRRP exchanges are not authenticated (the default).   |
|                               | <b>text</b>   | VRRP exchanges are authenticated with a clear-text password.  |
| <b>auth-key</b> <key>         | Is the clear-text password used to authenticate VRRP exchanges. If you specify the <b>text</b> keyword, you must also specify the <b>auth-key</b> parameter.  |   |
| <b>warmup-period</b><br><num> | Specifies the amount of delay (in seconds) before this virtual router is initialized, following a system reboot. Specify any number between 0 and 180. This delay is used to prevent a virtual router from preempting an existing Master before having received all of the routing updates from neighboring routers. (Default delay is 30 seconds). |   |
| <b>icmp-response</b>          | Specifies whether the backup router will respond to ICMP echo requests (pings) to the virtual IP address when the backup router is in master state.   |   |

## Restrictions

Interfaces configured with PVCs do not support VRRP.

## Examples

To specify 200 as the priority used by virtual router 1 on interface int1:

```
xp(config)# ip-redundancy set vrrp 1 interface int1 priority 200
```

To set the advertisement interval to 3 seconds:

```
xp(config)# ip-redundancy set vrrp 1 interface int1 adv-interval 3
```

To prevent a Backup router from taking over as Master from a Master router that has a lower priority:

```
xp(config)# ip-redundancy set vrrp 1 interface int1 preempt-mode disabled
```



To authenticate VRRP exchanges on virtual router 1 on interface int1 with a password of 'yellow':

```
xp(config)# ip-redundancy set vrrp 1 interface int1 auth-type text auth-key yellow
```

When enterprise customers run an X-Pedition router in a VRRP configuration, the customers may not know if a problem exists with the Backup router. As a result, the X-Pedition feature set includes the ability to ping the Backup router while the router is in a non-Master state. When a Backup VRRP router assumes mastership, RFC 2338 specifies that it must not answer to ICMP echo requests (pings) destined to the associated virtual address. In some network situations, however, you may want to permit the Backup router to respond with an ICMP Echo Response when it is in the Master state. Use the following command to enable ICMP Echo Response:

```
ip-redundancy set vrrp <vrID> interface <interface> icmp-response
```

# ip-redundancy show

## Purpose

Shows information about virtual routers.

## Format

**ip-redundancy show vrrp interface** <interface> [**id** <vrid>] [**verbose**] [**summary**]

## Mode

Enable.

## Description

The **ip-redundancy show vrrp** command displays configuration information about virtual routers on an interface. You can display information for one virtual router or for all the virtual routers on an interface. If you specify the verbose option, additional statistics are shown, including the number of times a Backup router became the Master, the number of VRRP advertisements received, and counts of VRRP packets that contain errors. These statistics are gathered from the time you start the virtual router, or from the time you last ran the **ip-redundancy clear vrrp-stats** command.

## Parameters

|                |  |
|----------------|--|
| <interface>    | Is the name of the interface where the virtual router resides. If you do not specify the <vrid> parameter, information about all virtual routers on the interface is displayed.<br><br><b>Note:</b> Enterasys recommends that you use alphabetic characters when defining interface names—purely numeric interfaces will be interpreted as IP addresses. The X-Pedition router will display interface names up to 32 characters in length. |
| <vrid>         | Is the identifier of a virtual router. Specify a number between 1-255.   |
| <b>verbose</b> | Causes VRRP statistics to be displayed for each virtual router   |

## Restrictions

- Interfaces configured with PVCs do not support VRRP.
- The X-Pedition router supports only 512 instances of VRRP. An instance is defined as one virtual router running on one interface. Running a single virtual router on four interfaces is considered four instances of VRRP, as is running four virtual routers on a single interface.

## Examples

To display information about all virtual routers on interface int1:

```
xp# ip-redundancy show vrrp interface int1

VRRP Virtual Router 100 - Interface int1
-----
Uptime                0 days, 0 hours, 0 minutes, 17 seconds.
State                 Backup
Priority              100 (default value)
Virtual MAC address   00005E:000164
Advertise Interval    1 sec(s) (default value)
Preempt Mode         Enabled (default value)
Authentication        None (default value)
Primary Address       10.8.0.2
Associated Addresses  10.8.0.1
                    100.0.0.1

VRRP Virtual Router 200 - Interface int1
-----
Uptime                0 days, 0 hours, 0 minutes, 17 seconds.
State                 Master
Priority              255 (default value)
Virtual MAC address   00005E:0001C8
Advertise Interval    1 sec(s) (default value)
Preempt Mode         Enabled (default value)
Authentication        None (default value)
Primary Address       10.8.0.2
Associated Addresses  10.8.0.2
```

To display VRRP statistics for virtual router 100 on interface int1:

```
xp# ip-redundancy show vrrp 1 interface int1 verbose

VRRP Virtual Router 100 - Interface int1
-----
Uptime                0 days, 0 hours, 0 minutes, 17 seconds.
State                  Backup
Priority                100 (default value)
Virtual MAC address    00005E:000164
Advertise Interval     1 sec(s) (default value)
Preempt Mode           Enabled (default value)
Authentication         None (default value)
Primary Address        10.8.0.2
Associated Addresses    10.8.0.1
                      100.0.0.1

Stats:
Number of transitions to master state      2
VRRP advertisements rcvd                  0
VRRP packets sent with 0 priority          1
VRRP packets rcvd with 0 priority          0
VRRP packets rcvd with IP-address list mismatch 0
VRRP packets rcvd with auth-type mismatch  0
VRRP packets rcvd with checksum error      0
VRRP packets rcvd with invalid version     0
VRRP packets rcvd with invalid VR-Id       0
VRRP packets rcvd with invalid adv-interval 0
VRRP packets rcvd with invalid TTL         0
VRRP packets rcvd with invalid 'type' field 0
VRRP packets rcvd with invalid auth-type   0
VRRP packets rcvd with invalid auth-key    0
```

# ip-redundancy start vrrp

## Purpose

Starts a virtual router.

## Format

**ip-redundancy start vrrp** <vrid> **interface** <interface>

## Mode

Configure.

## Description

The **ip-redundancy start vrrp** command starts a virtual router on the specified interface.

## Parameters

|   |  |
|---|--|
| <vrid>  | Is the identifier of a virtual router. Specify a number between 1-255. |
| <interface>   | Is the name of the interface where the virtual router resides.         |
| <b>Note:</b> Enterasys recommends that you use alphabetic characters when defining interface names—purely numeric interfaces will be interpreted as IP addresses. The X-Pedition router will display interface names up to 32 characters in length. |  |

## Restrictions

- Interfaces configured with PVCs do not support VRRP.
- The X-Pedition router supports only 512 instances of VRRP. An instance is defined as one virtual router running on one interface. Running a single virtual router on four interfaces is considered four instances of VRRP, as is running four virtual routers on a single interface.

## Example

To start virtual router 1 on interface int1:

```
xp# ip-redundancy start vrrp 1 interface int1
```

# ip-redundancy trace

## Purpose

Traces VRRP events.

## Format

```
ip-redundancy trace vrrp [events [enabled | disabled]] [state-transitions [enabled | disabled]]  
[packet-errors [enabled | disabled]] [all [enabled | disabled]]
```

## Mode

Configure.

## Description

The **ip-redundancy trace vrrp** command displays messages when certain VRRP events take place on the X-Pedition router. Use this command to display messages when a virtual router changes from one state to another (i.e., from Backup to Master), a VRRP packet error is detected, or when any VRRP event occurs.

## Parameters

|                             |   |
|-----------------------------|---|
| <b>events</b>               | Displays a message when VRRP receives any type of event. This option is disabled by default.                |
| <b>state-transitions</b>    | Displays a message when a VRRP router changes from one state to another. This option is enabled by default. |
| <b>packet-errors</b>        | Displays a message when a VRRP packet error is detected. This option is enabled by default.                 |
| <b>all enabled disabled</b> | Enables or disables all VRRP tracing.   |

## Restrictions

- Interfaces configured with PVCs do not support VRRP.
- The X-Pedition router supports only 512 instances of VRRP. An instance is defined as one virtual router running on one interface. Running a single virtual router on four interfaces is considered four instances of VRRP, as is running four virtual routers on a single interface.

# Chapter 33

## ip-router Commands

The **ip-router** commands let you configure and monitor features and functions that work across the various routing protocols. The commands in this chapter affect IPv4 only; however, the following **ip-router** commands affect both IPv4 and IPv6:

- **ip-router authentication**
- **ip-router policy add optional-attributes-list**
- **ip-router policy create { aspath-export-source | bgp-export-destination | bgp-export-source | bgp-import-source | optional-attributes-list | ospfase-export-source | ospf-export-destination | ospf-export-source | ospf-import-source | ospfnssa-export-destination | redirect-import-source | rip-export-destination | rip-export-source | rip-import-source }**

A sequence-number option is provided on some policy commands. This allows the policies to be arranged in the desired sequence. Absent a sequence number, policies are ordered by policy name string or number. Using numbers for the policy name results in policies being ordered in ascending policy name number. Using a name string results in policies being ordered alphabetically by name string.

For ipv6-router commands, refer to [Chapter 34, ipv6-router Commands](#).

## Command Summary

**Table 28** lists the **ip-router** commands. The sections following the table describe the command syntax.

**Table 28. ip-router Commands**

|  |
|--|
| <b>ip-router authentication add key-chain</b> [key <string>] [type primary secondary]  |
| <b>ip-router authentication create key-chain</b> [key <string>] [type primary secondary] [id]  |
| <b>ip-router find route</b> <ipAddr> [ignore-state]  |
| <b>ip-router global add interface</b> <name-or-IPAddr><br><b>ip-router global add martian</b> <ipAddr/mask>[default [host] [allow]   |
| <b>ip-router global set</b> [autonomous-system <num1> loops <num2>]<br>[router-id <hostname-or-IPAddr>] [interface { <interface-name> all} [preference <num>]<br>[down-preference <num>] [passive] [autonomous-system <num>]]<br>[confederation-id <num>] [max-bgjob-interval <num>] |
| <b>ip-router global set trace-level</b> <num>  |
| <b>ip-router global set trace-options</b> [all none]   [[startup] [parse] [debug] [adv] [symbols]<br>[if-list] [general] [state] [normal] [policy] [task] [timer] [route]]   |
| <b>ip-router global set trace-state</b> on off   |
| <b>ip-router global use</b> provided_config  |
| <b>ip-router kernel trace</b> packets   routes   redirect   interface   other   remnants   request   info<br>[detail send receive]   |
| <b>ip-router policy add filter</b> <number-or-string> [network <ipAddr/mask>   all   default]<br>[exact refines between <low-high>][host-net]  |
| <b>ip-router policy add optional-attributes-list</b> <number-or-string><br>[<standard-community-string>   <extended-community-string>] no-advertise   no-export  <br>no-export-subconfed   none  |
| <b>ip-router policy aggr-gen destination</b> <number-or-string> [source <number-or-string>]<br>[filter <number-or-string>]   [network <ipAddr/mask>   all   default] [exact refines  <br>between <low-high>] [preference <number>  restrict] [multicast unicast]                     |
| <b>ip-router policy create aggr-export-source</b> <number-or-string> [metric <number>   noagg  <br>restrict   sequence-number <num>]   |
| <b>ip-router policy create aggr-gen-dest</b> <number-or-string> [network <ipAddr/mask> default]<br>[type aggregate generation]   [preference <num>]   brief   bgp   noinstall   unicast   multicast  |
| <b>ip-router policy create aggr-gen-source</b> <number-or-string> protocol <string>  <br>autonomous-system <num>   aspath-regular-expression <string>   tag <num>  <br>preference <num>   origin <string>   optional-attributes-list <num-or-string>   restrict                      |



Table 28. ip-router Commands (Continued)

|  |
|--|
| <b>ip-router policy create aspath-export-source</b> <number-or-string><br>[ <b>aspath-regular-expression</b> <string>   <b>origin</b> <string>   <b>protocol bgp</b>   <b>sequence-number</b> <num>   <b>optional-attributes-list</b> <num-or-string>] [ <b>metric</b> <num>] [ <b>restrict</b> ]  |
| <b>ip-router policy create bgp-export-destination</b> <number-or-string> <b>autonomous-system</b> <num>   <b>add-optional-attributes-list</b> <num-or-string>   <b>del-optional-attributes-list</b> <num-or-string>   <b>metric</b> <num>   <b>restrict</b>   <b>noagg</b>   <b>sequence-number</b> <num>  |
| <b>ip-router policy create bgp-export-source</b> <number-or-string> <b>autonomous-system</b> <num>   <b>optional-attributes-list</b> <num-or-string>   <b>metric</b> <num>   <b>restrict</b>   <b>noagg</b>   <b>sequence-number</b> <num>   |
| <b>ip-router policy create bgp-import-source</b> <number-or-string> [ <b>autonomous-system</b> <num>]   [ <b>aspath-regular-expression</b> <string>   <b>origin</b> <value>] [ <b>optional-attribute-list</b> <num-or-string>] [ <b>preference</b> <num>   <b>restrict</b> ] [ <b>unicast</b> ] [ <b>multicast</b> ] [ <b>sequence-number</b> <num>] |
| <b>ip-router policy create direct-export-source</b> <number-or-string> <b>interface</b> <name-or-IPAddr>   <b>metric</b> <num>   <b>restrict</b>   <b>noagg</b>   <b>sequence-number</b> <num>   |
| <b>ip-router policy create filter</b> <number-or-string> [ <b>network</b> <ipAddr/mask>   <b>all</b>   <b>default</b> ] [ <b>exact</b>   <b>refines</b>   <b>between</b> <low-high>] [ <b>host-net</b> ]   |
| <b>ip-router policy create optional-attributes-list</b> <number-or-string><br>[<standard-community-string>   <extended-community-string>] <b>none</b>   <b>no-export</b>   <b>no-advertise</b>   <b>no-export-subconfed</b>  |
| <b>ip-router policy create ospfase-export-source</b> <number-or-string> { <b>metric</b> <num>   <b>restrict</b>   <b>noagg</b>   <b>tag</b> <num>   <b>sequence-number</b> <num>}  |
| <b>ip-router policy create ospf-export-destination</b> <number-or-string> <b>tag</b> <num>   [ <b>type 1 2</b> ]   <b>metric</b> <num>   <b>restrict</b>   <b>sequence-number</b> <num>  |
| <b>ip-router policy create ospf-export-source</b> <number-or-string> { <b>metric</b> <num>   <b>restrict</b>   <b>noagg</b>   <b>tag</b> <num>   <b>sequence-number</b> <num>}   |
| <b>ip-router policy create ospf-import-source</b> <number-or-string> <b>tag</b> <num>   <b>preference</b> <num>   <b>restrict</b>   <b>unicast</b>   <b>multicast</b>   <b>sequence-number</b> <num>   |
| <b>ip-router policy create ospfnssa-export-destination</b> <number-or-string> <b>tag</b> <num>   [ <b>type 1 2</b> ]   <b>metric</b> <num>   <b>restrict</b>   <b>sequence-number</b> <num>  |
| <b>ip-router policy create redirect-import-source</b> <number-or-string><br><b>interface</b> <name-or-IPAddr>   <b>gateway</b> <name-or-IPAddr>   <b>preference</b> <num>   <b>restrict</b>   <b>unicast</b>   <b>multicast</b>   <b>sequence-number</b> <num>   |
| <b>ip-router policy create rip-export-destination</b> <number-or-string><br>[ <b>interface</b> <name-or-IPAddr>   <b>all</b> ]   <b>gateway</b> <name-or-IPAddr>   <b>metric</b> <num>   <b>restrict</b>   <b>tag</b> <num>   <b>sequence-number</b> <num>   |

Table 28. ip-router Commands (Continued)

|   |
|---|
| <b>ip-router policy create rip-export-source</b> <number-or-string> <b>interface</b> <name-or-IPaddr>   <b>gateway</b> <name-or-IPaddr>   <b>metric</b> <num>   <b>restrict</b>   <b>tag</b> <num>   <b>noagg</b>   <b>sequence-number</b> <num>  |
| <b>ip-router policy create rip-import-source</b> <number-or-string> <b>interface</b> <name-or-IPaddr>   <b>gateway</b> <name-or-IPaddr>   <b>preference</b> <num>   <b>restrict</b>   <b>tag</b> <num>   <b>unicast</b>   <b>multicast</b>   <b>sequence-number</b> <num>   |
| <b>ip-router policy create static-export-source</b> <number-or-string> <b>interface</b>   <b>metric</b> <num>   <b>restrict</b>   <b>noagg</b>   <b>sequence-number</b> <num>   |
| <b>ip-router policy create tag-export-source</b> <number-or-string> <b>protocol</b> <string>   <b>tag</b> <num>   <b>metric</b> <num>   <b>restrict</b>   <b>sequence-number</b> <num>  |
| <b>ip-router policy export destination</b> <exp-dest-id> [ <b>source</b> <exp-src-id>] [ <b>filter</b> <filter-id>] [ <b>network</b> <ipAddr/mask>   <b>all</b>   <b>default</b> ] [ <b>exact</b>   <b>refines</b>   <b>between</b> <low-high>] [ <b>metric</b> <number>]   [ <b>restrict</b> ]   |
| <b>ip-router policy import source</b> <imp-src-id> [ <b>filter</b> <filter-id>] [ <b>network</b> <ipAddr/mask>   <b>all</b>   <b>default</b> ] [ <b>exact</b>   <b>refines</b>   <b>between</b> <low-high>] [ <b>preference</b> <number>] [ <b>restrict</b> ] [ <b>fromribs</b> <b>unicast</b>   <b>multicast</b>   <b>both</b> ] [ <b>unicast</b> ] [ <b>multicast</b> ] |
| <b>ip-router policy redistribute from-proto</b> <protocol> <b>to-proto</b> <protocol> [ <b>network</b> <ipAddr/mask>   <b>all</b>   <b>default</b> ] [ <b>exact</b>   <b>refines</b>   <b>between</b> <low-high>] [ <b>metric</b> <number>] [ <b>restrict</b> ] [ <b>source-as</b> <number>] [ <b>target-as</b> <number>] [ <b>tag</b> ] [ <b>ase-type</b> ]              |
| <b>ip-router policy summarize route</b> <ipAddr/mask>   <b>default</b> [ <b>from-network</b> <ipAddr/mask>] [ <b>exact</b>   <b>refines</b>   <b>between</b> <low-high>] [ <b>preference</b> <number>  <b>restrict</b> ] [ <b>unicast</b> ] [ <b>multicast</b> ] [ <b>source-proto</b> <protocol>] [ <b>type</b> <b>aggregate</b>   <b>generation</b> ] [ <b>brief</b> ]  |
| <b>ip-router set</b> {[ <b>trace-state</b> <b>on</b>   <b>off</b> ]   <b>trace-level</b> <num>   <b>max-bgjob-interval</b> <num>}   |
| <b>ip-router set trace-options</b> [ <b>all</b>   <b>none</b> ]   [ <b>startup</b>   <b>parse</b>   <b>yydebug</b>   <b>adv</b>   <b>symbols</b>   <b>iflist</b>   <b>general</b>   <b>state</b>   <b>normal</b>   <b>policy</b>   <b>task</b>   <b>timer</b>   <b>route</b> ]  |
| <b>ip-router show configuration-file</b> <b>active</b>   <b>permanent</b>   |
| <b>ip-router show rib</b> [ <b>detail</b> ]   |
| <b>ip-router show route</b> [<ip-addr-mask>  <b>default</b> ] [ <b>detail</b> ]   |
| <b>ip-router show state</b> [ <b>all</b> ] [ <b>memory</b> ] [ <b>timers</b> ] [ <b>to-file</b> ] [ <b>to-terminal</b> ] [ <b>task</b> <string>  <b>all</b>   <b>gii</b>   <b>icmp</b>   <b>inet</b>   <b>interface</b>   <b>krt</b>   <b>route</b> ]   |

# ip-router authentication add key-chain

## Purpose

Add a key to an existing key-chain.

## Format

**ip-router authentication add key-chain** [**key** *<string>*] [**type** **primary**|**secondary**]

## Mode

Configure.

## Parameters

|  |   |
|--|---|
| <b>key</b> <i>&lt;string&gt;</i>                 | Adds a new key to an existing key-chain. The key can be up to 16 characters long.   |
| <b>type</b><br><b>primary</b>   <b>secondary</b> | Specifies whether the key is a primary key or a secondary key within the key chain. |

## Restrictions

None.

## ip-router authentication create key-chain

### Purpose

Create a key-chain and associate an identifier with it.

### Format

**ip-router authentication create key-chain** [**key** <*string*>] [**type** **primary**|**secondary**] [**id**]

### Mode

Configure.

### Parameters

|  |  |
|--|--|
| <b>key</b> < <i>string</i> >                     | Specifies a key to be included in this key chain. The key can be up to 16 characters long.           |
| <b>type</b><br><b>primary</b>   <b>secondary</b> | Specifies whether the key is a primary key or a secondary key within the key chain.                  |
| <b>id</b>  | Specifies an integer between 1 and 255. This option is only necessary for MD5 authentication method. |

### Restrictions

None.

# ip-router find route

## Purpose

Find the active route in the RIB which the packet will use.

## Format

**ip-router find route** *<ipAddr>* [**ignore-state**]

## Mode

Enable.

## Parameters

|                       |   |
|-----------------------|---|
| <i>&lt;ipAddr&gt;</i> | Specifies the destination of the packet.  |
| <b>ignore-state</b>   | This optional parameter allows inactive routes to be considered in route determination. |

## Restrictions

None.

# ip-router global add

## Purpose

Add an interface or martian. Martians are invalid addresses that are rejected by the routing software.

## Format

**ip-router global add interface** *<name-or-IPaddr>*

**ip-router global add martian** *<ipAddr/mask>* **|default [host] [allow]**

## Mode

Configure.

## Parameters

|  |  |  |
|--|--|--|
| <b>interface</b><br><i>&lt;name-or-IPaddr&gt;</i>  | Makes an interface known to the IP router.     |  |
|  | <b>Note:</b>                                   | Enterasys recommends that you use alphabetic characters when defining interface names—purely numeric interfaces will be interpreted as IP addresses. The X-Pedition router will display interface names up to 32 characters in length. |
| <b>martian</b><br><i>&lt;ipAddr/mask&gt;</i> <b> </b><br><b>default [host]</b><br><b>[allow]</b> | Adds a martian. Specify the following options: |  |
|  | <i>&lt;ipAddr/mask&gt;</i>                     | The IP address and netmask for the martian.  |
|  | <b>default</b>                                 | Adds default martian.  |
|  | <b>host</b>                                    | Specifies that this martian is a host address.   |
|  | <b>allow</b>                                   | Allows a subset of a range that was disallowed.  |

## Restrictions

None.

# ip-router global set

## Purpose

Set various global parameters required by various protocols.

## Format

```
ip-router global set [autonomous-system <num1> loops <num2>]
[router-id <hostname-or-IPaddr>]
[interface { <interface-name>|all} [preference <num>] [down-preference <num>]
[passive] [autonomous-system <num>]]
[confederation-id <num>] [max-bgjob-interval <num>]
```

## Mode

Configure.

## Parameters

|  |  |
|--|--|
| <b>autonomous-system</b><br><num1> <b>loops</b> <num2> | The autonomous system number. <num1> sets the <b>as</b> number for the router. It is only required if the router is going to run BGP. Specify a number from 1 – 65534. <num2> controls the number of times the <b>as</b> may appear in the as-path. Default is 1. It is only required if the router is going to run protocols that support as-path, such as BGP.   |
| <b>router-id</b><br><hostname-or-IPaddr>               | The router ID for use by BGP and OSPF. The most preferred address is any address other than 127.0.0.1 on the loopback interface. If there are no secondary addresses on the loopback interface, then the default router ID is set to the address of the first interface which is in the up state that the X-Pedition router encounters (except the interface en0, which is the Control Module's interface). The address of a non point-to-point interface is preferred over the local address of a point-to-point interface. |

|   |   |
|---|---|
| <b>interface</b><br><interface-name>  <b>all</b><br><b>preference</b> <num><br><b>down-preference</b><br><num> <b>passive</b><br><b>autonomous-system</b><br><num><interface-name><br>>  <b>all</b> | Specify the following:<br><br>Specify an interface that was added using the <i>ip-router global add interface</i> command, or <b>all</b> for all interfaces.<br><br><b>Note:</b> Enterasys recommends that you use alphabetic characters when defining interface names—purely numeric interfaces will be interpreted as IP addresses. The X-Pedition router will display interface names up to 32 characters in length. |
| <b>preference</b> <num>   | Sets the preference for routes to this interface when it is up and functioning. Specify a number from 0 – 255. Default value is 0.  |
| <b>down-preference</b> <num>  | Sets the preference for routes to this interface when it is down. Specify a number from 0 – 255. Default value is 255.  |
| <b>passive</b>  | Prevents changing of route preference to this interface if it is down.  |
| <b>autonomous-system</b> <num>  | The AS that will be used to create as-path associated with the route created from the definition of this interface.   |
| <b>confederation-id</b><br><num>  | Sets the autonomous system number that is the identifier to the outside world for the BGP confederation. Number is 1 to 65535.  |
| <b>max-bgjob-interval</b><br><num>  | Sets the maximum time interval in seconds for which a background job would wait. The value can be from 4 to 600.  |

## Restrictions

None.



## **ip-router global set trace-level**

### **Purpose**

Set the trace level.

### **Format**

**ip-router global set trace-level** *<num>*

### **Mode**

Configure.

### **Parameters**

---

|                    |                                 |
|--------------------|---------------------------------|
| <i>&lt;num&gt;</i> | The value can be from 0 to 255. |
|--------------------|---------------------------------|

---

### **Restrictions**

None.

# ip-router global set trace-options

## Purpose

Set various trace options.

## Format

**ip-router global set trace-options** [**all**|**none**] | [[**startup**] [**parse**] [**debug**] [**adv**] [**symbols**] [**if-list**] [**general**] [**state**] [**normal**] [**policy**] [**task**] [**timer**] [**route**]]

## Mode

Configure.

## Parameters

|                |  |
|----------------|--|
| <b>all</b>     | Turn on all tracing.   |
| <b>none</b>    | Turn off all tracing for this protocol or peer.  |
| <b>startup</b> | Trace startup events.  |
| <b>parse</b>   | Trace lexical analyzer and parser of gated config files.                                     |
| <b>debug</b>   | Trace lexical analyzer and parser in detail.   |
| <b>adv</b>     | Trace allocation and freeing of policy blocks.   |
| <b>symbols</b> | Trace symbols read from kernel at startup.   |
| <b>if-list</b> | Trace the reading of the kernel interface list.  |
| <b>general</b> | Turn on normal and route tracing.  |
| <b>state</b>   | Trace state machine transitions in protocols.  |
| <b>normal</b>  | Trace normal protocol occurrences. The X-Pedition router always traces abnormal occurrences. |
| <b>policy</b>  | Traces the application of policy to imported and exported routes.                            |
| <b>task</b>    | Traces system interfaces and task processing associated with this protocol or peer.          |
| <b>timer</b>   | Traces timer usage by this protocol or peer.   |
| <b>route</b>   | Traces routing table changes for routes installed by this protocol or peer.                  |

## Restrictions

None.

# **ip-router global set trace-state**

## **Purpose**

Enable or disable tracing.

## **Format**

**ip-router global set trace-state on|off**

## **Mode**

Configure.

## **Parameters**

|            |   |
|------------|---|
| <b>on</b>  | Enables tracing.                              |
| <b>off</b> | Disables tracing. The default is <b>off</b> . |

## **Restrictions**

None.

## **ip-router global use provided\_config**

### **Purpose**

Causes the X-Pedition router to use the configuration file stored in the Control Module's NVRAM.

### **Format**

**ip-router global use provided\_config**

### **Mode**

Configure.

### **Parameters**

None.

### **Restrictions**

This command requires that you first copy the GateD configuration into the Control Module's NVRAM. To do this, enter the following command in Enable mode:

```
xp# copy tftp-server to gated.conf
TFTP server [10.50.89.88]? 10.50.89.88
Source filename [tmp/gated.conf]?
#####
%TFTP-I-XFERRATE, Received 5910 bytes in 0.1 seconds
```

# ip-router kernel trace

## Purpose

Provides trace capabilities between the Routing Information Base and the Forwarding Information Base. You can specify one or more kernel trace options.

## Format

**ip-router kernel trace** **packets** | **routes** | **redirect** | **interface** | **other** | **remnants** | **request** | **info**  
[**detail**|**send**|**receive**]

## Mode

Configure.

## Parameters

|                  |  |
|------------------|--|
| <b>packets</b>   | Packets exchanged with the kernel.   |
| <b>routes</b>    | Routes exchanged with the kernel.  |
| <b>redirect</b>  | Redirect messages received from the kernel.  |
| <b>interface</b> | Interface messages received from the kernel.   |
| <b>other</b>     | All other messages received from the kernel.   |
| <b>remnants</b>  | Routes read from the kernel when the X-Pedition routing process starts.  |
| <b>request</b>   | The X-Pedition routing process requests to Add/Delete/Change routes in the kernel forwarding table.                              |
| <b>info</b>      | Informational messages received from the routing socket, such as TCP loss, routing lookup failure, and route resolution request. |

## Restrictions

None.

# ip-router policy add filter

## Purpose

Adds to a route filter. Routes are specified by a set of filters that will match a certain set of routes by destination, or by destination and mask.

## Format

**ip-router policy add filter** <number-or-string> [**network** <ipAddr/mask> | **all** | **default**]  
[**exact**|**refines**|**between** <low-high>][**host-net**]

## Mode

Configure.

## Parameters

|   |   |
|---|---|
| <b>filter</b><br><number-or-string>                           | Specifies the identifier of the route filter.   |
| <b>network</b><br><ipAddr/mask>   <b>all</b>   <b>default</b> | <p>Specifies networks that are to be filtered. Matching usually requires both an address and a mask, although the mask can be implied. If no additional options qualifying the networks to be filtered are specified, then any destination that falls in the range implied by this network-specification is matched, so the mask of the destination is ignored. If a natural network is specified, the network, any subnets, and any hosts will be matched. If you specify the <b>exact</b>, <b>refines</b>, or <b>between</b> parameters, the mask of the destination is also considered.</p> <p>The <b>all</b> keyword matches anything. It is equivalent to the network specification of 0.0.0.0/0.0.0.0.</p> <p>The <b>default</b> keyword matches the default route. To match, the address must be the default address and the mask must be all zeros. This is equivalent to the network specification of 0.0.0.0/0.0.0.0 along with the exact option.</p> |
| <b>exact</b>  | Specifies that the mask of the routes to be filtered must match the supplied mask exactly. This is used to match a network, but not subnets or hosts of that network  |
| <b>refines</b>  | Specifies that the mask of the routes to be filtered must be more specific (i.e., longer) than the supplied mask. This is used to match subnets.  |

---

|                           |  |
|---------------------------|--|
| <b>between</b> <low-high> | Specifies that the mask of the destination must be as or more specific (i.e., as long as or longer) than the lower limit (the first number parameter) and no more specific (i.e., as long as or shorter) than the upper limit (the second parameter).                            |
| <b>host-net</b>           | This option qualifies that the specified network is a host. To match, the address must exactly match the specified and the network mask must be a host mask (i.e., all ones). This is equivalent to a network specification of host/255.255.255.255 along with the exact option. |

---

## Restrictions

None.

# ip-router policy add optional-attributes-list

## Purpose

Expands a previously created optional-attributes-list.

## Format

**ip-router policy add optional-attributes-list** *<number-or-string>*  
[*<standard-community-string>* | *<extended-community-string>*] **no-advertise** | **no-export** |  
**no-export-subconfed** | **none**

## Mode

Configure.

## Parameters

|  |  |  |
|--|--|--|
| <i>&lt;number-or-string&gt;</i>          | Specifies the identifier for the optional attributes list you are expanding.   |  |
| <i>&lt;standard-community-string&gt;</i> | Is a standard community string in the form:<br><i>&lt;AS-identifier&gt;:&lt;community-identifier&gt;</i>                 |  |
|  | <i>&lt;AS-identifier&gt;</i>   | Autonomous system number. Can be any value from 0 to 65535.  |
|  | <i>&lt;community-identifier&gt;</i>  | Community identifier. Can be any value from 0 to 65535.  |
| <i>&lt;extended-community-string&gt;</i> | Is an extended community string, in the form:<br><i>&lt;type&gt;:{&lt;AS-identifier&gt;   &lt;IPaddr&gt;}:&lt;id&gt;</i> |  |
|  | <i>&lt;type&gt;</i>  | Type of this extended community. You can specify one of the following:<br><br><b>target</b> Target community identifies the destination to which a router is going.<br><br><b>origin</b> Origin community identifies where a route originated. |
|  | <i>&lt;AS-identifier&gt;</i>   | Autonomous system number. Can be any value from 1 to 65535.  |
|  | <i>&lt;IPaddr&gt;</i>  | IP address.  |
|  | <i>&lt;id&gt;</i>  | ID of the extended community that identifies the local provider. It is two bytes long when used IP addresses and four bytes long when used with AS numbers.  |
|  |  |  |



|                            |  |
|----------------------------|--|
| <b>no-advertise</b>        | Specifies that all routes received with this attribute value <i>will not</i> be advertised to other BGP peers.   |
| <b>no-export</b>           | Specifies that all routes received with this attribute value will not be advertised outside a BGP confederation boundary.  |
| <b>no-export-subconfed</b> | Specifies that all routes received with this attribute value <i>will not</i> be advertised to external BGP peers (this includes peers in other members autonomous systems inside a BGP confederation). |
| <b>none</b>                | This is not actually a community but a keyword that specifies that a received BGP update is only to be matched if no communities are present. It has no effect when originating communities.           |

## Restrictions

None.

# ip-router policy aggr-gen destination

## Purpose

Creates an aggregate or generate route. Assembles the building blocks constructed by the policy create/add commands:

**ip-router policy create aggr-gen-dest**  
**ip-router policy create aggr-gen-source**  
**ip-router policy create/add filter**

## Format

**ip-router policy aggr-gen destination** <number-or-string> [**source** <number-or-string>]  
[**filter** <number-or-string>] | [**network** <ipAddr/mask> | **all** | **default**] [**exact**| **refines** |  
**between** <low-high>] [**preference** <number>| **restrict**] [**multicast**|**unicast**]

## Mode

Configure.

## Parameters

|  |   |
|--|---|
| <b>destination</b><br><number-or-string>                         | Is the identifier of the aggregate-destination that specifies the aggregate/summarized route.   |
| <b>source</b><br><number-or-string>                              | Is the identifier of the aggregate-source that contributes to an aggregate route.   |
| <b>filter</b><br><number-or-string>                              | Specifies the filter for an aggregate/generate.   |
| <b>network</b><br><ipAddr/mask>   <b>all</b>  <br><b>default</b> | <p>Specifies networks that are to be aggregated. Matching usually requires both an address and a mask, although the mask can be implied. If no additional options qualifying the networks to be aggregated are specified, then any destination that falls in the range implied by this network-specification is matched, so the mask of the destination is ignored. If a natural network is specified, the network, any subnets, and any hosts will be matched. If you specify the <b>exact</b>, <b>refines</b>, or <b>between</b> parameters, the mask of the destination is also considered.</p> <p>The <b>all</b> keyword matches anything. It is equivalent to the network specification of 0.0.0.0/0.0.0.0.</p> <p>The <b>default</b> keyword matches the default route. To match, the address must be the default address and the mask must be all zeros. This is equivalent to the network specification of 0.0.0.0/0.0.0.0 along with the exact option.</p> |

|                               |   |
|-------------------------------|---|
| <b>exact</b>                  | Specifies that the mask of the routes to be aggregated must match the supplied mask exactly. This is used to match a network, but not subnets or hosts of that network  |
| <b>refines</b>                | Specifies that the mask of the routes to be aggregated must be more specific (i.e., longer) than the supplied mask. This is used to match subnets.  |
| <b>between</b> <low-high>     | Specifies that the mask of the destination must be as or more specific (i.e., as long as or longer) than the lower limit (the first number parameter) and no more specific (i.e., as long as or shorter) than the upper limit (the second parameter). |
| <b>preference</b><br><number> | Specifies the preference to be assigned to the resulting aggregate route.   |
| <b>restrict</b>               | Specifies that routes matching the filter are not to be imported.   |
| <b>unicast</b>                | Specifies that the resulting aggregate should be installed into the unicast rib. If neither unicast nor multicast is specified, the aggregate will belong to the unicast rib only.  |
| <b>multicast</b>              | Specifies that the resulting aggregate should be installed into the multicast rib. If neither unicast nor multicast is specified, the aggregate will belong to the unicast rib only.  |

## Restrictions

None.

## Example

Export aggregate routes into RIP:

```
xp# ip-router policy create aggr-gen-dest aggrDst140 network 140.1.0.0/16
xp#ip-router policy create aggr-gen-source allAggrSrc protocol all
xp#ip-router policy aggr-gen destination aggrDst140 source allAggrSrc network 140.1.1.0/24
xp#ip-router policy aggr-gen destination aggrDst140 source allAggrSrc network 140.1.2.0/24
xp#ip-router policy create rip-export-destination ripExpDst130 interface 130.1.1.1
xp#ip-router policy export destination ripExpDst130 source aggrExpSrc network 140.1.0.0/16
```

## ip-router policy create aggr-export-source

### Purpose

Used when creating an export policy. Constructs a source option for the **ip-router policy export destination** command.

### Format

**ip-router policy create aggr-export-source** <number-or-string> [**metric** <number> | **noagg** | **restrict** | **sequence-number** <num>]

### Mode

Configure.

### Parameters

|                              |  |
|------------------------------|--|
| <number-or-string>           | Specifies the identifier of the aggregate export source.   |
| <b>metric</b> <number>       | Specifies the metric to be associated with the exported routes.  |
| <b>noagg</b>                 | Specifies that any route matching the other filters must not be contributing to an aggregate route or it will not be exported. |
| <b>restrict</b>              | Specifies that nothing is exported from the specified source.  |
| <b>sequence-number</b> <num> | Specifies the position of this export source in the list of configured export destinations. The range is 1 to 128.             |

### Restrictions

None.

# ip-router policy create aggr-gen-dest

## Purpose

Used when creating an aggregate or generate route. Constructs a destination for the **ip-router policy aggr-gen destination** command.

## Format

**ip-router policy create aggr-gen-dest** <number-or-string> [**network** <ipAddr/mask>|**default**]  
[**type** aggregate|generation] | [**preference** <num>] | **brief** | **bgp** | **noinstall** | **unicast** | **multicast**

## Mode

Configure.

## Parameters

|   |  |
|---|--|
| <number-or-string>                            | Specifies the identifier of an aggregate-generation destination.   |
| <b>network</b> <ipAddr/mask>   <b>default</b> | Specifies the aggregate or generated route.  |
| <b>type</b> aggregate generation              | Specifies that the destination is an aggregate or generate.  |
| <b>preference</b> <num>                       | Specifies the preference to be assigned to the resulting aggregate route. The default preference is 130. Values can be from 0 to 255.  |
| <b>brief</b>                                  | Specifies that the AS path should be truncated to the longest common AS path. The default is to build an AS patch consisting of SETs and SEQUENCES of all contributing AS paths. |
| <b>bgp</b>                                    | Specifies that the BGP rules will be used to determine whether or not to include this route. This option is valid for <b>type aggregate</b> only.                                |
| <b>noinstall</b>                              | Used with <b>type generation</b> to specify routes that are not installed in the FIB.  |
| <b>unicast</b>                                | Specifies that this aggregate will be installed in the unicast RIB and contributing routes may be taken from the unicast RIB. The default is both unicast and multicast.         |
| <b>multicast</b>                              | Specifies that this aggregate will be installed in the multicast RIB and contributing routes may be taken from the multicast RIB.  |

## Restrictions

None.

# ip-router policy create aggr-gen-source

## Purpose

Used when creating an aggregate or generate route. Constructs a source option for the **ip-router policy aggr-gen destination** command.

## Format

**ip-router policy create aggr-gen-source** *<number-or-string>* **protocol** *<string>* | **autonomous-system** *<num>* | **aspath-regular-expression** *<string>* | **tag** *<num>* | **preference** *<num>* | **origin** *<string>* | **optional-attributes-list** *<num-or-string>* | **restrict**

## Mode

Configure.

## Parameters

|  |  |
|--|--|
| <i>&lt;number-or-string&gt;</i>                        | Specifies the identifier of an aggregate-generation source.  |
| <b>protocol</b> <i>&lt;string&gt;</i>                  | Specifies the protocol of the contributing aggregate source. Specify one of the following:<br><b>all</b><br><b>static</b><br><b>direct</b><br><b>aggregate</b><br><b>rip</b><br><b>ospf</b><br><b>bgp</b><br><b>ospfase</b>              |
| <b>autonomous-system</b> <i>&lt;num&gt;</i>            | Restricts selection of routes to those learned from the specified autonomous system. This selection may also be carried out by using route filters to explicitly list the set of routes to be accepted. Specify a number from 1 – 65534. |
| <b>aspath-regular-expression</b> <i>&lt;string&gt;</i> | Restricts selection of routes to those specified by the aspath. The allowable strings are described in RFC1164.  |
| <b>tag</b> <i>&lt;num&gt;</i>                          | Restricts selection of routes to those identified by a tag.  |
| <b>preference</b> <i>&lt;num&gt;</i>                   | Specifies the preference to assign to the contributing routes.   |

|   |   |
|---|---|
| <b>origin</b> <string>                          | Specifies where the route originated and should match one of the following:<br><b>any</b> The origin attribute can be IGP, EGP or incomplete.<br><b>igp</b> The origin attribute should be IGP.<br><b>egp</b> The origin attribute should be EGP.<br><b>incomplete</b> The origin attribute should be incomplete. |
| <b>optional-attributes-list</b> <num-or-string> | Specifies the identifier of the <b>optional-attributes-list</b> which is defined from the <b>ip-router policy create optional-attributes-list</b> command. The <b>optional-attribute-list</b> creates the community string or extended community string for identifying particular BGP attributes.                |
| <b>restrict</b>                                 | Indicates that these routes cannot contribute to the aggregate.   |

## Restrictions

None.

# ip-router policy create aspath-export-source

## Purpose

Used when creating an export policy. Constructs a source option for the **ip-router policy export destination** command. Used where routes to be exported are identified by the autonomous system path associated with them. This command applies only if you are using BGP.

You can only choose one Autonomous System (AS) path export source option. However, you can specify **metric** or **restrict** even if you specified **protocol**, **aspath-regular-expression**, or **origin**.

## Format

**ip-router policy create aspath-export-source** <number-or-string> [**aspath-regular-expression** <string> | **origin** <string> | **protocol bgp** | **sequence-number** <num> | **optional-attributes-list** <num-or-string>] [**metric** <num>] [**restrict**]

## Mode

Configure.

## Parameters

|   |   |
|---|---|
| <number-or-string>                              | Specifies a name or number for the AS path export source.   |
| <b>aspath-regular-expression</b> <string>       | Specifies an aspath regular expression which should be satisfied for the route to be exported. The allowable strings are described in RFC 1164.   |
| <b>origin</b> <string>                          | Specifies whether the origin of the routes to be exported was an interior gateway or exterior gateway protocol. Specify one of the following:<br><b>any</b> The origin attribute can be IGP, EGP or incomplete.<br><b>igp</b> The origin attribute should be IGP.<br><b>egp</b> The origin attribute should be EGP.<br><b>incomplete</b> The origin attribute should be incomplete. |
| <b>protocol bgp</b>                             | Specifies that BGP routes matching the specified aspath regular expression should be considered as potential sources for export.  |
| <b>sequence-number</b> <num>                    | Specifies the position of this export source in the list of configured export sources. Enter a value between 1 and 128, inclusive.  |
| <b>optional-attributes-list</b> <num-or-string> | Specifies the identifier for the optional-attributes-list which identifies the community attributes of the routes to be exported.   |
| <b>metric</b> <num>                             | Specifies metric associated with the exported routes.   |
| <b>restrict</b>                                 | Specifies that nothing is exported from the specified source.   |



## **Restrictions**

None.

# ip-router policy create bgp-export-destination

## Purpose

Used when creating an export policy. Constructs a destination for the **ip-router policy export destination** command. Used as an export destination for BGP routes.

## Format

**ip-router policy create bgp-export-destination** *<number-or-string>* **autonomous-system** *<num>* | **add-optional-attributes-list** *<num-or-string>* | **del-optional-attributes-list** *<num-or-string>* | **metric** *<num>* | **restrict** | **noagg** | **sequence-number** *<num>*

## Mode

Configure.

## Parameters

|  |   |
|--|---|
| <i>&lt;number-or-string&gt;</i>                                  | Creates a BGP export destination and associates an identifier (tag) with it.  |
| <b>autonomous-system</b> <i>&lt;num&gt;</i>                      | Specifies the autonomous system of the peer-group to which we would be exporting. Specify a number from 1 – 65535.  |
| <b>add-optional-attributes-list</b> <i>&lt;num-or-string&gt;</i> | Specifies the identifier of the optional-attributes-list which contains the optional attributes which are to be sent along with these exported routes. This option may be used to send the BGP community attribute. Any communities specified in the optional-attributes-list are sent in addition to any received with the route or those specified with the <b>set peer-group</b> or <b>set peer-host</b> commands. |
| <b>del-optional-attributes-list</b> <i>&lt;num-or-string&gt;</i> | Specifies the identifier of the optional-attributes-list which contains the optional attributes to be deleted from routes when they are exported.   |
| <b>metric</b> <i>&lt;num&gt;</i>                                 | Specifies the metric to be associated with the BGP exported routes.   |
| <b>restrict</b>  | Restricts the export of BGP routes to the specified destination.  |
| <b>noagg</b>   | Specifies that any route matching the other filters, will be exported only if it is not be contributing to an aggregate.  |
| <b>sequence-number</b> <i>&lt;num&gt;</i>                        | Specifies the relative position of this export-destination in a list of bgp export-destinations. Enter a value between 1 and 128, inclusive.  |

## Restrictions

None.

# ip-router policy create bgp-export-source

## Purpose

Used when creating an export policy. Constructs a source option for the **ip-router policy export destination** command. Use as a source for exporting bgp routes.

## Format

**ip-router policy create bgp-export-source** *<number-or-string>* **autonomous-system** *<num>* | **optional-attributes-list** *<num-or-string>* | **metric** *<num>* | **restrict** | **noagg** | **sequence-number** *<num>*

## Mode

Configure.

## Parameters

|  |  |
|--|--|
| <i>&lt;number-or-string&gt;</i>                              | Creates a BGP export source and associates an identifier (tag) with it.  |
| <b>autonomous-system</b> <i>&lt;num&gt;</i>                  | Specifies the autonomous system of the peer-group from which we would be exporting. A route filter could alternatively be used to explicitly list a set of routes to be accepted. Specify a number from 1 – 65534. |
| <b>optional-attributes-list</b> <i>&lt;num-or-string&gt;</i> | Specifies the identifier of the optional-attributes-list which contains the optional attributes which are matched on routes received from the specified autonomous system.   |
| <b>metric</b> <i>&lt;num&gt;</i>                             | Specifies the metric to be associated with the BGP exported routes.  |
| <b>restrict</b>  | Restricts the export of BGP routes from the specified source.  |
| <b>noagg</b>   | Specifies that any route matching the other filters will be exported only if it is not contributing to an aggregate.   |
| <b>sequence-number</b> <i>&lt;num&gt;</i>                    | Specifies the position of this export source in the list of configured export destinations. Enter a value between 1 and 128, inclusive.  |

## Restrictions

None.

# ip-router policy create bgp-import-source

## Purpose

Used when creating an import policy. Constructs the source for the **ip-router policy import source** command. A source for importing BGP routes.

## Format

**ip-router policy create bgp-import-source** *<number-or-string>* [**autonomous-system** *<num>*] | [**aspath-regular-expression** *<string>* | **origin** *<value>*] [**optional-attribute-list** *<num-or-string>*] [**preference** *<num>* | **restrict**] [**unicast**] [**multicast**] [**sequence-number** *<num>*]

## Mode

Configure.

## Parameters

|  |  |
|--|--|
| <i>&lt;number-or-string&gt;</i>                        | Creates a BGP import source and associates an identifier (tag) with it.  |
| <b>autonomous-system</b> <i>&lt;num&gt;</i>            | Specifies the autonomous system of the peer-group from which we would be exporting. A route filter could alternatively be used to explicitly list a set of routes to be accepted. Specify a number from 1 – 65534.   |
| <b>aspath-regular-expression</b> <i>&lt;string&gt;</i> | Specifies the as path regular expression that must be satisfied for the route to be exported. A route filter could alternatively be used to explicitly list a set of routes to be announced.   |
| <b>origin</b> <i>&lt;value&gt;</i>                     | Specifies the origin attribute. Specify one of the following:<br><br><b>any</b> Specifies that the origin attribute can be any one of <b>igp</b> , <b>egp</b> and <b>incomplete</b> .<br><br><b>igp</b> Specifies that the origin attribute of the imported routes is IGP.<br><br><b>egp</b> Specifies that the origin attribute of the imported routes is EGP.<br><br><b>incomplete</b> Specifies that the origin attribute of the imported routes is incomplete. |

|   |  |
|---|--|
| <b>optional-attribute-list</b> <i>&lt;num-or-string&gt;</i> | Specifies the identifier of the optional-attribute-list. This option allows the specification of import policy based on the path attributes found in the BGP update. If multiple communities are specified in the aspath-opt option, only updates carrying all of the specified communities will be matched. If none is specified, only updates lacking the community attribute will be matched. |
| <b>preference</b> <i>&lt;num&gt;</i>                        | Specifies the preference to be associated with the BGP imported routes.  |
| <b>fromribs unicast   multicast   both</b>                  | Specifies the RIB from which a route will be imported. The default is both.  |
| <b>unicast</b>  | Specifies the routes will be imported to the unicast RIB. If neither unicast or multicast is specified then the routes will be imported to the unicast RIB only.   |
| <b>multicast</b>  | Specifies that the routes will be imported to the multicast RIB. If neither unicast or multicast is specified then the routes will be imported to the unicast RIB only.  |
| <b>restrict</b>   | Specifies that nothing is exported from the specified source.  |
| <b>sequence-number</b> <i>&lt;num&gt;</i>                   | Indicates the position this bgp import source will have in a list of BGP import sources. Enter a value between 1 and 128, inclusive.   |

## Restrictions

None.

# ip-router policy create direct-export-source

## Purpose

Used when creating an export policy. Constructs a source option for the **ip-router policy export destination** command. An export source for interface routes.

## Format

**ip-router policy create direct-export-source** <number-or-string> **interface** <name-or-IPaddr> | **metric** <num> | **restrict** | **noagg** | **sequence-number** <num>

## Mode

Configure.

## Parameters

|                                      |   |
|--------------------------------------|---|
| <number-or-string>                   | Creates a source for exporting <b>interface (direct)</b> routes and associates an identifier with it.   |
| <b>interface</b><br><name-or-IPaddr> | This option qualifies that the direct routes should be associated with the specific interface.<br><br><b>Note:</b> Enterasys recommends that you use alphabetic characters when defining interface names—purely numeric interfaces will be interpreted as IP addresses. The X-Pedition router will display interface names up to 32 characters in length. |
| <b>metric</b> <num>                  | Specifies the metric to be associated with the exported routes.   |
| <b>restrict</b>                      | Restricts the export of routes from the specified source.   |
| <b>noagg</b>                         | Specifies that any route matching the other filters, will be exported only if it is not be contributing to an aggregate.  |
| <b>sequence-number</b><br><num>      | Specifies the position of this export source in the list of configured export destinations. Enter a value between 1 and 128, inclusive.   |

## Restrictions

None.

# ip-router policy create filter

## Purpose

Used when creating an import, export, or aggr-gen policy. Constructs a filter option for policy commands:

**ip-router policy export destination**  
**ip-router policy import source**  
**ip-router policy aggr-gen destination**

Creates a route filter. Routes are filtered by specifying a set of filters that will match a certain set of routes by destination, or by destination and mask.

## Format

**ip-router policy create filter** <number-or-string> [**network** <ipAddr/mask> | **all** | **default**]  
 [**exact** | **refines** | **between** <low-high>] [**host-net**]

## Mode

Configure.

## Parameters

|  |   |
|--|---|
| <b>filter</b><br><number-or-string>                          | Specifies the identifier of the route filter.   |
| <b>network</b><br><IP-address>   <b>all</b>   <b>default</b> | <p>Specifies networks which are to be filtered. Matching usually requires both an address and a mask, although the mask can be implied. If no additional options qualifying the networks to be filtered are specified, then any destination that falls in the range implied by this network-specification is matched, so the mask of the destination is ignored. If a natural network is specified, the network, any subnets, and any hosts will be matched. If you specify the <b>exact</b>, <b>refines</b>, or <b>between</b> parameter, the mask of the destination is also considered.</p> <p>The <b>all</b> keyword matches anything. It is equivalent to the network specification of 0.0.0.0/0.0.0.0.</p> <p>The <b>default</b> keyword matches the default route. To match, the address must be the default address and the mask must be all zeros. This is equivalent to the network specification of 0.0.0.0/0.0.0.0 along with the exact option.</p> |
| <b>exact</b>   | Specifies that the mask of the routes to be filtered must match the supplied mask exactly. This is used to match a network, but not subnets or hosts of that network  |

|  |  |
|--|--|
| <b>refines</b>                         | Specifies that the mask of the routes to be filtered must be more specific (i.e., longer) than the supplied mask. This is used to match subnets.   |
| <b>between</b> <i>&lt;low-high&gt;</i> | Specifies that the mask of the destination must be as or more specific (i.e., as long as or longer) than the lower limit (the first number parameter) and no more specific (i.e., as long as or shorter) than the upper limit (the second parameter).                |
| <b>host-net</b>                        | Qualifies that the specified network is a host. To match, the address must exactly match the specified and the network mask must be a host mask (i.e., all ones). This is equivalent to a network specification of host/255.255.255.255 along with the exact option. |

## Restrictions

None.



# ip-router policy create optional-attributes-list

## Purpose

Creates an optional-attributes-list for BGP and associates an identifier (tag) with the list.

## Format

**ip-router policy create optional-attributes-list** *<number-or-string>*  
 [*<standard-community-string>* | *<extended-community-string>*] **none** | **no-export** | **no-advertise** |  
**no-export-subconfed**

## Mode

Configure.

## Parameters

|  |  |  |
|--|--|--|
| <i>&lt;number-or-string&gt;</i>          | Specifies the identifier for the attributes list.  |  |
| <i>&lt;standard-community-string&gt;</i> | Is a standard community string in the form:<br><i>&lt;AS-identifier&gt;:&lt;community-identifier&gt;</i>                 |  |
|  | <i>&lt;AS-identifier&gt;</i>   | Autonomous system number. Can be any value from 0 to 65535.  |
|  | <i>&lt;community-identifier&gt;</i>  | Community identifier. Can be any value from 0 to 65535.  |
| <i>&lt;extended-community-string&gt;</i> | Is an extended community string, in the form:<br><i>&lt;type&gt;:{&lt;AS-identifier&gt;   &lt;IPaddr&gt;}:&lt;id&gt;</i> |  |
|  | <i>&lt;type&gt;</i>  | Type of this extended community. You can specify one of the following:<br><br><b>target</b> Target community identifies the destination to which a router is going.<br><br><b>origin</b> Origin community identifies where a route originated. |
|  | <i>&lt;AS-identifier&gt;</i>   | Autonomous system number. Can be any value from 1 to 65535.  |
|  | <i>&lt;IPaddr&gt;</i>  | IP address.  |
|  | <i>&lt;id&gt;</i>  | ID of the extended community that identifies the local provider. It is two bytes long when used IP addresses and four bytes long when used with AS numbers.  |

|                            |   |
|----------------------------|---|
| <b>none</b>                | This is not actually a community but a keyword that specifies that a received BGP update is only to be matched if no communities are present. It has no effect when originating communities.                |
| <b>no-export</b>           | Special community that indicates the routes associated with this attribute must not be advertised outside a BGP confederation boundary.   |
| <b>no-advertise</b>        | Special community indicating that the routes associated with this attribute must not be advertised to other BGP peers.  |
| <b>no-export-subconfed</b> | Special community indicating the routes associated with this attribute must not be advertised to external BGP peers. (This includes peers in other members' autonomous systems inside a BGP confederation.) |

## Restrictions

None.

# ip-router policy create ospfase-export-source

## Purpose

Used when creating an export policy. Constructs a source option for the **ip-router policy export destination** command. A source for exporting OSPF-ASE routes into other protocols.

## Format

**ip-router policy create ospfase-export-source** <number-or-string> {**metric** <num> | **restrict** | **noagg** | **tag** <num> | **sequence-number** <num>}

## Mode

Configure.

## Parameters

|                              |   |
|------------------------------|---|
| <number-or-string>           | Creates an OSPFASE export source and associates an identifier with it.  |
| <b>metric</b> <num>          | Specifies the metric to be associated with the exported routes.   |
| <b>restrict</b>              | Specifies that nothing is to be exported from this source.  |
| <b>noagg</b>                 | Specifies that any route match the other filters will not be exported if it contributes to an aggregate.                                |
| <b>tag</b> <num>             | Specifies the tag to be associated with the exported routes.  |
| <b>sequence-number</b> <num> | Specifies the position of this export source in the list of configured export destinations. Enter a value between 1 and 128, inclusive. |

## Restrictions

At least one of the following parameters is required: **tag**, **metric**, **restrict**, or **sequence-number**.

## ip-router policy create ospf-export-destination

### Purpose

Used when creating an export policy. Constructs a destination for the **ip-router policy export destination** command. A destination for exporting routes into OSPF.

### Format

**ip-router policy create ospf-export-destination** <number-or-string> **tag** <num> | [**type 1|2**] | **metric** <num> | **restrict** | **sequence-number** <num>

### Mode

Configure.

### Parameters

|                              |  |
|------------------------------|--|
| <number-or-string>           | Creates an OSPF export destination and associates an identifier with it.   |
| <b>tag</b> <num>             | Tag to be associated with exported OSPF routes.  |
| <b>type 1 2</b>              | Specifies that OSPF routes to be exported are type 1 or type 2 ASE routes. Specify 1 or 2.   |
| <b>metric</b> <num>          | Specifies the metric to be associated with the exported routes.  |
| <b>restrict</b>              | Restricts the export of the specified routes.  |
| <b>sequence-number</b> <num> | Specifies the position of this export destination in the list of configured export destinations. Enter a value between 1 and 128, inclusive. |

### Restrictions

It is not possible to create OSPF intra- or inter-area routes by exporting routes from the routing table into OSPF. You can only export from the routing table into OSPF ASE routes.

# ip-router policy create ospf-export-source

## Purpose

Used when creating an export policy. Constructs a source option for the **ip-router policy export destination** command. A source for exporting OSPF routes into other protocols.

## Format

**ip-router policy create ospf-export-source** <number-or-string> { **metric** <num> | **restrict** | **noagg** | **tag** <num> | **sequence-number** <num> }

## Mode

Configure.

## Parameters

|                              |   |
|------------------------------|---|
| <number-or-string>           | Creates an OSPF export source and associates an identifier with it.   |
| <b>metric</b> <num>          | Specifies the metric to be associated with the exported routes.   |
| <b>restrict</b>              | Specifies that nothing is to be exported from this source.  |
| <b>noagg</b>                 | Specifies that any route match the other filters will not be exported if it contributes to an aggregate.                                |
| <b>tag</b> <num>             | Specifies the tag to be associated with the exported routes.  |
| <b>sequence-number</b> <num> | Specifies the position of this export source in the list of configured export destinations. Enter a value between 1 and 128, inclusive. |

## Restrictions

At least one of the following parameters is required: **tag**, **metric**, **restrict**, or **sequence-number**.

# ip-router policy create ospf-import-source

## Purpose

Used when creating an import policy. Constructs a source for the **ip-router policy import source** command. A source for importing OSPF routes.

## Format

**ip-router policy create ospf-import-source** <number-or-string> **tag** <num> | **preference** <num> | **restrict** | **unicast** | **multicast** | **sequence-number** <num>

## Mode

Configure.

## Parameters

|                              |  |
|------------------------------|--|
| <number-or-string>           | Creates an OSPF import source and associates an identifier with it.  |
| <b>tag</b> <num>             | Tag to be associated with the imported routes.   |
| <b>preference</b> <num>      | Preference associated with the imported OSPF routes.   |
| <b>restrict</b>              | Specifies that matching ospf-ase routes are not imported.  |
| <b>unicast</b>               | Specifies that the imported routes will be installed in the unicast RIB. If neither unicast or multicast is specified, the routes will belong to the unicast RIB only.   |
| <b>multicast</b>             | Specifies that the imported routes will be installed in the multicast RIB. If neither unicast or multicast is specified, the routes will belong to the unicast RIB only. |
| <b>sequence-number</b> <num> | Specifies the position of this import source in the list of configured import sources. Enter a value between 1 and 128, inclusive.                                       |

## Restrictions

None.

# ip-router policy create ospfnssa-export-destination

## Purpose

Used when creating an export policy. Constructs a destination for the **ip-router policy export destination** command. A destination for exporting routes into OSPFNSSA.

## Format

**ip-router policy create ospfnssa-export-destination** *<number-or-string>* **tag** *<num>* | **[type 1|2]** | **metric** *<num>* | **restrict** | **sequence-number** *<num>*

## Mode

Configure.

## Parameters

|   |  |
|---|--|
| <i>&lt;number-or-string&gt;</i>           | Creates an OSPFNSSA export destination and associates an identifier with it.                                     |
| <b>tag</b> <i>&lt;num&gt;</i>             | Tag to be associated with exported OSPFNSSA routes.  |
| <b>type 1 2</b>                           | Specifies that OSPFNSSA routes to be exported are type 1 or type 2 routes. Specify 1 or 2.                       |
| <b>metric</b> <i>&lt;num&gt;</i>          | Specifies the metric to be associated with the exported routes. Enter a value between 0 and 16777215, inclusive. |
| <b>restrict</b>                           | Restricts the export of the specified routes.  |
| <b>sequence-number</b> <i>&lt;num&gt;</i> | Specifies the position of this export destination in the list of configured export destinations.                 |

## Restrictions

None.

# ip-router policy create redirect-import-source

## Purpose

Used when creating an import policy. Constructs a source for the **ip-router policy import** command. A source for importing redirect routes.

## Format

**ip-router policy create redirect-import-source** *<number-or-string>*  
**interface** *<name-or-IPaddr>* | **gateway** *<name-or-IPaddr>* | **preference** *<num>* | **restrict** |  
**unicast** | **multicast** | **sequence-number** *<num>*

## Mode

Configure.

## Parameters

|   |   |
|---|---|
| <i>&lt;number-or-string&gt;</i>                   | Specifies an identifier for the redirect import source.   |
| <b>interface</b><br><i>&lt;name-or-IPaddr&gt;</i> | Indicates that only routes learned over specified interfaces are imported.<br><br><b>Note:</b> Enterasys recommends that you use alphabetic characters when defining interface names—purely numeric interfaces will be interpreted as IP addresses. The X-Pedition router will display interface names up to 32 characters in length. |
| <b>gateway</b><br><i>&lt;name-or-IPaddr&gt;</i>   | Indicates that only routes learned over specified gateways are imported.  |
| <b>preference</b> <i>&lt;num&gt;</i>              | Specifies the preference to be associated with the imported routes. Enter a value between 0 and 255, inclusive.   |
| <b>restrict</b>                                   | Indicates that nothing is imported from the specified source.   |
| <b>unicast</b>                                    | Specifies that imported routes should be installed into the unicast rib.  |
| <b>multicast</b>                                  | Specifies that imported routes should be installed into the multicast rib.<br><br><b>Note:</b> If neither unicast or multicast is specified, the routes will be imported to the unicast rib only.   |
| <b>sequence-number</b><br><i>&lt;num&gt;</i>      | Specifies the position this source will have in the list of import sources. Enter a value between 1 and 128, inclusive.   |

## Restrictions

None.



# ip-router policy create rip-export-destination

## Purpose

Used when creating an export policy. Constructs a destination for the ip-router policy export destination command. A destination for exporting routes into RIP.

## Format

**ip-router policy create rip-export-destination** *<number-or-string>*  
**[interface** *<name-or-IPaddr>* **| all] | gateway** *<name-or-IPaddr>* **| metric** *<num>* **| restrict |**  
**tag** *<num>* **| sequence-number** *<num>*

## Mode

Configure.

## Parameters

|   |  |
|---|--|
| <i>&lt;number-or-string&gt;</i>                             | Specifies an identifier for the RIP export destination:  |
| <b>interface</b> <i>&lt;name-or-IPaddr&gt;</i> <b>  all</b> | Specifies router interfaces over which to export routes. Specify <b>all</b> to export routes to all interfaces.<br><br><b>Note:</b> Enterasys recommends that you use alphabetic characters when defining interface names—purely numeric interfaces will be interpreted as IP addresses. The X-Pedition router will display interface names up to 32 characters in length. |
| <b>gateway</b> <i>&lt;name-or-IPaddr&gt;</i>                | Specifies the gateway that will receive the exported routes.   |
| <b>metric</b> <i>&lt;num&gt;</i>                            | Specifies the metric to be associated with the exported routes. Specify a number from 1 to 16.   |
| <b>restrict</b>   | Restricts the export of routes to the specified destination.   |
| <b>tag</b> <i>&lt;num&gt;</i>                               | Specifies a tag to be associated with the exported RIP routes. Enter a value between 1 and 65534, inclusive.   |
| <b>sequence-number</b> <i>&lt;num&gt;</i>                   | Specifies the position of the rip export destination in the list of configured export destinations. Enter a value between 1 and 128, inclusive.  |

## Restrictions

When you use this command in conjunction with the *gateway* option in **ip-router policy export**, you must use **rip add source-gateways** for each address indicated in the gateway option.

# ip-router policy create rip-export-source

## Purpose

Used when creating an export policy. Constructs a source option for the **ip-router policy export destination** command. A source for exporting RIP routes into other protocols.

## Format

**ip-router policy create rip-export-source** <number-or-string> **interface** <name-or-IPaddr> | **gateway** <name-or-IPaddr> | **metric** <num> | **restrict** | **tag** <num> | **noagg** | **sequence-number** <num>

## Mode

Configure.

## Parameters

|                                      |   |
|--------------------------------------|---|
| <number-or-string>                   | Specifies an identifier for the RIP export source:  |
| <b>interface</b><br><name-or-IPaddr> | Indicates that only routes learned over specified interfaces are exported.<br><br><b>Note:</b> Enterasys recommends that you use alphabetic characters when defining interface names—purely numeric interfaces will be interpreted as IP addresses. The X-Pedition router will display interface names up to 32 characters in length. |
| <b>gateway</b><br><name-or-IPaddr>   | Indicates that only routes learned over specified gateways are exported.  |
| <b>metric</b> <num>                  | Specifies the metric to be associated with the exported routes.   |
| <b>restrict</b>                      | Indicates that nothing is exported from the specified source.   |
| <b>tag</b> <num>                     | Specifies a tag to be associated with the exported RIP routes. Enter a value between 1 and 65534, inclusive.  |
| <b>noagg</b>                         | Specifies that any route matching the other filters will not be exported if it contributes to an aggregate.   |
| <b>sequence-number</b><br><num>      | Specifies the position of this export source in the list of configured export destinations. Enter a value between 1 and 128, inclusive.   |

## Restrictions

None.

# ip-router policy create rip-import-source

## Purpose

Used when creating an import policy. Constructs a source for the **ip-router policy import** command. A source for importing RIP routes.

## Format

**ip-router policy create rip-import-source** *<number-or-string>* **interface** *<name-or-IPaddr>* | **gateway** *<name-or-IPaddr>* | **preference** *<num>* | **restrict** | **tag** *<num>* | **unicast** | **multicast** | **sequence-number** *<num>*

## Mode

Configure.

## Parameters

|   |   |
|---|---|
| <i>&lt;number-or-string&gt;</i>                   | Specifies an identifier for the RIP import source.  |
| <b>interface</b><br><i>&lt;name-or-IPaddr&gt;</i> | Indicates that only routes learned over specified interfaces are imported.<br><br><b>Note:</b> Enterasys recommends that you use alphabetic characters when defining interface names—purely numeric interfaces will be interpreted as IP addresses. The X-Pedition router will display interface names up to 32 characters in length. |
| <b>gateway</b><br><i>&lt;name-or-IPaddr&gt;</i>   | Indicates that only routes learned over specified gateways are imported.  |
| <b>preference</b> <i>&lt;num&gt;</i>              | Specifies the preference to be associated with the imported routes.   |
| <b>restrict</b>                                   | Indicates that nothing is imported from the specified source.   |
| <b>tag</b> <i>&lt;num&gt;</i>                     | Specifies a tag to be associated with the imported RIP routes. Enter a value between 1 and 65534, inclusive.  |
| <b>unicast</b>                                    | Specifies that imported routes should be installed into the unicast rib.  |
| <b>multicast</b>                                  | Specifies that imported routes should be installed into the multicast rib.<br><br><b>Note:</b> If neither unicast or multicast is specified, the routes will be imported to the unicast rib only.   |
| <b>sequence-number</b><br><i>&lt;num&gt;</i>      | Specifies the position this source will have in the list of RIP import sources. Enter a value between 1 and 128, inclusive.   |

## **Restrictions**

None.

# ip-router policy create static-export-source

## Purpose

Used when creating an export policy. Constructs a source option for the **ip-router policy export destination** command. A source for exporting static routes into other protocols.

## Format

**ip-router policy create static-export-source** *<number-or-string>* **interface** | **metric** *<num>* | **restrict** | **noagg** | **sequence-number** *<num>*

## Mode

Configure.

## Parameters

|   |   |
|---|---|
| <i>&lt;number-or-string&gt;</i>           | Creates a source for exporting <b>static</b> routes and associates an identifier with it.   |
| <b>interface</b>                          | This option qualifies that the static routes should be associated with the specific interface.<br><br><b>Note:</b> Enterasys recommends that you use alphabetic characters when defining interface names—purely numeric interfaces will be interpreted as IP addresses. The X-Pedition router will display interface names up to 32 characters in length. |
| <b>metric</b> <i>&lt;num&gt;</i>          | Specifies the metric to be associated with the exported routes.   |
| <b>restrict</b>                           | Restricts the export of routes from the specified source.   |
| <b>noagg</b>                              | Specifies that if the route matches the other filters, it will not be exported if it contributes to an aggregate.   |
| <b>sequence-number</b> <i>&lt;num&gt;</i> | Specifies the position of this export source in the list of configured export destinations. Enter a value between 1 and 128, inclusive.   |

## Restrictions

None.

# ip-router policy create tag-export-source

## Purpose

Used when creating an export policy. Constructs a source option for the **ip-router policy export destination** command. An export source where routes to be exported are identified by the tag associated with them.

## Format

**ip-router policy create tag-export-source** *<number-or-string>* **protocol** *<string>* | **tag** *<num>* | **metric** *<num>* | **restrict** | **sequence-number** *<num>*

## Mode

Configure.

## Parameters

|   |  |
|---|--|
| <i>&lt;number-or-string&gt;</i>           | Specifies the identifier of an tag-export source.  |
| <b>protocol</b> <i>&lt;string&gt;</i>     | Specifies the protocol of the contributing source. Specify one of the following: <ul style="list-style-type: none"><li>• <b>all</b></li><li>• <b>static</b></li><li>• <b>direct</b></li><li>• <b>aggregate</b></li><li>• <b>rip</b></li><li>• <b>ospf</b></li><li>• <b>bgp</b></li></ul> |
| <b>tag</b> <i>&lt;num&gt;</i>             | Restricts selection of routes to those identified by a tag.  |
| <b>metric</b> <i>&lt;num&gt;</i>          | Specifies the metric to assign to the exported routes.   |
| <b>restrict</b>                           | Indicates that the matching routes are not exported.   |
| <b>sequence-number</b> <i>&lt;num&gt;</i> | Specifies the position of this export source in the list of configured export destinations. Enter a value between 1 and 128, inclusive.  |

## Restrictions

None.

# ip-router policy export destination

## Purpose

Creates an export policy from the various building blocks created by policy commands:

```
ip-router policy create aspath-export-source
ip-router policy create bgp-export-source
ip-router policy create direct-export-source
ip-router policy create ospf-export-source
ip-router policy create ospfase-export-source
ip-router policy create static-export-source
ip-router policy create aggr-export-source
ip-router policy create rip-export-source
ip-router policy create tag-export-source
ip-router policy create bgp-export-destination
ip-router policy create ospf-export-destination
ip-router policy create ospfnssa-export-destination
ip-router policy create rip-export-destination
ip-router policy create/add filter
```

## Format

```
ip-router policy export destination <exp-dest-id> [source <exp-src-id>]
[filter <filter-id>] [network <ipAddr/mask> | all | default] [exact|refines|between <low-high>]
[metric <number>] | [restrict]
```

## Mode

Configure.

## Parameters

|               |   |
|---------------|---|
| <exp-dest-id> | Is the identifier of the export-destination which determines where the routes are to be exported. If no routes to a particular destination are to be exported, then no additional parameters are required.  |
| <exp-src-id>  | If specified, is the identifier of the export-source which determines the source of the exported routes. If a export-policy for a given export-destination has more than one export-source, then the <b>ip-router policy export destination</b> <exp-dest-id> command should be repeated for each <exp-src-id>. |

|  |  |
|--|--|
| <b>&lt;filter-id&gt;</b>                                     | If specified, is the identifier of the route-filter associated with this export-policy. If there is more than one route-filter for any export-destination and export-source combination, then the <b>ip-router policy export destination &lt;exp-dest-id&gt; source &lt;exp-src-id&gt;</b> command should be repeated for each <filter-id>.  |
| <b>network</b><br><b>&lt;ipAddr/mask&gt; [all   default]</b> | <p>Specifies networks which are to be exported. Matching usually requires both an address and a mask, although the mask can be implied. If no additional options qualifying the networks to be exported are specified, then any destination that falls in the range implied by this network-specification is matched, so the mask of the destination is ignored. If a natural network is specified, the network, any subnets, and any hosts will be matched. If you specify the <b>exact</b>, <b>refines</b>, or <b>between</b> parameters, the mask of the destination is also considered.</p> <p>The <b>all</b> keyword matches anything. It is equivalent to the network specification of 0.0.0.0/0.0.0.0.</p> <p>The <b>default</b> keyword matches the default route. To match, the address must be the default address and the mask must be all zeros. This is equivalent to the network specification of 0.0.0.0/0.0.0.0 along with the exact option.</p> |
| <b>exact</b>   | Specifies that the mask of the routes to be exported must match the supplied mask exactly. This is used to match a network, but not subnets or hosts of that network   |
| <b>refines</b>   | Specifies that the mask of the routes to be exported must be more specific (i.e., longer) than the supplied mask. This is used to match subnets.   |
| <b>between &lt;low-high&gt;</b>                              | Specifies that the mask of the destination must be as or more specific (i.e., as long as or longer) than the lower limit (the first number parameter) and no more specific (i.e., as long as or shorter) than the upper limit (the second parameter).  |
| <b>restrict</b>  | Specifies that routes matching the filter are not to be exported.  |
| <b>metric &lt;number&gt;</b>                                 | Specifies the metric to be associated with the routes that match the specified filter.   |
| <b>unicast</b>   | Specifies that imported routes should be installed into the unicast rib.   |
| <b>multicast</b>   | Specifies that imported routes should be installed into the multicast rib.   |
|  | <p><b>Note:</b> If neither unicast or multicast is specified, the routes will be imported to the unicast rib only.</p>   |

## Restrictions

None.



## Example

Exporting all routes to OSPF, except for 10.10/16 network from BGP.

### Building Blocks

```
ip-router policy create ospf-export-destination ospfExpDst
ip-router policy create ospf-export-source ospfExpSrc type OSPF sequence-number 20
ip-router policy create ospf-export-source ospfAseExpSrc type OSPF-ASE sequence-number 10
ip-router policy create static-export-source statExpSrc sequence-number 30
ip-router policy create direct-export-source directExpSrc sequence-number 40
ip-router policy create bgp-export-source bgpExpSrc autonomous-system 65901 sequence-number 50
ip-router policy create filter net10 network 10.10/16
```

### Export Statements

```
ip-router policy export destination ospfExpDst source statExpSrc network all
ip-router policy export destination ospfExpDst source directExpSrc network all
ip-router policy export destination ospfExpDst source ospfExpSrc network all
ip-router policy export destination ospfExpDst source ospfAseExpSrc network all
ip-router policy export destination ospfExpDst source bgpExpSrc filter net10 network all
```

**Note:** The sequence-number option on the export-source statements causes the sources to be applied in ascending sequence-number order. If the sequence number is not used, the sources are ordered based on their name value. If the name is a number, the sources are applied in ascending number order. If the name is alphanumeric, the sources are applied in alphabetical order.

# ip-router policy import source

## Purpose

Creates an import policy from the various building blocks constructed by policy commands:

```
ip-router policy create bgp-import-source
ip-router policy create ospf-import-source
ip-router policy create redirect-import-source
ip-router policy create rip-import-source
ip-router policy create/add filter
```

## Format

```
ip-router policy import source <imp-src-id> [filter <filter-id>]
[network <ipAddr/mask> | all | default] [exact|refines|between <low-high>]
[preference <number>] [restrict] [fromribs unicast|multicast|both] [unicast] [multicast]
```

## Mode

Configure.

## Parameters

|                           |   |
|---------------------------|---|
| <i>&lt;imp-src-id&gt;</i> | Is the identifier of the import-source that determines the source of the imported routes. If no routes from a particular source are to be imported, then no additional parameters are required.   |
| <i>&lt;filter-id&gt;</i>  | If specified, is the identifier of the route-filter associated with this import-policy. If there is more than one route-filter for any import-source, then the <b>ip-router policy import source</b> <i>&lt;imp-src-id&gt;</i> command should be repeated for each <i>&lt;filter-id&gt;</i> . |

|  |  |
|--|--|
| <b>network</b><br><ipAddr/mask>   <b>all</b>  <br><b>default</b> | <p>Specifies networks which are to be imported. Matching usually requires both an address and a mask, although the mask can be implied. If no additional options qualifying the networks to be imported are specified, then any destination that falls in the range implied by this network-specification is matched, so the mask of the destination is ignored. If a natural network is specified, the network, any subnets, and any hosts will be matched. If you specify the <b>exact</b>, <b>refines</b>, or <b>between</b> parameters, the mask of the destination is also considered.</p> <p>The <b>all</b> keyword matches anything. It is equivalent to the network specification of 0.0.0.0/0.0.0.0.</p> <p>The <b>default</b> keyword matches the default route. To match, the address must be the default address and the mask must be all zeros. This is equivalent to the network specification of 0.0.0.0/0.0.0.0 along with the exact option.</p> |
| <b>exact</b>   | Specifies that the mask of the routes to be imported must match the supplied mask exactly. This is used to match a network, but not subnets or hosts of that network   |
| <b>refines</b>   | Specifies that the mask of the routes to be imported must be more specific (i.e., longer) than the supplied mask. This is used to match subnets.   |
| <b>between</b> <low-high>  | Specifies that the mask of the destination must be as or more specific (i.e., as long as or longer) than the lower limit (the first number parameter) and no more specific (i.e., as long as or shorter) than the upper limit (the second parameter).  |
| <b>preference</b> <num>  | Specifies the preference with which the imported routes that match the specified filter should be installed.   |
| <b>restrict</b>  | Specifies that routes matching the filter are not to be imported.  |
| <b>fromribs</b><br><b>unicast multicast both</b>                 | Applies only for BGP imports. It specifies the ribs from which a route will be imported.   |
| <b>unicast</b>   | Specifies that the imported routes should be installed into the unicast rib. If neither unicast nor multicast is specified, the routes will belong to the unicast rib only.  |
| <b>multicast</b>   | Specifies that the imported routes should be installed into the multicast rib. If neither unicast nor multicast is specified, the routes will belong to the unicast rib only.  |

## Restrictions

None.

## Example

Import a selected subset of routes from one RIP Trusted Gateway:

```
xp# ip-router policy create rip-import-source ripImpSrc144 gateway 140.1.1.41
xp# ip-router policy create import source ripImpSrc144 network all
xp# ip-router policy create import source ripImpSrc144 network 10.51.0.0/restrict
```

# ip-router policy redistribute

## Purpose

Creates a simple route redistribution policy.

## Format

```
ip-router policy redistribute from-proto <protocol> to-proto <protocol>
[network <ipAddr/mask> | all | default] [exact|refines|between <low-high>]
[metric <number>] [restrict] [source-as <number>] [target-as <number>] [tag] [ase-type]
```

## Mode

Configure.

## Parameters

|   |   |
|---|---|
| <b>from-proto</b><br><protocol>                               | Specifies the protocol of the source routes. The values for the from-proto parameter are <b>rip</b> , <b>ospf</b> , <b>bgp</b> , <b>direct</b> , <b>static</b> , <b>aggregate</b> , or <b>ospf-ase</b> .  |
| <b>to-proto</b> <protocol>                                    | Specifies the destination protocol where the routes are to be exported. The values for the to-proto parameter are <b>rip</b> , <b>ospf</b> , <b>bgp</b> , or <b>ospfnssa</b> .  |
| <b>network</b><br><ipAddr/mask>   <b>all</b>   <b>default</b> | <p>Provides a means to define a filter for the routes to be distributed. The network parameter defines a filter that is made up of an IP address and a mask. Routes that match the filter are considered as eligible for redistribution.</p> <p>Matching usually requires both an address and a mask, although the mask can be implied. If no additional options qualifying the networks to be redistributed are specified, then any destination that falls in the range implied by this network-specification is matched, so the mask of the destination is ignored. If a natural network is specified, the network, any subnets, and any hosts will be matched. If you specify the <b>exact</b>, <b>refines</b>, or <b>between</b> parameters, the mask of the destination is also considered.</p> <p>The <b>all</b> keyword matches anything. It is equivalent to the network specification of 0.0.0.0/0.0.0.0.</p> <p>The <b>default</b> keyword matches the default route. To match, the address must be the default address and the mask must be all zeros. This is equivalent to the network specification of 0.0.0.0/0.0.0.0 along with the exact option.</p> |
| <b>exact</b>  | Specifies that the mask of the routes to be redistributed must match the supplied mask exactly. This is used to match a network, but not subnets or hosts of that network.  |

|                           |  |
|---------------------------|--|
| <b>refines</b>            | Specifies that the mask of the routes to be redistributed must be more specific (i.e., longer) than the supplied mask. This is used to match subnets.  |
| <b>between</b> <low-high> | Specifies that the mask of the destination must be as or more specific (i.e., as long as or longer) than the lower limit (the first number parameter) and no more specific (i.e., as long as or shorter) than the upper limit (the second parameter).  |
| <b>restrict</b>           | Specifies that routes matching the filter are not to be redistributed.   |
| <b>metric</b>             | Indicates the metric to be associated with the redistributed routes.   |
| <b>tag</b>                | Tag to be associated with the exported OSPF routes.  |
| <b>ase-type</b>           | <p>Routes exported from the GateD routing table into OSPF default to type 1 ASEs. This default may be explicitly overridden here. Thus, this option should be used to specify if the routes are to be exported as OSPF Type 1 or Type 2 ASE routes.</p> <p><b>Note:</b> Each protocol (RIP, OSPF, and BGP) has a configurable parameter that specifies the default-metric associated with routes exported to that protocol. If a metric is not explicitly specified with the redistribute command, then it is inherited from the default-metric associated with the protocol to which the routes are being exported.</p> |

## Restrictions

None.

# ip-router policy summarize route

## Purpose

This command creates a simple aggregate or generation.

## Format

**ip-router policy summarize route** *<ipAddr/mask>* | **default** [**from-network** *<ipAddr/mask>*] [**exact** | **refines** | **between** *<low-high>*] [**preference** *<number>*] [**restrict**] [**unicast**] [**multicast**] [**source-proto** *<protocol>*] [**type aggregate**| **generation**] [**brief**]

## Mode

Configure.

## Parameters

|  |   |
|--|---|
| <b>route</b><br><i>&lt;ipAddr/mask&gt;</i>  <br><b>default</b> | The summarized network. Specify <b>default</b> for default networks.  |
| <b>from-network</b>  | Specifies the network to be summarized. If no additional options that qualify the networks to be filtered are specified, then any destination that falls in the range implied by this network specification is matched; the mask of the destination is ignored. If a natural network is specified, the network and any subnets and any hosts will be matched. |
| <b>exact</b>   | Specifies that the mask of the routes to be summarized must match the supplied mask exactly. This is used to match a network, but no subnets or hosts of that network.  |
| <b>refines</b>   | Specifies that the mask of the routes to be summarized must be more specific (i.e., longer) than the supplied mask. This is used to match subnets and/or hosts of a network, but not the network.   |
| <b>between</b> <i>&lt;low-high&gt;</i>                         | Specifies that the mask of the routes to be summarized must be as or more specific (i.e., as long as or longer) than the lower limit (the first number value) and no more specific (i.e., as long as or shorter) than the upper limit (the second number value).  |
| <b>preference</b> <i>&lt;num&gt;</i>                           | If specified, is the metric to be associated with the routes that match the filter.   |
| <b>restrict</b>  | If specified, routes that match the filter are not to be summarized.  |
| <b>unicast</b>   | Specifies that the resulting aggregate should be installed into the unicast rib. If neither unicast nor multicast is specified, the aggregate will belong to the unicast rib only.  |

|                                       |  |                       |
|---------------------------------------|--|-----------------------|
| <b>multicast</b>                      | Specifies that the resulting aggregate should be installed into the multicast rib. If neither unicast nor multicast is specified, the aggregate will belong to the unicast rib only. |                       |
| <b>source-proto</b><br><protocol>     | Specifies the protocol of the source routes. Specify one of the following:   |                       |
|                                       | <b>all</b>   | All protocols.        |
|                                       | <b>bgp</b>   | BGP routes.           |
|                                       | <b>direct</b>  | Direct routes.        |
|                                       | <b>isis-level-1</b>  | IS-IS level 1 routes. |
|                                       | <b>isis-level-2</b>  | IS-IS level 2 routes. |
|                                       | <b>ospf</b>  | OSPF routes.          |
|                                       | <b>rip</b>   | RIP routes.           |
|                                       | <b>static</b>  | Static routes.        |
| <b>type aggregate <br/>generation</b> | Specifies whether the object being created is an aggregate or a generation.  |                       |
| <b>brief</b>                          | Specifies that the AS path is to be truncated to the longest common AS path. The default is to build an AS path that consists of SETs and SEQUENCES of all contributing AS paths.    |                       |

## Restrictions

None.



# ip-router set

## Purpose

Sets various options on global unicast IP routing related parameters.

## Format

**ip-router set** {[**trace-state on|off**] | **trace-level** <num> | **max-bgjob-interval** <num>}

## Mode

Enable.

## Parameters

|                                 |  |
|---------------------------------|--|
| <b>trace-state on off</b>       | Sets the state of tracing. Use <b>on</b> to trace unicast routing events to a trace file or to a terminal (telnet/console). Use <b>off</b> to disable tracing of unicast routing events. |
| <b>trace-level</b> <num>        | Sets the trace level. The value can be from 0 to 255.  |
| <b>max-bgjob-interval</b> <num> | Sets the maximum time interval in seconds for which a background job would wait. The value can be from 4 to 600.   |

## Restrictions

None.

# ip-router set trace-options

## Purpose

Sets various trace options on global unicast IP routing related parameters.

## Format

**ip-router set trace-options** [**all** | **none**] [**startup** | **parse** | **yydebug** | **adv** | **symbols** | **iflist** | **general** | **state** | **normal** | **policy** | **task** | **timer** | **route**]

## Mode

Enable.

## Parameters

|                |  |
|----------------|--|
| <b>all</b>     | Turns on all tracing.  |
| <b>none</b>    | Specifies that all tracing should be turned off for this protocol or peer.   |
| <b>startup</b> | Trace startup events.  |
| <b>parse</b>   | Trace the lexical analyzer and parser. This should only be required by those users who are supplying their own Configuration File. |
| <b>yydebug</b> | Trace the lexical analyzer and parser in detail.   |
| <b>adv</b>     | Trace the allocation of and freeing of policy blocks.  |
| <b>symbols</b> | Trace symbols read from the kernel at startup.   |
| <b>iflist</b>  | Trace the reading of the kernel interface list.  |
| <b>general</b> | Turns on normal and route tracing.   |
| <b>state</b>   | Traces state machine transitions in the protocols.   |
| <b>normal</b>  | Traces normal protocol occurrences. Abnormal protocol occurrences are always traced.   |
| <b>policy</b>  | Traces application of protocol and user-specified policy to routes being imported and exported.                                    |
| <b>task</b>    | Traces system interface and processing associated with this protocol or peer.  |
| <b>timer</b>   | Traces timer usage used by this protocol or peer.  |
| <b>route</b>   | Traces routing table changes for routes installed by this protocol or peer.  |

## Restrictions

None.

# **ip-router show configuration file**

## **Purpose**

Display the active or startup configuration file in GateD format. This command displays the GateD configuration for both IPv4 and IPv6.

## **Format**

**ip-router show configuration-file active|permanent**

## **Mode**

Enable.

## **Parameters**

|                  |  |
|------------------|--|
| <b>active</b>    | Shows the active GateD configuration file in RAM. This is the default. |
| <b>permanent</b> | Shows the permanent GateD configuration file in NVRAM, if available.   |

## **Restrictions**

None.

# ip-router show rib

## Purpose

Display routing information base, for both IPv4 and IPv6.

## Format

**ip-router show rib [detail]**

## Mode

Enable.

## Description

The **ip-router show rib** command shows the route-manager's routing information base (RIB) and includes both IPv4 and IPv6 routing information. For any given network, the routing daemon could have multiple routes. The active route to any network is shown with a plus (+) sign next to it. The last active route is shown with a minus (-) next to it. If a route has been the last active route and is also the current active route, then it is shown with an asterisk (\*) sign next to it. The legend is as follows:

- “+” Active Route
- “-” Last Active
- “\*” Both

If the **detail** option is used, then additional information is displayed about these routes. The announcements bits for the active route are shown which shows the protocol into which this route is advertised.

## Parameters

---

|               |  |
|---------------|--|
| <b>detail</b> | Allows you to view additional information about the routes in the RIB. |
|---------------|--|

---

## Restrictions

None.

## Examples

A sample output of the **ip-router show rib** command is shown below:

```

box1# ip-router show rib
Routing Tables:
Destinations: 4    Routes: 4
Holddown: 0    Delete: 0    Hidden: 0
Codes: Network/Mask - Destination Network Address/Mask
      U - Unicast Status + = Best Route, - = Last Active, * = Both
      M - Multicast Status + = Best Route, - = Last Active, * = Both
      Src - Source of the route:
          Ag - Aggregate, B - BGP derived, C - Connected
          R - RIP derived, St - Static, NO - OSPF derived
          NOE - OSPF ASE derived, ON - OSPF NSSA derived, D - Default
      Next hop - Gateway for the route; Next hops in use: 4
      Netif - Next hop interface
      Prfl - Preference of the route
      Mtrc1 - Metric1 of the route, Mtrc2 - Metric2 of the route
      M - Metric1 and metric2 of the route
      Age - Age of the route since last refreshed

Network/Mask      U M Src Next hop      Netif      Prfl Mtrc1 Mtrc2      Age
-----
20.1.1/24         * * C 20.1.1.2      intf2       0       1       0 1:19:30
127/8             *   St 127.0.0.1      lo          0       0       0 1:20:09
127.0.0.1/32      * * C 127.0.0.1      lo          0       1       0 1:20:09
192.132.2/24      * * C 192.132.2.1    en          0       1       0 1:20:09

IPv6 Routing Table:
Destinations: 10    Routes: 10
Holddown: 0    Delete: 0    Hidden: 0

Src: C U: * ::1/128 Netif: lo1
Next hop: ::1 Prfl: 0 M: 1/0 Age: 1:20:09

Src: C U: * 2000::/64 Netif: intf1
Next hop: 2000:: Prfl: 0 M: 1/0 Age: 1:19:30

Src: C U: 2000::/64 Netif: intf1
Next hop: 2000::2 Prfl: 0 M: 1/0 Age: 1:19:30

Src: RNG U: * 2200::/64 Netif: intf1
Next hop: fe80::2e0:63ff:fe13:2003%intf1 Prfl: 100 M: 2/0 Age: 40

Src: C U: * 2300::/64 Netif: intf3
Next hop: 2300:: Prfl: 0 M: 1/0 Age: 1:19:29

Src: C U: 2300::/64 Netif: intf3
Next hop: 2300::1 Prfl: 0 M: 1/0 Age: 1:19:29

Src: C U: * 3000::1/128 Netif: tunnel1
Next hop: 3000::1 Prfl: 0 M: 1/0 Age: 1:14:23

Src: C U: * 3000::2/128 Netif: tunnel1
Next hop: 3000::1 Prfl: 0 M: 1/0 Age: 1:14:23

```

To see a specific route, use the **ip-router show route** command.

# ip-router show route

## Purpose

Display specific route information from RIB, for both IPv4 and IPv6.

## Format

**ip-router show route** [*<ip-addr-mask>* | **default**] [**detail**]

## Mode

Enable.

## Description

This command shows a specific route in the route-manager's routing information base (RIB). For any given network, the routing daemon could have multiple routes. The active route to any network is shown with a plus (+) sign next to it. The last active route is shown with a minus (-) next to it. If a route has been the last active route and is also the current active route, then it is shown with an asterisk (\*) sign next to it. The legend is as follows:

- “+” Active Route
- “-” Last Active
- “\*” Both

If the detail option is used, then additional information is displayed about this route. The announcements bits for the active route are shown which shows the protocol into which this route is advertised.

## Parameters

|  |   |
|--|---|
| <i>&lt;ipAddr/mask&gt;</i>  <br><b>default</b> | Allows you to specify a particular IP address mask for the RIB route in question, or refer to the default address mask. |
| <b>detail</b>                                  | Allows you to view additional information about the routes in the RIB.  |

## Restrictions

None.

## Example

A sample output of the **ip-router show route detail** command is shown below.

```
xp# ip-router show route 10.12.1.0/255.255.255.252 detail
10.12.1      mask 255.255.255.252
entries 2   announce 1
TSI:
RIP 150.1.255.255mc <> metric 1
RIP 222.1.1.255mc <> metric 1
BGP_Sync_64805 dest 10.12.1/2 metric 0
BGP group type Routing AS 64805 no metrics
Instability Histories:
*Direct Preference: 0
*NextHop: 10.12.1.2      Interface: 10.12.1.2(to-c4500)
State: <Int Active Retain>
Age: 5:12:10  Metric: 0  Metric2: 0  Tag: 0
Task: IF
Announcement bits(5):
2-KRT 4-RIP.0.0.0.0+520 5-RIP.0.0.0.0+520
6-BGP_Sync_64805
7-BGP_Group_64805
AS Path: IGP (Id 1)
OSPF Preference: -10
*NextHop: 10.12.1.1      Interface: 10.12.1.2(to-c4500)
State: <NotInstall NoAdvise Int Hidden Gateway>
Local AS: 64805
Age: 1:20:05  Metric: 1  Metric2: -1  Tag: 0
Task: OSPF
AS Path: (64805) IGP (Id 9551)
Cost: 1 Area: 0.0.0.0 Type: Net AdvRouter:
172.23.1.14
```

In this case there are two routes to network 10.12.1.0/255.255.255.252—one of them is a direct route and other route is learned through OSPF. The direct route has a better preference (lower preference is considered better preference), and is thus the active route. The direct route has been installed since 5 hours, 12 minutes and 10 seconds. This direct route is being announced to the Forwarding Information Base (FIB) which is indicated by KRT, over two RIP interfaces (which is indicated by 4-RIP.0.0.0.0+520, 5-RIP.0.0.0.0+520) and also to the BGP internal peer-group for autonomous system 64805.

To see all the routes in the RIB, use the **ip-router show rib** command.

## Field Definitions

| Field                 | Description  |
|-----------------------|--|
| TSI                   | Indicates that the X-Pedition has stored some internal bookkeeping for the protocols listed here.  |
| Instability Histories | The Flap histories associated with a particular route (i.e., how many times the route went up and down).   |
| [protocol]            | Indicates the route type (i.e., Direct OSPF, RIP, BGP, Static, or Aggregate).  |
| Preference            | The preference that the route has compared to other routes with the same destination.  |
| NextHop               | IP address of the next hop to use when routing a packet to this network.   |
| Interface             | The IP address and name where the NextHop is located.  |
| State                 | The internal state of the route. For example, "ActiveU" indicates that this is the Unicast route currently used in the FIB or Forwarding Information Base. "Gateway" denotes a route that is more than one hop away. |
| Age                   | The amount of time lapsed since the route was last refreshed.  |
| Metric                | The routing metric. For example, the cost of the link for OSPF; or the hop count for RIP.  |
| Metric2               | Alternate metric for routing decision.   |
| Tag                   | AS tag that is propagated through an OSPF.   |
| Task                  | Task that contributed the information displayed with this output (e.g., IF, OSPF, RIP, BGP).   |
| Announcement bits     | Listed by task, which and how many protocols provide access to the route.  |
| AS Path               | IGP/EGP info and BGP AS path if it exists.   |
| Local AS              | The Local Autonomous System (AS) on which this route resides.  |
| Cost                  | Link cost as calculated by OSPF.   |
| Area                  | The area from which this route originated.   |
| Type                  | The LSA type (e.g., 4,5,7).  |
| AdvRouter             | The router ID of the router that originated this LSA.  |



# ip-router show state

## Purpose

Displays the state of GateD, for both IPv4 and IPv6.

## Format

**ip-router show state** [**all**] [**memory**] [**timers**] [**to-file**] [**to-terminal**]  
[**task** <*string*> | **all** | **gii** | **icmp** | **inet** | **interface** | **krt** | **route**]

## Mode

Enable.

## Parameters

|                               |  |            |                                  |            |                        |             |                                      |             |                                      |                  |   |            |                                     |              |                                       |
|-------------------------------|--|------------|----------------------------------|------------|------------------------|-------------|--------------------------------------|-------------|--------------------------------------|------------------|---|------------|-------------------------------------|--------------|---------------------------------------|
| <b>all</b>                    | Shows all output.  |            |                                  |            |                        |             |                                      |             |                                      |                  |   |            |                                     |              |                                       |
| <b>memory</b>                 | Shows memory allocations.  |            |                                  |            |                        |             |                                      |             |                                      |                  |   |            |                                     |              |                                       |
| <b>timers</b>                 | Shows various GateD timers.  |            |                                  |            |                        |             |                                      |             |                                      |                  |   |            |                                     |              |                                       |
| <b>to-file</b>                | Saves the routing-process state in the gated.dmp file.   |            |                                  |            |                        |             |                                      |             |                                      |                  |   |            |                                     |              |                                       |
| <b>to-terminal</b>            | Displays the routing-process state on the console.   |            |                                  |            |                        |             |                                      |             |                                      |                  |   |            |                                     |              |                                       |
| <b>task</b> < <i>string</i> > | Shows task-specific information. The default is to show information for all tasks. You can specify a task using the following options: <table><tr><td><b>all</b></td><td>Shows information for all tasks.</td></tr><tr><td><b>gii</b></td><td>Shows GII information.</td></tr><tr><td><b>icmp</b></td><td>Shows information for the ICMP task.</td></tr><tr><td><b>inet</b></td><td>Shows information for the INET task.</td></tr><tr><td><b>interface</b></td><td>Shows information for the Interface task.</td></tr><tr><td><b>krt</b></td><td>Shows information for the KRT task.</td></tr><tr><td><b>route</b></td><td>Shows information for the route task.</td></tr></table> | <b>all</b> | Shows information for all tasks. | <b>gii</b> | Shows GII information. | <b>icmp</b> | Shows information for the ICMP task. | <b>inet</b> | Shows information for the INET task. | <b>interface</b> | Shows information for the Interface task. | <b>krt</b> | Shows information for the KRT task. | <b>route</b> | Shows information for the route task. |
| <b>all</b>                    | Shows information for all tasks.   |            |                                  |            |                        |             |                                      |             |                                      |                  |   |            |                                     |              |                                       |
| <b>gii</b>                    | Shows GII information.   |            |                                  |            |                        |             |                                      |             |                                      |                  |   |            |                                     |              |                                       |
| <b>icmp</b>                   | Shows information for the ICMP task.   |            |                                  |            |                        |             |                                      |             |                                      |                  |   |            |                                     |              |                                       |
| <b>inet</b>                   | Shows information for the INET task.   |            |                                  |            |                        |             |                                      |             |                                      |                  |   |            |                                     |              |                                       |
| <b>interface</b>              | Shows information for the Interface task.  |            |                                  |            |                        |             |                                      |             |                                      |                  |   |            |                                     |              |                                       |
| <b>krt</b>                    | Shows information for the KRT task.  |            |                                  |            |                        |             |                                      |             |                                      |                  |   |            |                                     |              |                                       |
| <b>route</b>                  | Shows information for the route task.  |            |                                  |            |                        |             |                                      |             |                                      |                  |   |            |                                     |              |                                       |

## Restrictions

None.



# Chapter 34

## ipv6-router Commands

The **ipv6-router** commands let you configure and monitor features and functions that work across the various IPv6 routing protocols.

### Command Summary

[Table 29](#) lists the **ipv6-router** commands. [Table 30 on page 557](#) lists the shared commands that affect both IPv4 and IPv6 routing but which are accessed through the **ip-router** facility.

The sections following the tables describe the **ipv6-router** command syntax.

**Table 29. ipv6-router Commands**

|  |
|--|
| <b>ipv6-router find route</b> <ipv6-addr> [ignore-state]   |
| <b>ipv6-router policy redistribute from-proto</b> <protocol> <b>to-proto</b> <protocol> [network <ipv6Addr/prefix>   default   all] [metric <number>   restrict] |
| <b>ipv6-router show route</b> [<IPv6addr-prefix>] [default] [detail]   |

[Table 30](#) lists the global router commands shared by both the IPv4 and IPv6 router functionality. They will continue to be accessed through the **ip-router** facility, although they will affect both IPv4 and IPv6 routing. Refer to [Chapter 33, ip-router Commands](#) for the **ip-router** facility commands.

**Table 30. Shared Global Router Commands**

|   |
|---|
| <b>ip-router set</b> {trace-options   trace-state   trace-level   max-bgjob-interval}   |
| <b>ip-router global set</b> {trace-options   trace-level   trace-state   max-bgjob-interval   autonomous-system   confederation-id   router-id} |
| <b>ip-router global use provided_config</b>   |

**Table 30. Shared Global Router Commands**

|  |
|--|
| <b>ip-router kernel trace</b>            |
| <b>ip-router show configuration file</b> |
| <b>ip-router show rib</b>                |
| <b>ip-router show state</b>              |

# ipv6-router find route

## Purpose

Find the active route in the IPv6 RIB which the packet will use.

## Format

**ipv6-router find route** *<ipv6-addr>* [**ignore-state**]

## Mode

Enable.

## Parameters

|                          |  |
|--------------------------|--|
| <i>&lt;ipv6-addr&gt;</i> | Specifies the destination of the packet.   |
| <b>ignore-state</b>      | This optional parameter allows inactive routes to be considered in route determination |

## Restrictions

None.

## Example

The following example displays the route to 23::1.

xp# **ipv6-router find route 23::1**

Routing Tables:

Codes: Network/Mask - Destination Network Address/Mask

Source of the route:

Ag - Aggregate, B - BGP derived, C - Connected

R - RIP derived, St - Static, NO - OSPF derived

OE - OSPF ASE derived, D - Default

S - Status + = Best Route, - = Last Active, \* = Both

Netif - Next hop interface

Next hop - Gateway for the route

Prf1 - Preference of the route

M - Metric1 and metric2 of the route

Age - Age of the route

RNG S:\* 23::/64 Netif:intf1

Next hop:fe80::2e0:63ff:fe13:2043428ntf1 Prf1:100 M:2/0 Age:2

# **ipv6-router policy redistribute**

## **Purpose**

Creates a simple route redistribution policy

## **Format**

**ipv6-router policy redistribute from-proto** *<protocol>* **to-proto** *<protocol>*  
**[network** *<ipv6Addr/prefix>* **| default | all] [metric** *<number>* **| restrict]**

## **Mode**

Configure.

## **Parameters**

|  |  |
|--|--|
| <b>from-proto</b><br><i>&lt;protocol&gt;</i>                             | Specifies the protocol of the source routes. The values for the <b>from-proto</b> parameter are <b>ripng</b> , <b>direct</b> or <b>static</b> .  |
| <b>to-proto</b> <i>&lt;protocol&gt;</i>                                  | Specifies the destination protocol where the routes are to be exported. The only valid value for the <b>to-proto</b> parameter is <b>ripng</b> .   |
| <b>network</b><br><i>&lt;ipv6Addr/prefix&gt;</i><br><b>default   all</b> | Specifies networks to be redistributed.<br><br>Matching usually requires both an address and a prefix, although the prefix can be implied. If no additional options qualifying the networks to be redistributed are specified, then any destination that falls in the range implied by this network-specification is matched, so the prefix of the destination is ignored.                               |
| <b>restrict</b>  | Specifies that routes matching the filter are not to be redistributed.   |
| <b>metric</b>  | Indicates the metric to be associated with the redistributed routes.<br><br><b>Note:</b> RIPng has a configurable parameter that specifies the default-metric associated with routes exported to that protocol. If a metric is not explicitly specified with the redistribute command, then it is inherited from the default-metric associated with the protocol to which the routes are being exported. |

## **Restrictions**

None.

# **ipv6-router show route**

## **Purpose**

Display specific route information from RIB.

## **Format**

**ipv6-router show route** [*<IPv6addr-prefix>*] **default** [**detail**]

## **Mode**

Enable.

## **Description**

This command shows a specific route in the route-manager's routing information base (RIB). For any given network, the routing daemon could have multiple routes. The active route to any network is shown with a plus (+) sign next to it. The last active route is shown with a minus (-) next to it. If a route has been the last active route and is also the current active route, then it is shown with an asterisk (\*) sign next to it. The legend is as follows:

- “+” Active Route
- “-” Last Active
- “\*” Both

If the detail option is used, then additional information is displayed about this route. The announcements bits for the active route are shown which shows the protocol into which this route is advertised.

## **Parameters**

|  |   |
|--|---|
| <i>&lt;ipAddr/prefix&gt;</i><br><b>default</b> | Allows you to specify a particular IPv6 address prefix for the RIB route in question, or refer to the default address prefix. |
| <b>detail</b>                                  | Allows you to view additional information about the routes in the RIB.  |

## **Restrictions**

None.



## Examples

The following example shows the output of the **ipv6-show route** command:

```
xp(ipv6-router-show)# route 23::1

Routing Tables:
Codes: Network/Mask - Destination Network Address/Mask
Src - Source of the route:
    Ag - Aggregate, B - BGP derived, C - Connected
    R - RIP derived, St - Static, NO - OSPF derived
    NOE - OSPF ASE derived, D - Default
U - Unicast Status + = Best Route, - = Last Active, * = Both
M - Multicast Status + = Best Route, - = Last Active, * = Both
Netif - Next hop interface
Next hop - Gateway for the route
Prf1 - Preference of the route
M - Metric1 and metric2 of the route
Age - Age of the route since last refreshed
```

```
Src: RNG U: * 23::/64 Netif: intf1
Next hop: fe80::2e0:63ff:fe13:2043%intf1 Prf1: 100 M: 2/0 Age: 4
```

A sample output of the **ipv6-router show route detail** command is shown below.

```
xp# ipv6-router show route 23::1 detail

23::          mask ffff:ffff:ffff:ffff::
(U*) RIPNG Preference: 100
*NextHop: fe80::2e0:63ff:fe13:2043%intf1 Interface: fe80::2e0:63ff:fe13:2003%intf1(intf1) !
State: <Int Gateway ActiveU Unicast >
Age: 6 Metric: 2 Metric2: 0 Tag: 0
AS Path: IGP (Id 2)
```

To see all the routes in the RIB, use the **ip-router show rib** command.

## Field Definitions

| Field      | Description   |
|------------|---|
| [protocol] | Indicates the route type (RIPng or Static).   |
| Preference | The preference that the route has compared to other routes with the same destination. |
| NextHop    | IP address of the next hop to use when routing a packet to this network.              |

| Field     | Description  |
|-----------|--|
| Interface | The IP address and name where the NextHop is located.  |
| State     | The internal state of the route. For example, "ActiveU" indicates that this is the Unicast route currently used in the FIB or Forwarding Information Base. "Gateway" denotes a route that is more than one hop away. |
| Age       | The amount of time lapsed since the route was last refreshed.  |
| Metric    | The routing metric. For example, the hop count for RIP.  |
| Metric2   | Alternate metric for routing decision.   |
| Tag       | AS tag that is propagated through an OSPF.   |
| AS Path   | IGP/EGP info.  |

# Chapter 35

## ipx Commands

The **ipx** commands let you add entries to the IPX SAP table for SAP servers and display the IPX forwarding database, RIP table, and SAP table.

### Command Summary

[Table 31](#) lists the **ipx** commands. The sections following the table describe the command syntax.

**Table 31. ipx Commands**

|  |
|--|
| <b>ipx add route</b> <networkaddr> <nexttroutnextnode> <metric> <ticks>  |
| <b>ipx add sap</b> <type> <SrvName> <node> <socket> <metric> <interface-network>                               |
| <b>ipx find rip</b> <address>  |
| <b>ipx find sap</b> <type> all <SrvName> all <network> all <entrytype>   |
| <b>ipx l3-hash module</b> <num> all variant <num>  |
| <b>ipx set interface ifname</b> <string>  <b>ipg</b> <num>   <b>ripintvl</b> <num>   <b>sapintvl</b> <num>     |
| <b>ipx set rip buffers</b> <buffer-size>  <b>packets-per-iteration</b> <num>                                   |
| <b>ipx set ripreq buffers</b> <buffer-size>  <b>packets-per-iteration</b> <num>                                |
| <b>ipx set sap buffers</b> <buffer-size>  <b>packets-per-iteration</b> <num>  <b>topn</b>   <b>delay</b> <num> |
| <b>ipx set sapgns buffers</b> <buffer-size>   <b>round-robin</b>   <b>packets-per-iteration</b> <num>          |
| <b>ipx set type20 propagation on</b>   |
| <b>ipx set port forwarding-mode destination-based</b>  |
| <b>ipx show buffers</b>  |

**Table 31. ipx Commands (Continued)**

|   |
|---|
| <b>ipx show hash-variant</b> <i>&lt;num&gt;</i>   <b>all</b>                      |
| <b>ipx show interfaces</b> <i>&lt;interface&gt;</i>   <b>all</b> [ <b>brief</b> ] |
| <b>ipx show rib destination</b>   |
| <b>ipx show servers hops</b>   <b>net</b>   <b>name</b>   <b>type</b>             |
| <b>ipx show summary</b>   |
| <b>ipx show routes</b>  |
| <b>ipx show packets-per-iteration</b>   |

# ipx add route

## Purpose

Add an IPX RIP route entry to the routing table.

## Format

**ipx add route** <networkaddr> <nextroutnextnode> <metric> <ticks>

## Mode

Configure.

## Description

The **ipx add route** command adds a route into the IPX RIP routing table.

## Parameters

|                    |   |
|--------------------|---|
| <networkaddr>      | Destination network address.  |
| <nextroutnextnode> | Next router's Network.Node address.                                     |
| <metric>           | The number of hops to this route. You can specify a number from 0 – 14. |
| <ticks>            | Ticks associated with this route.                                       |

## Restrictions

- Route entries that you add using the **ipx add route** command override dynamically learned entries, regardless of hop count.
- IPX is not supported in partially meshed WAN networks unless each node has a unique network address.

## Example

To add an IPX route to IPX network A1B2C3F5 via router A1B2C3D4.00:E0:63:11:11:11 with a metric of 1 and a tick of 100:

```
xp(config)# ipx add route A1B2C3F5 A1B2C3D4.00:E0:63:11:11:11 1 100
```

# ipx add sap

## Purpose

Add an IPX SAP entry to the routing table.

## Format

**ipx add sap** <type> <SvcName> <node> <socket> <metric> <interface-network>

## Mode

Configure.

## Description

The **ipx add sap** command adds an entry for an IPX server to the IPX SAP table.

## Parameters

|                     |  |
|---------------------|--|
| <type>              | The type of service. Specify the service type using its hexadecimal value.   |
| <SvcName>           | Name of the IPX server. You can use any characters in the name except the following: " * . / : ; < = > ? [ ] \   ]<br><br><b>Note:</b> Lowercase characters are changed to uppercase characters. |
| <node>              | The IPX network and node address. Specify the address in the following format: <netaddr>.<macaddr>. Example: a1b2c3d4.aa:bb:cc:dd:ee:ff.   |
| <socket>            | The socket number for this SAP entry. You can specify a Hexadecimal number from 0x0 – 0xFFFF.  |
| <metric>            | The number of hops to the server. You can specify a number from 1 – 14.  |
| <interface-network> | The interface network associated with this SAP entry.  |

## Restrictions

SAP entries that you add using the **ipx add sap** command override dynamically learned entries, regardless of hop count. Moreover, if a dynamic route entry that is associated with the static SAP entry ages out or is deleted, the X-Pedition router does not advertise the corresponding static SAP entries for the service until it relearns the route.

# ipx find rip

## Purpose

Find an IPX address in the routing table.

## Format

**ipx find rip** <address>

## Mode

Enable.

## Description

The **ipx find rip** command searches for an IPX address in the routing table.

## Parameters

|           |   |
|-----------|---|
| <address> | The IPX network address of this interface. Specify the IPX address using its hexadecimal value. |
|-----------|---|

## Restrictions

None.

## Example

To find an IPX network in the route table:

```
xp(config)# ipx find rip A1B2C3F5
```

# ipx find sap

## Purpose

Find a SAP entry in the routing table.

## Format

**ipx find sap** <type>|**all** <SrvcName>|**all** <network>|**all** <entrytype>

## Mode

Enable.

## Description

The **ipx find sap** command searches for a SAP entry in the routing table.

## Parameters

|                        |  |                                       |
|------------------------|--|---------------------------------------|
| <type>  <b>all</b>     | The types of service. Specify the service type using its hexadecimal value. Specify <b>all</b> for all types of service.   |                                       |
| <SrvcName>  <b>all</b> | Name of the IPX service. You can use any characters in the name except the following: " * . / : ; < = > ? [ ] \  |                                       |
|                        | <b>Note:</b> Lowercase characters are changed to uppercase characters. Specify <b>all</b> for all IPX services.  |                                       |
| <network>  <b>all</b>  | Network on which the service resides. Specify an IPX network address in the following format: <netaddr.> Example: a1b2c3d4. Specify <b>all</b> for all networks. |                                       |
| <entrytype>            | The types of entry you want to find. Specify one of the following:   |                                       |
|                        | <b>all</b>   | Finds static and dynamic SAP entries. |
|                        | <b>dynamic</b>   | Finds only the dynamic SAP entries.   |
|                        | <b>static</b>  | Finds only the static SAP entries.    |

## Restrictions

None.



## Example

To find a SAP entry in the route table:

```
xp(config)# ipx find sap 4 FILESERVER a2b2c3d4 dynamic
```

## ipx l3-hash

### Purpose

Changes the hashing algorithm used for the L3 IPX lookup table.

### Format

**ipx l3-hash module** <num>|**all** **variant** <num>

### Mode

Configure.

### Description

The X-Pedition L3 Lookup table is organized as a hash table. The hash function reduces the destination and source MAC addresses to 16-bit quantities each. The hashing algorithm generates a uniform distribution within the MAC address space. However, given a particular set of addresses, the distribution may cause addresses to clump together in the table. To minimize the risk of thrashing in the tables, three variations to the basic hashing algorithm are defined. Only one variation is in effect on a line card at any given time. You can use the ipx **l3-hash** command to set which variation is in effect for a line card.

Swizzling shifts the hash value by a certain amount of bits, producing more random distribution across the L3 lookup table.

Auto-hashing periodically queries the L2 or L3 tables for hash bucket overflow on a port. If there are more overflows than a certain threshold level, auto-hashing will automatically change the hash mode for that port. Eventually a ‘best’ hash mode for the particular traffic will be found, which will provide a more even distribution across the L2 or L3 lookup table.

**Note:** This command is subject to merging. If you enter one command for a module setting the variant to 8 (enabling autohashing) and then enter another command for the same module setting it to another variant, the commands will merge. The second command will become activated and overwrite the first one, in this case disabling autohashing on the module.

**Note:** Setting a variant on an ER-16 module will set it on both channels on that module.

### Parameters

---

|                                 |  |
|---------------------------------|--|
| <b>module</b> <num>  <b>all</b> | Is a slot number on the X-Pedition router. Specify any number between 1 and 16. The hashing algorithm change affects all ports on the line card in the slot. The <b>all</b> option causes the hashing algorithm to change on all ports on all slots. |
|---------------------------------|--|

---

|                      |  |
|----------------------|--|
| <b>variant</b> <num> | Causes a variation to the basic hashing algorithm to be made. Valid variant numbers are: 0-3, and 4-7 (swizzled). If you specify 0, the default hashing algorithm is used. |
|----------------------|--|

## Restrictions

None.

## Example

To change the default hashing algorithm used for the L3 lookup table on all ports on slot 7:

```
xp(config)# ipx l3-hash module 7 variant 1
```

# ipx set interface

## Purpose

Sets the IPX interface parameters.

## Format

**ipx set interface ifname** <string> | **ipg** <num> | **ripintvl** <num> | **sapintvl** <num>

## Mode

Configure.

## Description

The **ipx set interface** command sets the IPX interface parameters such as interface name, inter-packet gap, broadcast interval for RIP, and broadcast interval for SAP.

## Parameters

|                        |  |
|------------------------|--|
| <b>ifname</b> <string> | Specify the interface name.<br><br><b>Note:</b> Enterasys recommends that you use alphabetic characters when defining interface names—purely numeric interfaces will be interpreted as IP addresses. The X-Pedition router will display interface names up to 32 characters in length. |
| <b>ipg</b> <num>       | Specify the Inter Packet Gap (in milliseconds). Specify any number between 30 and 180.   |
| <b>ripintvl</b> <num>  | Specify the broadcast interval for RIP (in seconds). Specify any number between 60 and 300.  |
| <b>sapintvl</b> <num>  | Specify the broadcast interval for SAP (in seconds). Specify any number between 60 and 300.  |

## Restrictions

None.

## ipx set rip

### Purpose

Sets the RIP socket buffer size in bytes or the number of packets per iteration.

### Format

**ipx set rip buffers** *<buffer-size>* | **packets-per-iteration** *<num>*

### Mode

Configure.

### Description

The **ipx set rip buffers** command sets the RIP socket buffer size or the number of rip packets processed per iteration.

### Parameters

|   |  |
|---|--|
| <b>buffers</b><br><i>&lt;buffer-size&gt;</i>    | Specify the socket buffer size in bytes.                         |
| <b>packets-per-iteration</b> <i>&lt;num&gt;</i> | Specify the number of rip packets to be processed per iteration. |

### Restrictions

None.

## ipx set ripreq

### Purpose

Sets the buffer size or number of packets per iteration for rip requests.

### Format

**ipx set ripreq buffers** *<buffer-size>* | **packets-per-iteration** *<num>*

### Mode

Configure.

### Description

The **ipx set ripreq** command sets the rip buffer size or the number of packets per iteration.

### Parameters

|   |  |
|---|--|
| <b>buffers</b><br><i>&lt;buffer-size&gt;</i>    | Size of the buffer in bytes.                               |
| <b>packets-per-iteration</b> <i>&lt;num&gt;</i> | The number of rip request packets processed per iteration. |

### Restrictions

None.

# ipx set sap

## Purpose

Sets various SAP socket parameters.

## Format

**ipx set sap buffers** <buffer-size> | **packets-per-iteration** <num> | **topn** | **delay** <num>

## Mode

Configure.

## Description

The **ipx set sap** command sets various SAP socket parameters.

## Parameters

|                                    |   |
|------------------------------------|---|
| <b>buffers</b><br><buffer-size>    | Specify the buffer size in bytes.                     |
| <b>packets-per-iteration</b> <num> | The number of SAP packets processed per iteration.    |
| <b>topn</b>                        | Send only the nearest N services for a general reply. |
| <b>delay</b> <num>                 | Delay multiple to be used for general SAP requests.   |

## Restrictions

None.

## ipx set sapgns

### Purpose

Sets parameters for sap get nearest server packets.

### Format

**ipx set sapgns buffers** *<buffer-size>* | **round-robin** | **packets-per-iteration** *<num>*

### Mode

Configure.

### Description

The **ipx set sapgns** command sets the following parameters for get nearest server packets:

- sets buffer size
- sets a round-robin scheme for finding servers

### Parameters

|   |   |
|---|---|
| <b>buffers</b><br><i>&lt;buffer-size&gt;</i>    | Specify the buffer size in bytes.                                     |
| <b>round-robin</b>                              | Sets a round-robin scheme for finding the nearest server.             |
| <b>packets-per-iteration</b> <i>&lt;num&gt;</i> | The number of SAP Get Nearest Server packets processed per iteration. |

### Restrictions

None.



# **ipx set type20 propagation**

## **Purpose**

Controls the propagation of type 20 packets.

## **Format**

**ipx set type20 propagation on**

## **Mode**

Configure.

## **Description**

The **ipx set type20 propagation** command controls the propagation of type 20 packets.

## **Parameters**

None.

## **Restrictions**

None.

## **ipx set port**

### **Purpose**

Configures an IPX port for forwarding mode.

### **Format**

**ipx set port forwarding-mode destination-based**

### **Mode**

Configure.

### **Description**

The **ipx set port forwarding-mode destination-based** command sets up an IPX port to forward traffic based on the packet destination network, node, and socket.

### **Parameters**

None.

### **Restrictions**

None.

# **ipx show buffers**

## **Purpose**

Display the RIP and SAP socket buffer sizes.

## **Format**

**ipx show buffers**

## **Mode**

Enable.

## **Description**

The **ipx show buffers** command displays the RIP and SAP socket buffer sizes.

## **Parameters**

None.

## **Restrictions**

None.

# ipx show hash-variant

## Purpose

Display IPX hash variant per module.

## Format

**ipx show hash-variant** <num>|all

## Mode

Enable.

## Description

The **ipx show hash-variant** command displays hash variant information. There are a total of 16 modules using the hash variant feature (1-16).

Enabling hash variant causes a variation to the basic hashing algorithm. This variation will prevent clustering of hash values and will provide a more even distribution across the L3 lookup table. Valid variant numbers are: 0-3, 4-7 (swizzled), and 8 (auto-hashed). The default hashing algorithm is 0.

Swizzling shifts the hash value by a certain amount of bits, causing a more random distribution across the L3 lookup table. Auto-hashing allows the X-Pedition router to auto-select a hashing algorithm optimized for ‘best case’ L3 table distribution.

## Parameters

|       |  |
|-------|--|
| <num> | Specifies the module. Specify any number between 1-16. |
| all   | Displays hash variant information for all modules.     |

## Restrictions

None.

## Example

To display IPX hash variant information on all 16 modules:

```
xp# ipx show hash-variant all
IPX Module      Hash Variant
-----
Module 2        variant-3
Module 3        variant-0
Module 4        variant-0
Module 5        variant-0
Module 6        variant-5
Module 7        variant-0
Module 8        variant-0
Module 9        variant-0
Module 10       variant-0
Module 11       variant-2
Module 12       variant-2
Module 13       variant-0
Module 14       variant-0
Module 15       variant-1
```

# ipx show interfaces

## Purpose

Display the configuration of IPX interfaces.

## Format

**ipx show interfaces** <interface>|all [brief]

## Mode

Enable.

## Description

The **ipx show interfaces** command displays the configuration of an IPX interface. If you issue the command without specifying an interface name then the configuration of all IPX interfaces is displayed.

## Parameters

|                 |  |
|-----------------|--|
| <interface> all | Name of the IPX interface (for example, xp14) or all interfaces.   |
| <b>Note:</b>    | Enterasys recommends that you use alphabetic characters when defining interface names—purely numeric interfaces will be interpreted as IP addresses. The X-Pedition router will display interface names up to 32 characters in length. |
| <b>brief</b>    | Shows a brief summary of the interface in tabular form.  |

## Restrictions

If you specify an interface name, the name must belong to an existing IPX interface.

## Example

To display the configuration of all IPX interfaces:

```
xp# ipx show interfaces all
xp12: flags=9863<UP,BROADCAST,NOTRAILERS,RUNNING,SIMPLEX,LINK0,MULTICAST>
      VLAN: _VLAN-1
      Ports: et.1.7
      IPX: A1B2C3D4.00:E0:63:11:11:11
xp14: flags=9863<UP,BROADCAST,NOTRAILERS,RUNNING,SIMPLEX,LINK0,MULTICAST>
      VLAN: _VLAN-2
      Ports: et.1.2
      IPX: ABCD1234.00:E0:63:11:11:11
```

## **ipx show rib destination**

### **Purpose**

Show IPX RIP table output sorted by destination.

### **Format**

**ipx show rib destination**

### **Mode**

User.

### **Description**

The **ipx show rib destination** command displays IPX RIP table output sorted by destination.

### **Parameters**

None.

### **Restrictions**

None.



# ipx show servers

## Purpose

Show IPX server information.

## Format

**ipx show servers hops | net | name | type**

## Mode

User

## Description

The **ipx show servers** command displays IPX server information sorted by any or all of the optional arguments. Sorting is done based on the order of optional arguments given.

## Parameters

|             |  |
|-------------|--|
| <b>hops</b> | Shows the number of hops that the service is away.       |
| <b>name</b> | Shows the Sap service name.                              |
| <b>net</b>  | Shows the interface type over which the service arrived. |
| <b>type</b> | Shows the Sap service type.                              |

## Restrictions

None.

## **ipx show summary**

### **Purpose**

Displays summary of the IPX RIP/SAP tables.

### **Format**

**ipx show summary**

### **Mode**

User.

### **Description**

The **ipx show summary** command displays a summary of the IPX RIP/SAP tables.

### **Parameters**

None.

### **Restrictions**

None.

# **ipx show routes**

## **Purpose**

Displays information for IPX routes.

## **Format**

**ipx show routes**

## **Mode**

User.

## **Description**

The **ipx show routes** command displays information for all IPX routes.

## **Parameters**

None.

## **Restrictions**

None.

## **ipx show packets-per-iteration**

### **Purpose**

Display the number of IPX control packets processed per iteration.

### **Format**

**ipx show packets-per-iteration**

### **Mode**

User.

### **Description**

The **ipx show packets-per-user** command displays the number of IPX control packets processed per iteration for rip, rip request, SAP, and SAP GNS.

### **Parameters**

None.

### **Restrictions**

None.

# Chapter 36

## I2-tables Commands

The **I2-tables** commands let you display various L2 tables related to MAC addresses.

### Command Summary

[Table 32](#) lists the **I2-tables** commands. The sections following the table describe the command syntax.

**Table 32. I2-tables Commands**

|  |
|--|
| <b>I2-tables show all-flows</b> [vlan <VLAN-num> [source-mac <MACaddr>]] [undecoded]   |
| <b>I2-tables show all-macs</b> [verbose [undecoded]]<br>[vlan <VLAN-num>] [source] [destination] [multicast]   |
| <b>I2-tables show bridge-management</b>  |
| <b>I2-tables show igmp-mcast-registrations</b> [vlan <VLAN-num>]   |
| <b>I2-tables show mac</b> <MACaddr> vlan <VLAN-num>  |
| <b>I2-tables show mac-table-stats</b>  |
| <b>I2-tables show port-macs</b> port <port-list> all-ports [[vlan <VLAN-num>] [source]<br>[destination] [multicast] [undecoded] [no-stats] [verbose] [decode-smarttrunks]] |
| <b>I2-tables show vlan-igmp-status</b> vlan <VLAN-num>   |
| <b>I2-tables show system-macs</b>  |

## **l2-tables show all-flows**

### **Purpose**

Show all L2 flows (for ports in flow-bridging mode).

### **Format**

**l2-tables show all-flows** [**vlan** <VLAN-num> [**source-mac** <MACaddr>]] [**undecoded**]

### **Mode**

User or Enable.

### **Description**

The **l2-tables show all-flows** command shows all the L2 flows learned by the X-Pedition router. The X-Pedition router learns flows on ports that are operating in flow-bridging mode.

### **Parameters**

---

|                        |  |
|------------------------|--|
| <b>vlan</b> <VLAN-num> | <p>The VLAN number (1-4095) associated with the flows. There are two special VLANs on the X-Pedition router: Default VLAN (ID=1) and VLAN with ID=4095 (i.e., the “Blackhole VLAN”).</p> <p>The Default VLAN contains all ports not in use by other VLANs. When you add ports to or remove them from a VLAN (with an ID other than 1), the router removes the ports from or adds them to the Default VLAN. The VLAN with the ID of 4095 serves as a repository for incoming frames with no destination. The following restrictions apply to these VLANs:</p> <ul style="list-style-type: none"><li>• You may not add ports explicitly to either of these VLANs.</li><li>• You cannot associate Layer 3 interfaces with the “Blackhole VLAN” (ID = 4095).</li><li>• You cannot associate IPX interfaces with the “Default VLAN” (ID = 1).</li><li>• In order to pass all IBM protocol types, you must configure a unique VLAN for both the SNA and the Bridged protocols. Additional information can be found online.</li></ul> |
|------------------------|--|

---

|                                |  |
|--------------------------------|--|
| <b>source-mac</b><br><MACaddr> | The source MAC address of the flows. Specify the MAC address in either of the following formats:<br><br>xx:xx:xx:xx:xx:xx<br>xxxxxx:xxxxxx   |
| <b>undecoded</b>               | Prevents the X-Pedition router from displaying the vendor names with the MAC addresses. Instead, the OUI of each MAC address is displayed “as is,” in hexadecimal format. If you do not use this option, the X-Pedition router decodes the OUI and displays the vendor name. |

## Restrictions

None.

# **l2-tables show all-macs**

## **Purpose**

Show all MAC addresses currently in the L2 tables.

## **Format**

**l2-tables show all-macs** [**verbose** [**undecoded**]] [**vlan** <*VLAN-num*>] [**source**] [**destination**] [**multicast**]

## **Mode**

User or Enable.

## **Description**

The **l2-tables show all-macs** command shows how many MAC addresses the X-Pedition router has in its L2 tables. You can format the displayed information based on VLAN, source MAC address, destination MAC address or multicast. If you enter the verbose option, the command also shows the individual MAC addresses.

## **Parameters**

|                                 |   |
|---------------------------------|---|
| <b>vlan</b> < <i>VLAN-num</i> > | Displays only MAC addresses in the specified VLAN.  |
| <b>source</b>                   | Displays only source addresses.   |
| <b>destination</b>              | Displays only destination addresses.  |
| <b>multicast</b>                | Displays only multicast and broadcast addresses.  |
| <b>verbose</b>                  | Shows detailed information for each MAC address entry.  |
| <b>undecoded</b>                | Prevents the X-Pedition router from displaying the vendor names with the MAC addresses. Instead, the OUI of each MAC address is displayed “as is,” in hexadecimal format. If you do not use this option, the router decodes the OUI and displays the vendor name. |

## **Restrictions**

None.



## **l2-tables show bridge-management**

### **Purpose**

Show information about all MAC addresses registered by the system.

### **Format**

**l2-tables show bridge-management**

### **Mode**

User or Enable.

### **Description**

The **l2-tables show bridge-management** command shows MAC addresses that have been inserted into the L2 tables for management purposes. Generally, these entries are configured so that a port forwards a frame to the Control Module if the management MAC matches the frame's destination MAC.

An example of a bridge-management MAC is Spanning Tree's bridge group address (0180C2:000000), which is registered in the L2 tables of X-Pedition ports on which the Spanning Tree Protocol (STP) is enabled.

### **Parameters**

None.

### **Restrictions**

None.

## **l2-tables show igmp-mcast-registrations**

### **Purpose**

Show information about multicast MAC addresses registered by IGMP.

### **Format**

**l2-tables show igmp-mcast-registrations** [**vlan** <VLAN-num>]

### **Mode**

User or Enable.

### **Description**

The **l2-tables show igmp-mcast-registrations** command shows the multicast MAC addresses that IGMP has registered with the L2 tables. The X-Pedition router forwards the multicast MAC addresses only to the ports that IGMP specifies.

### **Parameters**

---

|                        |  |
|------------------------|--|
| <b>vlan</b> <VLAN-num> | Displays only the multicast MAC addresses registered for the specified VLAN. |
|------------------------|--|

---

### **Restrictions**

None.

# l2-tables show mac

## Purpose

Show information about a particular MAC address.

## Format

**l2-tables show mac** <MACaddr> **vlan** <VLAN-num>

## Mode

User or Enable.

## Description

The **l2-tables show mac** command shows the port number on which the specified MAC address resides.

## Parameters

|                        |   |
|------------------------|---|
| <MACaddr>              | Is a MAC address. You can specify the address in either of the following formats:<br><br>xx:xx:xx:xx:xx:xx<br>xxxxxx:xxxxxx |
| <b>vlan</b> <VLAN-num> | Displays the MAC address for this VLAN.   |

## Restrictions

None.

## **l2-tables show mac-table-stats**

### **Purpose**

Show statistics for the MAC addresses in the MAC address tables.

### **Format**

**l2-tables show mac-table-stats**

### **Mode**

User or Enable.

### **Description**

The **l2-tables show mac-table-stats** command shows statistics for the master MAC address table in the Control Module and the MAC address tables on the individual ports.

### **Parameters**

None.

### **Restrictions**

None.

# l2-tables show port-macs

## Purpose

Show information about MACs residing in a port's L2 table.

## Format

**l2-tables show port-macs port** <port-list>|**all-ports**  
 [[**vlan** <VLAN-num>] [**source**] [**destination**] [**multicast**] [**undecoded**] [**no-stats**] [**verbose**]  
 [**decode-smarttrunks**]]

## Mode

User or Enable.

## Description

The **l2-tables show port-macs** command shows the information about the learned MAC addresses in individual L2 MAC address tables. Each port has its own MAC address table. The information includes the number of source MAC addresses and the number of destination MAC addresses in the table. If you enter the **verbose** option, the MAC addresses also are displayed.

## Parameters

|   |  |
|---|--|
| <b>port</b> <port-list>  <br><b>all-ports</b> | Specifies the port(s) for which you want to display MAC address information. You can specify a single port or a comma-separated list of ports. If you use the <b>all-ports</b> keyword, MAC address information is displayed for all ports.                        |
| <b>vlan</b> <VLAN-num>                        | Specifies the type of MAC address for which you want to show statistics.   |
| <b>source</b>                                 | Displays statistics for only source addresses.   |
| <b>destination</b>                            | Displays statistics for only destination addresses.  |
| <b>multicast</b>                              | Displays statistics for only multicast and broadcast addresses.  |
| <b>undecoded</b>                              | Displays the MAC addresses in hexadecimal format rather than undecoded format. Undecoded format does not show the vendor name in place of the first three hexadecimal digits (example: Enterasys:33:44:55). The default is undecoded (example: 00:11:22:33:44:55). |
| <b>no-stats</b>                               | Lists the MAC addresses without displaying any statistics.   |
| <b>verbose</b>                                | Shows detailed statistics for each MAC address entry.  |
| <b>decode-smarttrunks</b>                     | Shows l2 table information for SmartTRUNK ports.   |

## Restrictions

None.

## Example

```
xp(l2-tables-show)# port-macs port et.1.2 decode-smarttrunks
```

L2 table information for port et.1.2

-----

Number of source MAC addresses: 0

Number of destination MAC addresses: 0

Number of management-configured MAC addresses: 3

Port table capacity: 5888

Port table demand deletion upper & lower thresholds: 95% - 85%

Number of times table usage has reached upper threshold: 0

Number of times buckets have become full: 0

Number of duplicate learning frames: 0

Number of times LG port got out-of-sync: 0

Number of requests to learn a frame on an invalid VLAN: 0

Number of frames received from this switch (possible loop): 0

Aging is enabled

Addresses will be aged-out after 300 seconds

## l2-tables show vlan-igmp-status

### Purpose

Show whether IGMP is on or off on a VLAN.

### Format

**l2-tables show vlan-igmp-status vlan** <VLAN-num>

### Mode

Enable.

### Description

The **l2-tables show vlan-igmp-status** command shows the multicast MAC addresses that IGMP has registered with the L2 tables. This command also shows the ports to which the multicast MAC addresses are forwarded.

**Note:** For IGMP forwarding to occur for a multicast MAC address, IGMP must be enabled on the VLAN with which the MAC address is associated.

### Parameters

---

|                        |  |
|------------------------|--|
| <b>vlan</b> <VLAN-num> | <p>VLAN number (1-4095) associated with the flows. There are two special VLANs on the X-Pedition router—the Default VLAN (ID=1) and the VLAN with ID=4095 (i.e., the “Blackhole VLAN”).</p> <p>The Default VLAN contains all ports not in use by other VLANs. When adding or removing ports from a VLAN (with an ID other than 1), the router removes or adds them to the Default VLAN. The VLAN with the ID of 4095 serves as a repository for incoming frames with no destination. The following restrictions apply to these VLANs:</p> <ul style="list-style-type: none"><li>• You may not add ports explicitly to either of these VLANs.</li><li>• You cannot associate Layer 3 interfaces with the “Blackhole VLAN” (ID = 4095).</li><li>• You cannot associate IPX interfaces with the “Default VLAN” (ID = 1).</li></ul> <p>In order to pass all IBM protocol types, you must configure a unique VLAN for both the SNA and the Bridged protocols. Additional information can be found online.</p> |
|------------------------|--|

---

## **Restrictions**

None.



# l2-tables show system-macs

## Purpose

To display information about specific MACs registered by the system.

## Format

**l2-tables show system-macs**

## Mode

Enable.

## Description

The **l2-tables show system-macs** command displays information about MACs auto-registered by the system (e.g., VRRP MAC addresses).

## Parameters

None.

## Restrictions

None.

## Example

```
xp(l2-tables-show)# system-macs

Name:          VRRP Virtual-MAC
-----
Direction:     Source
Restriction:    force-to-go
VLAN:          30
Source MAC:     00005E:000102
In-List ports:  et.1.(1-2)
```



# Chapter 37

## load-balance Commands

The **load-balance** commands allow you to distribute session load across a pool of servers. These commands provide a way to load balance network traffic to multiple servers.

### Command Summary

[Table 33](#) lists the **load-balance** commands. The sections following the table describe the command syntax.

**Table 33. load-balance Commands**

|  |
|--|
| <b>load-balance add host-to-group</b> <ipaddr/range> <b>group-name</b> <group name><br><b>port</b> <port number> [ <b>weight</b> <weight>]   |
| <b>load-balance add host-to-vip-range</b> <range> <b>vip-range-name</b> <range name><br><b>port</b> <port number> [ <b>weight</b> <weight>]  |
| <b>load-balance allow access-to-servers client-ip</b> <ipaddr/range> <b>group-name</b> <group name>  |
| <b>load-balance create group-name</b> <group name> <b>virtual-ip</b> <ipaddr><br><b>virtual-port</b> <port number> <b>protocol</b> tcp udp [ <b>persistence-level</b> vpn tcp ssl sticky]  |
| <b>load-balance create vip-range-name</b> <range name> <b>vip-range</b> <range><br><b>virtual-port</b> <port number> <b>protocol</b> tcp udp [ <b>persistence-level</b> vpn tcp ssl sticky]  |
| <b>load-balance set aging-for-src-maps</b> <string> <b>aging-time</b> <num>  |
| <b>load-balance set client-proxy-subnet</b> <group name> <b>subnet</b> <num>   |
| <b>load-balance set ftp-control-port</b> <port number>   |
| <b>load-balance set group-options</b> <string> [ <b>ping-int</b> <num>] [ <b>ping-tries</b> <num>]<br>[ <b>app-int</b> <num>] [ <b>app-tries</b> <num>] [ <b>acv-command</b> <string> <b>acv-reply</b> <string>]<br>[ <b>acv-quit</b> <string>] [ <b>read-till-index</b> <num>] [ <b>check-port</b> <port number>] |

**Table 33. load-balance Commands (Continued)**

|   |
|---|
| <b>load-balance set group-conn-thresh</b> <i>&lt;string&gt;</i> <b>limit</b> <i>&lt;num&gt;</i>   |
| <b>load-balance set hash-variant</b> <i>&lt;value&gt;</i>   |
| <b>load-balance set policy-for-group</b> <i>&lt;group name&gt;</i> <b>policy</b> <i>&lt;policy&gt;</i>  |
| <b>load-balance set server-status server-ip</b> <i>&lt;ipaddr/range&gt;</i> <b>server-port</b> <i>&lt;port number&gt;</i><br><b>group-name</b> <i>&lt;group name&gt;</i> <b>status</b> up down  |
| <b>load-balance set server-options</b> <i>&lt;ipaddr&gt;</i> [ <b>port</b> <i>&lt;num&gt;</i> ] [ <b>ping-int</b> <i>&lt;num&gt;</i> ]<br>[ <b>ping-tries</b> <i>&lt;num&gt;</i> ] [ <b>app-int</b> <i>&lt;num&gt;</i> ] [ <b>app-tries</b> <i>&lt;num&gt;</i> ] [ <b>acv-command</b> <i>&lt;string&gt;</i> ]<br><b>acv-reply</b> <i>&lt;string&gt;</i> ] [ <b>acv-quit</b> <i>&lt;string&gt;</i> ] [ <b>read-till-index</b> <i>&lt;num&gt;</i> ]<br>[ <b>check-port</b> <i>&lt;port number&gt;</i> ] |
| <b>load-balance set vpn-dest-port</b> <i>&lt;num&gt;</i>  |
| <b>load-balance show acv-options</b> [ <b>group-name</b> <i>&lt;string&gt;</i> ] [ <b>destination-host-ip</b> <i>&lt;ipaddr&gt;</i> ]<br>[ <b>destination-host-port</b> <i>&lt;num&gt;</i> ]  |
| <b>load-balance show hash-stats</b>   |
| <b>load-balance show source-mappings client-ip</b> <i>&lt;ipaddr&gt;</i> <b>virtual-ip</b> <i>&lt;ipaddr&gt;</i><br><b>virtual-port</b> <i>&lt;port number&gt;</i> <b>destination-host-ip</b> <i>&lt;ipaddr&gt;</i>   |
| <b>load-balance show statistics group-name</b> <i>&lt;group name&gt;</i> <b>virtual-ip</b> <i>&lt;ipaddr&gt;</i><br><b>virtual-port</b> <i>&lt;port number&gt;</i>  |
| <b>load-balance show virtual-hosts group-name</b> <i>&lt;group name&gt;</i> <b>virtual-ip</b> <i>&lt;ipaddr&gt;</i><br><b>virtual-port</b> <i>&lt;port number&gt;</i>   |

# load-balance add host-to-group

## Purpose

Adds a server to a previously-created group of load balancing servers.

## Format

**load-balance add host-to-group** <ipaddr/range> **group-name** <group name>  
**port** <port number> [**weight** <weight>]

## Mode

Configure.

## Description

The **load-balance add host-to-group** command lets you add a server to a server group that was previously-created with the **load-balance create group-name** command.

## Parameters

|  |  |
|--|--|
| <b>host-to-group</b><br><ipaddr/range> | The IP address of the server being added to the group, in the form a.b.c.d or a range of IP addresses in the form 10.10.1.1-10.10.1.3.<br><br><b>Note:</b> Do not use an IP address for load-balancing that is already configured for VRRP.  |
| <b>group-name</b><br><group name>      | The name of the group of load balancing servers.   |
| <b>port</b> <port number>              | The port number to be used for load balancing communications for the server being added. Specify a number between 1 and 65535.   |
| <b>weight</b> <weight>                 | This parameter is only valid if you specify the weighted round robin policy for this group of load balancing servers. (The <b>load-balance set policy-for-group</b> command specifies the policy for distributing workload to the servers.) The weight determines how many sessions are assigned to this server during its turn in the weighted round robin selection. Specify a number between 1 and 65535. The default value is 1. |

## Restrictions

Do not use an IP address for load-balancing that is already configured for VRRP.

## Examples

To add a server 10.10.13.2 to the server group 'service2':

```
xp(config)# load-balance add host-to-group 10.10.13.2 group-name service2 port 80
```

To add servers 10.10.13.3, 10.10.13.4, and 10.10.13.5 to the server group 'service2':

```
xp(config)# load-balance add host-to-group 10.10.13.3-10.10.13.5 group-name service2 port 80
```

The following is an example of specifying the weighted round robin policy for distributing the workload on the server group 'service2.' To add servers 10.10.13.3, 10.10.13.4, and 10.10.13.5 to the server group 'service2,' a weight must be assigned to each server in the group:

```
xp(config)# load-balance set policy-for-group service2 policy weighted-round-robin  
xp(config)# load-balance add host-to-group 10.10.13.3 group-name service2 port 80 weight 10  
xp(config)# load-balance add host-to-group 10.10.13.4 group-name service2 port 80 weight 100  
xp(config)# load-balance add host-to-group 10.10.13.5 group-name service2 port 80 weight 1000
```

# load-balance add host-to-vip-range

## Purpose

Adds a range of servers to a range of virtual IP addresses that were created with the **load-balance create vip-range-name** command.

## Format

```
load-balance add host-to-vip-range <range> vip-range-name <range name>  
port <port number> [weight <weight>]
```

## Mode

Configure.

## Description

The **load-balance add host-to-vip-range** command lets you add a range of servers to a range of virtual IP addresses that were previously created with the **load-balance create vip-range-name** command. This command adds the first server address in the range to the first virtual IP address, the second server address to the second virtual IP address, and so on. Therefore, the number of servers in the specified range must *equal* the number of virtual IP addresses; if you specified 15 virtual IP addresses with the **load-balance create vip-range-name** command, then you must specify a range of 15 IP addresses in the **load-balance add host-to-vip-range** command.

## Parameters

|                                       |   |
|---------------------------------------|---|
| <b>host-to-vip-range</b><br><range>   | The IP range of the servers being added to the range, in the form 10.10.1.1-10.10.1.3. The number of servers in the range must be the same as the number of virtual IP addresses that were previously-created.<br><br><b>Note:</b> Do not use an IP address for load-balancing that is already configured for VRRP. |
| <b>vip-range-name</b><br><range name> | The name of the range of load balancing servers.<br><br><b>Note:</b> Do not use an IP address for load-balancing that is already configured for VRRP.   |
| <b>port</b> <port number>             | The port number to be used for load balancing communications for the server being added. Specify a number between 1 and 65535.  |

---

|                        |  |
|------------------------|--|
| <b>weight</b> <weight> | This parameter is only valid if you specify the weighted round robin policy for this group of load balancing servers. (The <b>load-balance set policy-for-group</b> command specifies the policy for distributing workload to the servers.) The weight determines how many sessions are assigned to this server during its turn in the weighted round robin selection. Specify a number between 1 and 65535. The default value is 1. |
|------------------------|--|

---

## Restrictions

None.

## Examples

The following command creates the server groups 'service1' through 'service15' with virtual IP addresses 207.135.89.1 through 207.135.89.15:

```
xp(config)# load-balance create vip-range-name service vip-range 207.135.89.1-207.135.89.15
virtual-port 80 protocol tcp
```

To add servers 10.10.13.1-10.10.13.15 to the server groups 'service1' through 'service15':

```
xp(config)# load-balance add host-to-vip-range 10.10.13.1-10.10.13.15 vip-range-name service port
80
```



# load-balance allow access-to-servers

## Purpose

Allows specified hosts to access the load balancing servers without address translation.

## Format

**load-balance allow access-to-servers client-ip** <ipaddr/range> **group-name** <group name>

## Mode

Configure.

## Description

Load balancing causes both source and destination addresses to be translated on the X-Pedition router. It may be undesirable in some cases for a source address to be translated; for example, when data is to be updated on each individual server. The **load-balance allow access-to-servers** command lets you specify the hosts which are allowed to access a group of load balancing servers without address translation.

Note that a host that is allowed to access a group of load balancing servers without address translation *cannot* use the virtual IP address and port to access servers in the group.

## Parameters

|                                    |  |
|------------------------------------|--|
| <b>client-ip</b><br><ipaddr/range> | The IP address of the host that is to be granted direct access, in the form a.b.c.d or a range of IP addresses in the form 10.10.1.1-10.10.1.3.<br><br><b>Note:</b> Do not use an IP address for load-balancing that is already configured for VRRP. |
| <b>group-name</b><br><group name>  | The name of the group of load balancing servers.   |

## Restrictions

None.

## Example

To allow the host 10.23.4.8 to directly access the server group 'service2':

```
xp(config)# load-balance allow access-to-servers client-ip 10.23.4.8 group-name service2
```

# load-balance create group-name

## Purpose

Creates a server group for load balancing.

## Format

```
load-balance create group-name <group name> virtual-ip <ipaddr>  
virtual-port <port number> protocol tcp|udp [persistence-level vpn|tcp|ssl| sticky]
```

## Mode

Configure.

## Description

The **load-balance create group-name** command lets you create a load balancing server group and specify a unique “virtual” IP address and port number that is used by a client to access any server in the group. You must also specify the protocol (for example, TCP for HTTP and FTP sessions) to be used by the load balancing servers. After you create the group with this command, use the **load-balance add host** command to add specific server systems to the group.

**Note:** If you want to create many groups, each with a virtual IP address, use the **load-balance create vip-range-name** command. Do not use an IP address for load-balancing that is already configured for VRRP.

## Parameters

|                                      |  |
|--------------------------------------|--|
| <b>group-name</b><br><group name>    | The name of this group of load balancing servers.  |
| <b>virtual-ip</b> <ipaddr>           | <p>The address in the form a.b.c.d that will be used as the IP address for this group.</p> <p><b>Note:</b> Do not use an IP address for load-balancing that is already configured for VRRP.</p>  |
| <b>virtual-port</b><br><port number> | <p>The port number to be used for this group. Specify a number between 1 and 65535.</p> <p><b>Note:</b> You cannot specify port number 20, as it is the FTP data port. If you create a group on the FTP control port for FTP, an implicit group will be created on port number 20.</p> |
| <b>protocol</b> tcp udp              | The protocol used by this group of load balancing servers.   |

|   |  |
|---|--|
| <b>persistence-level</b><br><b>vpn tcp ssl sticky</b> | The level of persistence to use for the bindings or connections, either vpn, tcp (TCP), ssl (secure socket layer), or sticky. tcp is the default if the persistence-level parameter is not specified. Sticky connections allow a client to connect to the same real server as in previous connections. |
|---|--|

## Restrictions

The X-Pedition router allows users to create two load balance groups that use the same address and port as long as the groups use the same protocol (i.e., UDP or TCP). If a user attempts to create groups with different protocols, the following error messages will appear:

```
%CLI-E-FAILED, Execution failed for "load-balance create group-name abc2 virtual-ip 10.10.10.1 virtual-port 12
protocol tcp"
%LOADBAL-E-VIPPORTUSED, Virtual IP 10.10.10.1 and Virtual Port 12 combination is already used
```

**Note:** Do not use an IP address for load-balancing that is already configured for VRRP.

## Example

To configure the server group 'service2':

```
xp(config)# load-balance create group-name service2 virtual-ip 10.10.100.100 virtual-port 80
protocol tcp
```

# load-balance create vip-range-name

## Purpose

Creates a group of servers for load balancing.

## Format

```
load-balance create vip-range-name <range name> vip-range <range>  
virtual-port <port number> protocol tcp|udp [persistence-level vpn|tcp|ssl| sticky]
```

## Mode

Configure.

## Description

The **load-balance create vip-range-name** command lets you specify a range of “virtual” IP addresses and a port number that is used by a client to access a server in the virtual IP address range. You must also specify the protocol (for example, TCP for HTTP and FTP sessions) to be used by the load balancing servers.

This command *implicitly* creates separate server groups for each virtual IP address in the specified range. The <range name> you specify becomes the base group name. Thus, the command **load-balance create vip-range-name myrange vip-range 207.135.89.1-207.135.89.15 virtual-port 80 protocol tcp** creates the groups ‘myrange1’ with virtual IP address 207.135.89.1, ‘myrange2’ with virtual IP address 207.135.89.2, etc. This command allows you to create *multiple* server groups, each with unique virtual IP addresses, whereas the **load-balance create group-name** command allows you to only create a *single* group with a *single* virtual IP address.

After you create groups with this command, you can use the **load-balance add host-to-group** command to identify specific server systems in each group. Or, you can use the **load-balance add host-to-vip-range** command to add a range of server IP addresses to each group.

## Parameters

|                                       |  |
|---------------------------------------|--|
| <b>vip-range-name</b><br><range name> | The base group name for this range of load balancing servers.  |
| <b>vip-range</b> <range>              | The range of virtual IP addresses to be created.   |
| <b>virtual-port</b><br><port number>  | The port number to be used for this virtual IP range. Specify a number between 1 and 65535.<br><br><b>Note:</b> You cannot specify port number 20, as it is the FTP data port. |
| <b>protocol</b> tcp udp               | The protocol used by this virtual IP range.  |

|   |   |
|---|---|
| <b>persistence-level</b><br><b>vpn tcp ssl sticky</b> | The level of persistence to use for the bindings, either <b>vpn</b> , <b>tcp</b> , or <b>ssl</b> (secure socket layer). <b>tcp</b> is the default if the persistence-level parameter is not specified. Sticky connections allow a client to connect to the same real server as in previous connections. |
|---|---|

## Restrictions

None.

## Example

To configure the server groups 'service1' through 'service15':

```
xp(config)# load-balance create vip-range-name service vip-range 207.135.89.1-207.135.89.15
virtual-port 80 protocol tcp
```

# load-balance set aging-for-src-maps

## Purpose

Set the aging time for the mappings of a group.

## Format

**load-balance set aging-for-src-maps** *<string>* **aging-time** *<num>*

## Mode

Configure.

## Description

The **load-balance set aging-for-src-maps** command sets the aging time for server group mapping. Once the aging time has expired, mapping from a client to a selected server within the group is cleared. This allows the user to better configure timeout values to specific server groups instead of using a general timeout value for all groups.

## Parameters

|  |  |
|--|--|
| <b>aging-for-src-maps</b><br><i>&lt;string&gt;</i> | Specifies the name of the server group.  |
| <b>aging-time</b> <i>&lt;num&gt;</i>               | Specifies the aging time in minutes. Specify a number between 1 and 4320. The default values depend on which persistence level is selected for a group. Persistence levels vpn and tcp has a default value of 3 minutes. Persistence levels ssl and sticky has a default value of 120 minutes. |

## Restrictions

None.

## Example

To set the aging time to 120 minutes for the server group 'group1':

```
xp(config)# load-balance set aging-for-src-maps group1 aging-time 120
```

# load-balance set client-proxy-subnet

## Purpose

Set the subnet for client address range mapping.

## Format

**load-balance set client-proxy-subnet** <group name> **subnet** <num>

## Mode

Configure.

## Description

The **load-balance set client-proxy-subnet** command sets the subnet used for mapping clients to a specific server group.

## Parameters

|  |  |
|--|--|
| <b>client-proxy-subnet</b><br><group name> | Specifies the name of the server group.                  |
| <b>subnet</b> <num>                        | Specifies the subnet. Specify a number between 1 and 31. |

## Restrictions

None.

## Example

To set the subnet number to 10 for the server group 'group1':

```
xp(config)# load-balance set client-proxy-subnet group1 subnet 10
```



# load-balance set ftp-control-port

## Purpose

Specifies the port for FTP control.

## Format

**load-balance set ftp-control-port** *<port number>*

## Mode

Configure.

## Description

File Transfer Protocol (FTP) packets require special handling with load balancing, because IP address information is contained within the FTP packet data. You can use the **load-balance set ftp-control-port** command to specify the port number that is used for FTP control. The default is port 21.

## Parameters

|   |  |
|---|--|
| <b>ftp-control-port</b><br><i>&lt;port number&gt;</i> | Specifies the port number used for FTP control. Specify a value between 1 and 65535. |
|---|--|

## Restrictions

None.

## Example

To set the FTP control port to 5000:

```
xp(config)# load-balance set ftp-control-port 5000
```

# load-balance set group-options

## Purpose

Sets options for a virtual group.

## Format

```
load-balance set group-options <string> [ping-int <num>] [ping-tries <num>]  
[app-int <num>] [app-tries <num>] [acv-command <string> acv-reply <string>]  
[acv-quit <string>] [read-till-index <num>] [check-port <port number>]
```

## Mode

Configure.

## Description

The **load-balance set group-options** command allows you to set various parameters for checking server content of a load balancing server group. This group must already be created with the **load-balance create group-name** command.

## Parameters

|                                  |   |
|----------------------------------|---|
| <b>group-options</b><br><string> | The name of the group of load balancing servers.  |
| <b>ping-int</b>                  | Use this parameter to set the ping interval (seconds) for servers in this group. Specify any value between 1 and 3600. The default value is 5.  |
| <b>ping-tries</b>                | Use this parameter to set the number of ping retries before marking the server down. Specify any value between 1 and 255. The default value is 4.   |
| <b>app-int</b>                   | Use this parameter to set the interval (seconds) between application checks. Specify any value between 1 and 3600. The default value is 15.   |
| <b>app-tries</b>                 | Use this parameter to set the number of retries before marking the application down. Specify any value between 1 and 255. The default value is 4.   |
| <b>acv-command</b>               | <p>The command or series of commands to pass to the server to request the desired file or response. For example, an HTTP command might be:<br/>“GET /index.html HTTP/1.1\r\nHost: &lt;server IP&gt;\r\n\r\n”</p> <p><b>Note:</b> You must explicitly add any carriage returns (\r) or line feeds (\n) to the end of any command you pass to the server.</p> |
| <b>acv-reply</b>                 | The response expected from the server.  |

|                        |   |
|------------------------|---|
| <b>acv-quit</b>        | The command that must be supplied to terminate the connection with the server (e.g., QUIT for SMTP, BYE for FTP—not required for HTTP). Please note that the CLI will add a Line Feed (\n) to this command before sending it to the server. |
| <b>read-till-index</b> | The number of bytes of the response to read (from 2 to 255) before starting an acv-reply.   |
| <b>check-port</b>      | Use this parameter to set an alternate port for application checks. Specify a number between 1 and 65535.   |

## Restrictions

None.

## Example

To set the load-balancing group-options for the server group 'service2' to ping every 5 seconds:

```
xp(config)# load-balance set group-options service2 ping-int 5
```

# load-balance set group-conn-thresh

## Purpose

Sets the connection threshold for each server in this group.

## Format

**load-balance set group-conn-thresh** *<string>* **limit** *<num>*

## Mode

Configure.

## Description

The **load-balance set group-options** command allows you to set a limit on how many connections will be supported for a load balancing server group. This number will be the maximum number of connections allowed for each server in the group. This group must already be created with the **load-balance create group-name** command.

## Parameters

|   |   |
|---|---|
| <b>group-conn-thresh</b><br><i>&lt;string&gt;</i> | The name of the group of load balancing servers.  |
| <b>limit</b> <i>&lt;num&gt;</i>                   | Specifies the number of connections that are supported by the server group. Specify any number between 1 and 65535. |

## Restrictions

None.

## Example

To set the maximum number of connections to 50000 connections for server group 'service2':

```
xp(config)# load-balance set group-conn-thresh service2 limit 50000
```

# load-balance set hash-variant

## Purpose

Sets the hash variant for calculating the load-balancing mappings index.

## Format

**load-balance set hash-variant** <value>

## Mode

Configure.

## Description

The **load-balance set hash-variant** command sets the hash variant that is used to calculate the load-balancing mappings index. You will only need to set this variant if the **load-balance show hash-stats** command output shows extremely uneven distribution of hash table entries.

## Parameters

|                                |   |
|--------------------------------|---|
| <b>hash-variant</b><br><value> | Specifies the hash variant. Specify 0, 1, or 2. The default value is 0. |
|--------------------------------|---|

## Restrictions

None.

## Example

To set the hash variant to 1:

```
xp(config)# load-balance set hash-variant 1
```

## load-balance set mappings-age-timer

### Purpose

Specifies the timeout for sessions between hosts and load-balancing servers.

### Format

**load-balance set mappings-age-timer** <timer>

### Mode

Configure.

### Description

A mapping between a host (source) and a load-balancing server (destination) times out after a period of non-use. The **load-balance set mappings-age-timer** command allows you to set the timeout for the mappings. The default is 3 minutes.

### Parameters

---

|                                      |   |
|--------------------------------------|---|
| <b>mappings-age-timer</b><br><timer> | The number of minutes before a source-destination mapping times out.<br>Specify a value between 3-4320. |
|--------------------------------------|---|

---

### Restrictions

None.

### Example

To set the timeout for load-balancing mappings to 720 minutes (12 hours):

```
xp(config)# load-balance set mappings-age-timer 720
```

# load-balance set policy-for-group

## Purpose

Specifies the policy for distributing workload on load-balancing servers.

## Format

**load-balance set policy-for-group** <group name> **policy** <policy>

## Mode

Configure.

## Description

The **load-balance set policy-for-group** command specifies how the X-Pedition router selects the server that will service a new session. The default policy for distributing workload among the load balancing servers is “round-robin,” where the router selects the server on a rotating basis.

## Parameters

|   |   |
|---|---|
| <b>policy-for-group</b><br><group name> | The name of this group of load balancing servers.   |
| <b>policy</b> <policy>                  | One of the following keywords: <ul style="list-style-type: none"><li><b>round-robin</b> The servers are selected sequentially (round-robin), without regard to the load on individual servers. This is the default policy.</li><li><b>weighted-round-robin</b> A variation of the round-robin policy. The router still selects servers in turn, but during its turn, each server takes on a number of session connections according to its assigned weight. For example, if server1 is assigned a weight of 1000 and server2 is assigned a weight of 10, then server1 will be assigned 1000 sessions during its turn and server2 will be assigned 10 sessions. If using this policy, you should assign different weights to each server in the group with the <b>load-balance add host-to-group</b> or the <b>load-balance add host-to-vip-range</b> command.</li><li><b>least-loaded</b> The server with the fewest number of sessions bound to it is selected to service the new session.</li></ul> |

## Restrictions

None.

## Example

To set the load-balancing policy for the server group ‘service2’ to ‘weighted round robin’:

```
xp(config)# load-balance set policy-for-group service2 policy weighted-round-robin
```



# load-balance set server-status

## Purpose

Sets the status of a load balancing server.

## Format

**load-balance set server-status server-ip** <ipaddr/range> **server-port** <port number>  
**group-name** <group name> **status up|down**

## Mode

Enable.

## Description

The **load-balance set server-status** command allows you to set the status of a load balancing server. When the status of a server is set to “down,” no *new* sessions are directed to that server. Current sessions on the server are not affected. This command can be used when server content needs to be updated or to bring one or more backup servers online during peak usage times.

## Parameters

|                                     |  |
|-------------------------------------|--|
| <b>server-ip</b><br><ipaddr/range>  | IP address of the server whose status is to be set.<br><br><b>Note:</b> Do not use an IP address for load-balancing that is already configured for VRRP. |
| <b>server-port</b><br><port number> | Port number of the server whose status is to be set.   |
| <b>group-name</b><br><group name>   | Group name to which this server belongs.   |
| <b>status up down</b>               | Sets the server status to up or down. Setting a server’s status to down will cause new sessions <i>not</i> to be directed to the server.                 |

## Restrictions

Do not use an IP address for load-balancing that is already configured for VRRP.

## Example

To set the status for the server 10.10.1.2 to 'down':

```
xp# load-balance set server-status server-ip 10.10.1.2 server-port 80 group-name service2 status  
down
```

# load-balance set server-options

## Purpose

Sets options for a destination server.

## Format

```
load-balance set server-options <string> [port <num>] [ping-int <num>] [ping-tries <num>]
[app-int <num>] [app-tries <num>] [acv-command <string> acv-reply <string>]
[acv-quit <string>] [read-till-index <num>] [check-port <port number>]
```

## Mode

Configure.

## Description

The **load-balance set server-options** command allows you to set various parameters for a load balancing destination server.

## Parameters

|                                   |   |
|-----------------------------------|---|
| <b>server-options</b><br><string> | The name of the destination server.   |
| <b>port</b> <num>                 | Use this parameter to select the port running the application on the destination server.  |
| <b>ping-int</b> <num>             | Use this parameter to set the ping interval (seconds) for servers in this group. Specify any value between 1 and 3600. The default value is 5.  |
| <b>ping-tries</b> <num>           | Use this parameter to set the number of ping retries before marking the server down. Specify any value between 1 and 255. The default value is 4.   |
| <b>app-int</b> <num>              | Use this parameter to set the interval (seconds) between application checks. Specify any value between 1 and 3600. The default value is 15.   |
| <b>app-tries</b> <num>            | Use this parameter to set the number of retries before marking the application down. Specify any value between 1 and 255. The default value is 4.   |
| <b>acv-command</b><br><string>    | <p>The command or series of commands to pass to the server to request the desired file or response. For example, an HTTP command might be:<br/>“GET /index.html HTTP/1.1\r\nHost: &lt;server IP&gt;\r\n\r\n”</p> <p><b>Note:</b> You must explicitly add any carriage returns (\r) or line feeds (\n) to the end of any command you pass to the server.</p> |

|                                    |   |
|------------------------------------|---|
| <b>acv-reply</b> <string>          | The response expected from the server.  |
| <b>acv-quit</b> <string>           | The command that must be supplied to terminate the connection with the server (e.g., QUIT for SMTP, BYE for FTP—not required for HTTP). Please note that the CLI will add a Line Feed (\n) to this command before sending it to the server. |
| <b>read-till-index</b>             | The number of bytes of the response to read (from 2 to 255) before starting an acv-reply.   |
| <b>check-port</b><br><port number> | Use this parameter to set an alternate port for application checks. Specify a number between 1 and 65535.   |

## Restrictions

None.

## Example

To set the load-balancing server-options for the destination server 'server2' to ping every 5 seconds:

```
xp(config)# load-balance set server-options server2 ping-int 5
```

# load-balance set vpn-dest-port

## Purpose

Sets the destination port for VPNs.

## Format

**load-balance set vpn-dest-port** <num>

## Mode

Configure.

## Description

The **load-balance set vpn-dest-port** command allows you to set the destination port number for load balanced VPNs.

## Parameters

|                               |  |
|-------------------------------|--|
| <b>vpn-dest-port</b><br><num> | Specifies the destination port number. Specify any number between 1 and 65535. Default is 500. |
|-------------------------------|--|

## Restrictions

Do not specify port 20, since this is the number designated for the FTP data port.

## Example

To set the destination port to port 5000:

```
xp(config)# load-balance set vpn-dest-port 5000
```

## load-balance show acv-options

### Purpose

Displays load balance application content verification (acv) options.

### Format

```
load-balance show acv-options [group-name <string>] [destination-host-ip <ipaddr>]  
[destination-host-port <num>]
```

### Mode

Enable.

### Description

The **load-balance show acv-options** command allows you to display load balancing acv options.

### Parameters

|  |  |
|--|--|
| <b>group-name</b><br><string>          | Use this parameter to show acv-options of the servers belonging to this group.   |
| <b>destination-host-ip</b><br><ipaddr> | Use this parameter to show acv-options of the servers that are a part of the group with this Virtual IP.                                       |
| <b>destination-host-port</b> <num>     | Use this parameter to show acv-options of servers that are a part of the group with this Virtual port. Specify any number between 1 and 65535. |

### Restrictions

None.

# **load-balance show hash-stats**

## **Purpose**

Displays load balancing hashing statistics.

## **Format**

**load-balance show hash-stats**

## **Mode**

Enable.

## **Description**

The **load-balance show hash-stats** command allows you to display load balancing hash statistics.

## **Parameters**

None.

## **Restrictions**

None.

## Example

To display hash statistics:

```
xp# load-balance show hash-stats
```

```
Total Mappings: 4502
```

```
Top 10 Hash Depths:
```

| +-----+-----+-----+ |            |                       |  |
|---------------------|------------|-----------------------|--|
| Index               | Hash Depth | Hash Depth Occurrence |  |
| +-----+-----+-----+ |            |                       |  |
| 1                   | 0          | 11882                 |  |
| 2                   | 1          | 4226                  |  |
| 3                   | 2          | 138                   |  |
| +-----+-----+-----+ |            |                       |  |

```
Top 10 Hash Depth Occurrences:
```

| +-----+-----+-----+ |                       |            |  |
|---------------------|-----------------------|------------|--|
| Index               | Hash Depth Occurrence | Hash Depth |  |
| +-----+-----+-----+ |                       |            |  |
| 1                   | 11882                 | 0          |  |
| 2                   | 4226                  | 1          |  |
| 3                   | 138                   | 2          |  |
| +-----+-----+-----+ |                       |            |  |



# load-balance show source-mappings

## Purpose

Displays load balancing source-destination bindings.

## Format

**load-balance show source-mappings client-ip** <ipaddr> **virtual-ip** <ipaddr>  
**virtual-port** <port number> **destination-host-ip** <ipaddr>

## Mode

Enable.

## Description

The **load-balance show source-mappings** command allows you to display load balancing source-destination bindings.

## Parameters

|                                     |  |
|-------------------------------------|--|
| <b>client-ip</b> <ipaddr>           | IP address of client whose mappings are to be shown.                 |
| <b>virtual-ip</b> <ipaddr>          | Virtual IP address whose mappings are to be shown.                   |
| <b>virtual-port</b> <port number>   | Virtual port number whose mappings are to be shown.                  |
| <b>destination-host-ip</b> <ipaddr> | IP address of the destination server whose mappings are to be shown. |

## Restrictions

None.

## Example

To display source-destination bindings:

```
xp# load-balance show source-mappings
```

Current Mappings:

FC: Flow Count

AC: Age Count

SPort: Source Port

VPort: Virtual Port

DPort: Destination Port

| Source Address | Sport | Virtual IP | VPort | Dst. Address | DPort | FC | AC |
|----------------|-------|------------|-------|--------------|-------|----|----|
| 70.1.0.71      | 1024  | 50.1.1.18  | 80    | 52.1.1.73    | 80    | 2  | 0  |
| 70.1.0.71      | 1025  | 50.1.1.17  | 80    | 52.1.1.71    | 80    | 2  | 0  |
| 70.1.0.72      | 1026  | 50.1.1.17  | 80    | 52.1.1.72    | 80    | 2  | 0  |
| 70.1.0.72      | 1027  | 50.1.1.18  | 80    | 52.1.1.74    | 80    | 2  | 0  |

4 source mapping(s) displayed.

# load-balance show statistics

## Purpose

Displays load balancing statistics.

## Format

**load-balance show statistics group-name** <group name> **virtual-ip** <ipaddr>  
**virtual-port** <port number>

## Mode

Enable.

## Description

The **load-balance show statistics** command allows you to display load balancing statistics.

## Parameters

|                                   |   |
|-----------------------------------|---|
| <b>group-name</b> <group name>    | Name of the group whose statistics are to be shown.   |
| <b>virtual-ip</b> <ipaddr>        | Virtual IP address whose statistics are to be shown.  |
| <b>virtual-port</b> <port number> | Virtual port number whose statistics are to be shown. |

## Restrictions

None.

## Example

To display load balance statistics:

```
xp# load-balance show statistics

Load Balancing Packets Dropped:
  No Such Virtual-IP Packet drop count:      73
  TTL expired Packet drop count:             0

Load Balance Group Statistics:

  Group Name: telnet Virtual-IP: 50.1.1.17 Virtual-Port: 23
    No destination selected Packet drop count: 0
    Memory Allocation error Packet drop count: 0
    No forward route found Packet drop count: 0
    Number of Packets forwarded:              23437
    Channel not Load Balancing compliant Packet drop count : 0
    No hosts in group Packet drop count:      0
    Client in Access List Packet drop count:   2

  Group Name: http Virtual-IP: 50.1.1.17 Virtual-Port: 80
    No destination selected Packet drop count: 2
    Memory Allocation error Packet drop count: 0
    No forward route found Packet drop count: 0
    Number of Packets forwarded:              34429
    Channel not Load Balancing compliant Packet drop count : 0
    No hosts in group Packet drop count:      0
    Client in Access List Packet drop count:   1

Statistics of 2 groups shown.
```

# load-balance show virtual-hosts

## Purpose

Displays hosts in a load balancing group.

## Format

**load-balance show virtual-hosts group-name** *<group name>* **virtual-ip** *<ipaddr>*  
**virtual-port** *<port number>*

## Mode

Enable.

## Description

The **load-balance show virtual-hosts** command allows you to display the hosts in a load balancing group.

## Parameters

|  |   |
|--|---|
| <b>group-name</b> <i>&lt;group name&gt;</i>    | The load balancing group that is to be shown. |
| <b>virtual-ip</b> <i>&lt;ipaddr&gt;</i>        | IP address of the group that is to be shown.  |
| <b>virtual-port</b> <i>&lt;port number&gt;</i> | Port number of the group that is to be shown. |

## Restrictions

None.

## Example

To display load balance groups:

```
xp# load-balance show virtual-hosts
```

Load Balanced Groups:

Flow Mode Count: 0

OS: Operational state of server

AS: Admin state of server

| Group Name | Virtual IP | Port | Hosts Added | Hosts Up | Next Index |
|------------|------------|------|-------------|----------|------------|
| telnet     | 50.1.1.17  | 23   | 2           | 2        | 0          |

| Index | Host IP   | Port | Client Count | OS | AS | Load Count |
|-------|-----------|------|--------------|----|----|------------|
| 0     | 52.1.1.73 | 23   | 0            | Up | Up | 0          |
| 1     | 52.1.1.74 | 23   | 0            | Up | Up | 0          |

| Group Name | Virtual IP | Port | Hosts Added | Hosts Up | Next Index |
|------------|------------|------|-------------|----------|------------|
| http       | 50.1.1.17  | 80   | 2           | 2        | 0          |

| Index | Host IP   | Port | Client Count | OS | AS | Load Count |
|-------|-----------|------|--------------|----|----|------------|
| 0     | 52.1.1.71 | 80   | 0            | Up | Up | 0          |
| 1     | 52.1.1.72 | 80   | 0            | Up | Up | 0          |

# Chapter 38

## logout Command

The **logout** command ends the CLI session.

### Format

**logout**

### Mode

All modes.

### Description

The **logout** command ends your CLI session. If you have uncommitted changes in the scratchpad, a message warns you that the changes are not saved and gives you an opportunity to cancel the logout and save the changes.

### Parameters

None.

### Restrictions

None.





# Chapter 39

## mstp Commands

The **mstp** commands let you display and change settings for the Multiple Spanning Tree Protocol (802.1s).

### Command Summary

[Table 34](#) lists the **mstp** commands. The sections following the table describe the command syntax.

**Table 34. mstp Commands**

|  |
|--|
| <b>mstp start</b>  |
| <b>mstp create msti</b> <num>  |
| <b>mstp disable edge-auto-detection</b>  |
| <b>mstp enable legacy-path-cost</b>  |
| <b>mstp enable per-port-hello-mode</b>   |
| <b>mstp enable port</b> <port-list>  |
| <b>mstp map</b> <num> <b>vlan</b> <num>  |
| <b>mstp set bridging forward-delay</b> <num>   |
| <b>mstp set bridging hello-time</b> <num> [ <b>port</b> <port-list>]                             |
| <b>mstp set bridging max-age</b> <num>   |
| <b>mstp set bridging max-hops</b> <num>  |
| <b>mstp set bridging priority</b> <num> [ <b>msti</b> <num>]                                     |
| <b>mstp set configuration-id</b> [ <b>name</b> <string mstp-null-name>] [ <b>revision</b> <num>] |

**Table 34. mstp Commands (Continued)**

|  |
|--|
| <b>mstp set port</b> <port-list> [ <b>priority</b> <num> <b>msti</b> <num>] [ <b>port-cost</b> <num> <b>msti</b> <num>]<br>[ <b>point-to-point</b> <ForceTrue ForceFalse Auto>] [ <b>edge-port</b> <True False>] |
| <b>mstp set version</b> <mstp rstp stp>  |
| <b>mstp show bpdu-stats port</b> <port-list all-mstp-ports> <b>msti</b> <num>  |
| <b>mstp show bridging</b>  |
| <b>mstp show instances</b>   |
| <b>mstp show map</b>   |
| <b>mstp show stats msti</b> <num> [ <b>port</b> <port-list all-mstp-ports>]  |

**Note:** The X-Pedition router does not support MSTP over ATM, WAN or Packet over SONET (POS).

**Note:** The X-Pedition router does not support concurrently running MSTP with other spanning tree protocols (STP, RSTP, and PVST). If any non-mstp spanning tree protocol command is present, **mstp** commands will display errors.

# **mstp start**

## **Purpose**

Enable the 802.1s MSTP protocol.

## **Format**

**mstp start**

## **Mode**

Configure.

## **Description**

The **mstp start** command enables the 802.1s MSTP protocol. The **mstp** configuration commands cannot be added to the active configuration until the **mstp start** command is configured.

## **Restrictions**

MSTP cannot be started if the active configuration already contains valid STP, RSTP, or PVST or commands.

## mstp create msti

### Purpose

Create a Multiple Spanning Tree Instance (MSTI) for MSTP.

### Format

**mstp create msti** <num>

### Mode

Configure.

### Description

The **mstp create msti** command creates an MSTI for MSTP. MSTP supports a total of 64 MSTIs, not including the Common and Internal Spanning Tree (CIST).

### Parameters

---

|                   |  |
|-------------------|--|
| <b>msti</b> <num> | A number from 1 to 4094. 0 is the reserved number of the CIST. |
|-------------------|--|

---

### Restrictions

MSTP must be enabled with the **mstp start** command.

# **mstp disable edge-auto-detection**

## **Purpose**

Disable automatic detection of edge ports for MSTP.

## **Format**

**mstp disable edge-auto-detection**

## **Mode**

Configure.

## **Description**

The **mstp disable edge-auto-detection** command disables the automatic detection of edge ports feature for MSTP. You can manually configure a port as an edge port using the **mstp set port** command.

## **Restrictions**

MSTP must be enabled with the **mstp start** command.

## mstp enable legacy-path-cost

### Purpose

Force MSTP to use legacy path cost calculations.

### Format

**mstp enable legacy-path-cost**

### Mode

Configure.

### Description

The **mstp enable legacy-path-cost** command forces MSTP to use legacy path cost calculations for all ports. This command overrides any previously values configured with the **mstp set port port-cost** command. The **no mstp enable legacy-path-cost** command configures the ports to use 802.1t path cost algorithms. The default legacy port value costs are based on port speed as follows:

|                     |                      |
|---------------------|----------------------|
| Speed 1Mb cost 1000 | Speed 200Mb cost 17  |
| Speed 2Mb cost 500  | Speed 300Mb cost 15  |
| Speed 3Mb cost 333  | Speed 400Mb cost 14  |
| Speed 4Mb cost 250  | Speed 500Mb cost 12  |
| Speed 5Mb cost 200  | Speed 600Mb cost 10  |
| Speed 6Mb cost 166  | Speed 700Mb cost 9   |
| Speed 7Mb cost 142  | Speed 800Mb cost 7   |
| Speed 8Mb cost 125  | Speed 900Mb cost 5   |
| Speed 9Mb cost 111  | Speed 1000Mb cost 4  |
| Speed 10Mb cost 99  | Speed 2000Mb cost 4  |
| Speed 20Mb cost 90  | Speed 3000Mb cost 4  |
| Speed 30Mb cost 81  | Speed 4000Mb cost 4  |
| Speed 40Mb cost 72  | Speed 5000Mb cost 3  |
| Speed 50Mb cost 63  | Speed 6000Mb cost 3  |
| Speed 60Mb cost 54  | Speed 7000Mb cost 3  |
| Speed 70Mb cost 45  | Speed 8000Mb cost 3  |
| Speed 80Mb cost 36  | Speed 9000Mb cost 2  |
| Speed 90Mb cost 27  | Speed 10000Mb cost 2 |
| Speed 100Mb cost 19 | Speed 50000Mb cost 1 |

**Note:** Enterasys recommends that you comment out any previous values configured with the **mstp set port port-cost** command.

## **Restrictions**

MSTP must be enabled with the **mstp start** command.

## **mstp enable per-port-hello-mode**

### **Purpose**

Enable hello time parameters to be configured on a per port basis for MSTP.

### **Format**

**mstp enable per-port-hello-mode**

### **Mode**

Configure.

### **Description**

The **mstp enable per-port-hello-mode** command allows hello time parameters to be configured on a per port basis. By default, the **mstp set bridging hello-time** command is applied to all ports. If the **mstp enable per-port-hello-mode** command is configured, the **port** option may be specified in the **mstp set bridging hello-time** command.

### **Restrictions**

MSTP must be enabled with the **mstp start** command.



# mstp enable port

## Purpose

Enable MSTP on one or more ports.

## Format

**mstp enable port** *<port-list>*

## Mode

Configure.

## Description

The **mstp enable port** command enables MSTP on the specified ports.

## Parameters

---

|                          |  |
|--------------------------|--|
| <i>&lt;port-list&gt;</i> | You can specify a single port or a comma-separated list of ports.<br>Example: et.1.3,et.(1-3).(4,6-8). |
|--------------------------|--|

---

## Restrictions

- MSTP must be enabled with the **mstp start** command.
- Individual ports that are members of SmartTRUNKs, ATM, WAN, or Packet over SONET (POS) cannot be specified in the port list.

# mstp map vlan

## Purpose

Map one or more VLANs to an MSTI for MSTP.

## Format

**mstp map** <num> **vlan** <num>

## Mode

Configure.

## Description

The **mstp map vlan** command maps one or more VLANs to an MSTI. On the X-Pedition router, the VLAN identification (VID) to Filtering identification (FID) are mapped 1 to 1. By assigning a VLAN to an MSTI, the same FID is assigned to the MSTI. The VID/FID to MSTI mappings must be identical for all devices configured in an MST region. The mappings are used to create the Configuration Digest portion of a device's Configuration Identifier. If the Configuration Identifier differs between devices, the devices will consider themselves part of different MST regions. By default, all VIDs/FIDs are mapped to MSTI 0, which is the CIST.

If a **mstp map vlan** command is negated, all the VIDs/FIDs in the command will be mapped back to the CIST. Multiple **mstp map vlan** commands for the same MSTI are automatically merged into one command.

## Parameters

|                     |   |
|---------------------|---|
| <b>[msti]</b> <num> | A number from 1 to 4094. The MSTI number must already exist, otherwise this command will error out.   |
| <b>vlan</b> <num>   | A number from 1 to 4095. The VLAN does not need to exist for this command to work. If the VLAN does not exist, the FID mapping will still be set appropriately. |

## Restrictions

MSTP must be enabled with the **mstp start** command.

# **mstp set bridging forward-delay**

## **Purpose**

Set the bridging forward delay for MSTP.

## **Format**

**mstp set bridging forward-delay** *<num>*

## **Mode**

Configure.

## **Description**

The **mstp set bridging forward-delay** command sets the forward delay (in seconds), which is the time the port transitions from learning to forwarding.

## **Parameters**

---

|                    |   |
|--------------------|---|
| <i>&lt;num&gt;</i> | A number from 4 to 30. The time is specified in seconds. The default is 15 seconds. |
|--------------------|---|

---

## **Restrictions**

MSTP must be enabled with the **mstp start** command.

# mstp set bridging hello-time

## Purpose

Set the bridging hello time for MSTP.

## Format

**mstp set bridging hello-time** <num> [**port** <port-list>]

## Mode

Configure.

## Description

The **mstp set bridging hello-time** command sets the hello time (in seconds). By default, this parameter applies to all ports on the device. If the **msti enable per-port-hello-mode** command was issued, the **port** option of the **mstp set bridging hello-time** command may be specified. The **port** option allows the hello time to be set on a per port basis.

## Parameters

|                         |  |
|-------------------------|--|
| <b>hello-time</b> <num> | A number from 1 to 10. The time is specified in seconds. The default is 2 seconds.   |
| <b>port</b> <port-list> | The ports on which you are setting the hello time. You can specify a single port or a comma-separated list of ports. Example: et.1.3,et.(1-3).(4,6-8). |

## Restrictions

- MSTP must be enabled with the **mstp start** command.
- To specify individual ports, you must first enter the **msti enable per-port-hello-mode** command.

# **mstp set bridging max-age**

## **Purpose**

Set the bridging max age for MSTP.

## **Format**

**mstp set bridging max-age** *<num>*

## **Mode**

Configure.

## **Description**

The **mstp set bridging max-age** command sets the max age (in seconds) for discarding stored configuration messages.

## **Parameters**

---

|                                   |   |
|-----------------------------------|---|
| <b>max-age</b> <i>&lt;num&gt;</i> | A number from 6 to 40. The time is specified in seconds. The default is 20 seconds. |
|-----------------------------------|---|

---

## **Restrictions**

MSTP must be enabled with the **mstp start** command.

# mstp set bridging max-hops

## Purpose

Set the bridging max hops for MSTP.

## Format

**mstp set bridging max-hops** <num>

## Mode

Configure.

## Description

The **mstp set bridging max-hops** command sets the max hops count. Each packet has the max hops number decremented after every hop, and it is discarded once it reaches 0. You should set the max hops count large enough so that the packet can reach every system in the region, accounting for path failures where the packet has to take the longest route. However, you should not set the count high enough that the packet can transverse the region multiple times.

## Parameters

---

|       |   |
|-------|---|
| <num> | A number from 0 to 255. The default is 20 hops. |
|-------|---|

---

## Restrictions

MSTP must be enabled with the **mstp start** command.

# mstp set bridging priority

## Purpose

Set the bridging priority for an MSTI for MSTP.

## Format

**mstp set bridging priority** <num> [**msti** <num>]

## Mode

Configure.

## Description

The **mstp set bridging priority** command sets the device priority for an MSTI. If the **msti** option is not specified, this command is applied to the CIST.

## Parameters

|                       |   |
|-----------------------|---|
| <b>priority</b> <num> | The <b>priority</b> option administratively sets the bridging priority of the device for the specified MSTI. 802.1s states that the priority can range from 0 to 61440, being specified in increments of 4096. The <b>priority</b> option can range from 0 to 15. The value is internally multiplied by 4096. By default, the bridge priority is 32768 ( <i>num</i> is set to 8). |
| <b>msti</b> <num>     | The set command is applied to this MSTI. If an <b>msti</b> is not specified, this command is applied to the CIST. The CIST is MSTI 0.   |

## Restrictions

MSTP must be enabled with the **mstp start** command.

# mstp set configuration-id

## Purpose

Set the configuration identifier parameters for MSTP.

## Format

**mstp set configuration-id** [**name** <string|mstp-null-name>] [**revision** <num>]

## Mode

Configure.

## Description

The **mstp set configuration-id** command sets the configurable Configuration Identifier parameters for MSTP. All devices in the same MST region must have identical Configuration Identifiers. The Configuration Identifier has four parts: Format Selector, Configuration Name, Revision Level and Configuration Digest. The Configuration Name and Revision Level can be administratively set. The Format Selector is always 0. The configured VID/FID to MSTI mappings are used internally to generate the Configuration Digest.

## Parameters

|  |   |
|--|---|
| <b>name</b> <string  <b>mstp-null-name</b> > | The Configuration Name can contain up to 32 characters. The default Configuration Name is a string version of the device's MAC address. The <b>mstp-null-name</b> keyword is used by SNMP to set a NULL string. |
| <b>revision</b> <num>                        | The Revision Level may be any number from 0 to 65535. The default Revision Level is 0.  |

## Restrictions

MSTP must be enabled with the **mstp start** command.



# mstp set port

## Purpose

Set port related parameters for MSTP.

## Format

```
mstp set port <port-list> [priority <num> msti <num>] [port-cost <num> msti <num>]
[point-to-point <ForceTrue|ForceFalse|Auto>] [edge-port <True|False>]
```

## Mode

Configure.

## Description

The **mstp set port** command configures the port related parameters.

## Parameters

|  |  |
|--|--|
| <b>port</b> <port-list>                                  | The ports you wish to configure. You can specify a single port or a comma-separated list of ports. Example: et.1.3,et.(1-3).(4,6-8).   |
| <b>priority</b> <num><br><b>msti</b> <num>               | Administratively sets the port priority of the specified ports for the specified MSTI. 802.1s states that the port priority can range from 0 to 240, being specified in increments of 16. The <b>priority</b> option can range from 0 to 15. The value is internally multiplied by 16. By default, the port priority is set to 128 ( <i>num</i> is set to 8).<br><br>The command is applied to a specified MSTI. If an <b>msti</b> is not specified, this command is applied to the CIST, which is MSTI 0. |
| <b>port-cost</b> <num><br><b>msti</b> <num>              | Administratively sets the port cost of the specified ports for the specified MSTI. The <b>port-cost</b> can range from 0 to 200,000,000. By default, MSTP uses the IEEE 802.1t path cost values.<br><br>The command is applied to specified MSTI. If an <b>msti</b> is not specified, this command is applied to the CIST, which is MSTI 0.  |
| <b>point-to-point</b><br><ForceTrue   ForceFalse   Auto> | Specifies a point-to-point link or non-point-to-point link. The default is <b>Auto</b> , which allows for the automatic detection of point-to-point links.   |
| <b>edge-port</b><br><True False>                         | Initializes the port as an edge port or non-edge port. The default is <b>False</b> (non-edge).   |

## Restrictions

MSTP must be enabled with the **mstp start** command.

# mstp set version

## Purpose

Force MSTP to run a specific version of spanning protocol.

## Format

**mstp set version** <mstp|rstp|stp>

## Mode

Configure.

## Description

The **mstp set version** command forces MSTP to run a specific version of spanning tree protocol: STP, RSTP, or MSTP. The type of BPDUs transmitted changes according to the version selected. Therefore you still use the MSTP commands to run legacy STP or RSTP. However, you cannot configure spanning tree over ATM, WAN, or Packet over SONET (POS).

## Parameters

|                               |   |
|-------------------------------|---|
| <b>version</b>                | The default spanning tree protocol version is <b>mstp</b> . |
| <b>&lt;mstp rstp  stp&gt;</b> |   |

## Restrictions

MSTP must be enabled with the **mstp start** command.

# mstp show bpdu-stats msti port

## Purpose

Display port BPDU statistics.

## Format

**mstp show bpdu-stats port** <port-list|all-mstp-ports> **msti** <num>

## Mode

Enable.

## Description

The **mstp show bpdu-stats** command displays the BPDU information for the specified ports for a given MSTI.

## Parameters

|   |   |
|---|---|
| <b>&lt;port-list  <br/>all-mstp-ports&gt;</b> | Specifies a single port or a comma-separated list of ports. Example: et.1.3,et.(1-3).(4,6-8). The <b>all-mstp-ports</b> keyword specifies all MSTP enabled ports. |
| <b>msti &lt;num&gt;</b>                       | Specifies the MSTI. If an <b>msti</b> is not specified, the command is applied to the CIST. The CIST is MSTI 0.   |

## Example

```
SSR6# mstp show bpdu-stats port et.14.3 msti 0
Port: et.14.3 MSTI: 0
-----
RX TCN: 1
RX CFG: 0
RX CFG/TC: 0
RX RSTP: 0
RX RSTP/TC: 0
RX MSTP: 1
RX MSTP/TC: 0
TX TCN: 0
TX CFG: 1
TX CFG/TC: 0
TX RSTP: 0
TX RSTP/TC: 0
TX MSTP: 46
TX MSTP/TC: 11
Invalid BPDUs: 0
```

## Restrictions

MSTP must be enabled with the **mstp start** command.

## mstp show bridging

### Purpose

Display MSTP Configuration Identifier and global MSTP configuration values.

### Format

**mstp show bridging**

### Mode

Enable.

### Description

The **mstp show bridging** command displays the MSTP Configuration Identifier and global MSTP values that are not port or MSTI specific.

### Example

```
SR6# mstp show bridging
MSTP Configuration ID
-----
Configuration Name:    South
Format Selector:      0
Revision Level:       0
Configuration Digest:  ac:36:17:7f:50:28:3c:d4:b8:38:21:d8:ab:26:de:62

MSTP Global Values
-----
Edge Auto Detection:   Enabled
Legacy Path Cost:      Enabled
Hello Mode:            Disabled
Hello Time:            2
Priority:               32768
Max Age:               20
Forward Delay:         15
Max Hops:              20
Protocol Version:      MSTP
```

### Restrictions

MSTP must be enabled with the **mstp start** command.

# **mstp show instances**

## **Purpose**

Display configured MSTIs.

## **Format**

**mstp show instances**

## **Mode**

Enable.

## **Description**

The **mstp show instances** command displays the configured MSTIs on the device.

## **Example**

```
SSR2# mstp show instances
The following multiple spanning tree instances (msti) have been created:
 1 2 3 4 5 6 7 8 9 10
Total number of MSTIs: 10
```

## **Restrictions**

MSTP must be enabled with the **mstp start** command.

## mstp show map

### Purpose

Display the VLAN/FID to MSTI table mapping.

### Format

**mstp show map**

### Mode

Enable.

### Description

The **mstp show map** command displays the VLAN/FID to MSTI table mapping.

### Example

```
SSR2# mstp show map
MSTI    Mapped VLANs (also known as FIDs)
=====
 1      1
 2      2
 3      3
 4      4
 5      5
 6      6
 7      7
 8      8
 9      9
10     10
```

### Restrictions

MSTP must be enabled with the **mstp start** command.



# mstp show stats msti

## Purpose

Display MSTI specific information.

## Format

**mstp show stats msti** <num> [**port** <port-list|all-mstp-ports>]

## Mode

Enable.

## Description

The **mstp show stats msti** command displays MSTI specific information.

## Parameters

|   |  |
|---|--|
| <b>msti</b> <num>                                   | Specifies the MSTI. The CIST is MSTI 0.  |
| <b>port</b> <port-list  <br><b>all-mstp-ports</b> > | You can specify a single port or a comma-separated list of ports.<br>Example: et.1.3,et.(1-3).(4,6-8). The <b>all-mstp-ports</b> keyword specifies all MSTP enabled ports. |

## Example

```
SSR2# mstp show stats msti 0 port gi.4.1
Spanning tree instance      - 0
Designated Root MacAddr    - 00:00:1d:0d:64:9a
Designated Root Priority    - 32768
Designated Root Cost       - 2
Designated Root Port       - st.3
Root Max Age               - 20 sec
Root Hello Time            - 2 sec
Root Hold Time             - 1 sec
Root Forward Delay         - 1500 sec
Bridge ID MacAddr          - 00:e0:63:a1:86:ef
Bridge ID Priority          - 32768
Bridge Max Age             - 20 sec
Bridge Hello Time          - 2 sec
Bridge Forward Delay       - 15 sec
Topology Change Count      - 8
Max Hops                   - 20
```

Information for: Port gi.4.1; MSTI 0  
Priority - 128  
State - Blocking  
Admin Path Cost - 0  
Operational Path Cost - 1  
Designated Root - 0x80:00:00:00:1d:0d:64:9a  
Designated Cost - 10  
Designated Bridge - 0x80:00:00:e0:63:0c:67:1a  
Designated Port - 80c5  
Role - Alternate  
Point to Point - Auto  
Edge Port - NO

## Restrictions

MSTP must be enabled with the **mstp start** command.

# Chapter 40

## multicast Commands

The **multicast** commands let you display information about IP multicast interfaces.

### Command Summary

[Table 35](#) lists the **multicast** commands. The sections following the table describe the command syntax.

**Table 35. multicast Commands**

|                                 |
|---------------------------------|
| <b>multicast show mfc</b>       |
| <b>multicast show sg-counts</b> |
| <b>multicast show vif</b>       |

## multicast show mfc

### Purpose

Displays the multicast forwarding cache information, including the exit port (s) for each (S,G) flow.

### Format

**multicast show mfc**

### Mode

Enable.

### Description

The Multicast Forwarding Cache stores forwarding information for each (S,G) flow. The **multicast show mfc** command displays a table containing this information.

### Parameters

None.

### Example

To display the multicast forwarding cache information, enter the following:

| xp# <b>multicast show mfc</b> |               |              |                |                  |
|-------------------------------|---------------|--------------|----------------|------------------|
| Source Address                | Group Address | Incoming I/f | Outgoing I/f   | Exit Ports       |
| -----                         | -----         | -----        | -----          | -----            |
| 20.0.0.1                      | 224.1.0.5     | NET20        | IXIA2<br>NET30 | et.2.8<br>gi.4.2 |
| 62.0.0.2                      | 224.1.0.7     | IXIA2        | NET20<br>NET30 | gi.4.1<br>gi.4.2 |

# multicast show sg-counts

## Purpose

Displays the packet and byte counts for each multicast forwarding cache entry.

## Format

**multicast show sg-counts**

## Mode

Enable.

## Description

The Multicast Forwarding Cache stores forwarding information for each (S,G) flow. The **multicast show sg-counts** command displays a table byte counts and packet counts.

## Parameters

None.

## Example

To display table byte and packet counts for multicast forwarding cache entries, enter the following:

|                                     |               |            |            |
|-------------------------------------|---------------|------------|------------|
| xp# <b>multicast show sg-counts</b> |               |            |            |
| Source Address                      | Group Address | Packet Cnt | Byte Count |
| -----                               | -----         | -----      | -----      |
| 10.32.32.5                          | 227.1.1.64    | 26920      | 41322130   |

# multicast show vif

## Purpose

Displays the virtual interface information for all multicast capable interfaces.

## Format

**multicast show vif**

## Mode

Enable.

## Description

Displays information about the virtual interface configurations used in multicast.

## Parameters

None.

## Example

To display the virtual interface configuration information, enter the following:

|   |              |    |            |             |          |
|---|--------------|----|------------|-------------|----------|
| <b>xp# multicast show vif</b>                 |              |    |            |             |          |
| F ->    0x01   - Vif is tunnel end-point      |              |    |            |             |          |
| 0x02   - Tunnel is using IP source routing    |              |    |            |             |          |
| 0x04   - Vif is used for register encap/decap |              |    |            |             |          |
| Vif   | Interface    | F  | Local Addr | Remote Addr | Portmask |
| ---   | -----        | -  | -----      | -----       | -----    |
| 0   | register_vif | 04 | 127.0.0.3  | 127.0.0.0   |          |

**Note:**    The “F” above represents flags.

# Chapter 41

## nat Commands

The **nat** commands allow you to define Network Address Translation (NAT) bindings for local (inside) and global (outside) network addresses.

### Command Summary

[Table 36](#) lists the **nat** commands. The sections following the table describe the command syntax.

**Table 36. nat Commands**

|   |
|---|
| <b>nat clear-err-stats out-of-globals   port-mode</b>   |
| <b>nat create dynamic local-acl-pool</b> <local-acl> <b>global-pool</b> <ip-addr/ip-addr-range/ip-addr-list> [ <b>matches-interface</b> <interface>] [ <b>enable-ip-overload</b> ]  |
| <b>nat create static protocol ip tcp udp local-ip</b> <local-ip-addr/address range> <b>global-ip</b> <global-ip-addr/address range> [ <b>local-port</b> <tcp/udp-local-port>  <b>any</b> ] [ <b>global-port</b> <tcp/udp-global-port>  <b>any</b> ]                           |
| <b>nat flush-dynamic-binding all  pool-specified</b> [ <b>local-acl-pool</b> <local-acl>] [ <b>global-pool</b> <ip-addr/ip-addr-range/ ip-addr-list>]   [ <b>type-specified dynamic   overloaded-dynamic</b> ]   <b>owner-specified</b> [ <b>dns  ftp-control  ftp-data</b> ] |
| <b>nat set dns-name-extension-error on off</b>  |
| <b>nat set dns-session-timeout</b> <num>  |
| <b>nat set dynamic-binding-timeout</b> <minutes>  <b>disable</b>  |
| <b>nat set ftp-control-port</b> <port number>   |
| <b>nat set ftp-session-timeout</b> <minutes>  |
| <b>nat set interface</b> <name> <b>inside outside</b>   |

**Table 36. nat Commands (Continued)**

|  |
|--|
| <b>nat set secure-plus on   off</b>                    |
| <b>nat show [translations] [timeouts] [statistics]</b> |



# nat clear-err-stats

## Purpose

Clears NAT error statistics.

## Format

**nat clear-err-stats out-of-globals | port-mode**

## Mode

Enable.

## Description

The **nat clear-err-stats** command allows you to clear specific NAT error statistics such as out-of-globals messages in the case of dynamic bindings and port misconfiguration.

## Parameters

|                       |  |
|-----------------------|--|
| <b>out-of-globals</b> | Clears error statistics during dynamic binding in the case where there are no more global IP addresses in the global address pool.   |
| <b>port-mode</b>      | Clears error statistics that occur because of port misconfigurations. Such cases are where the port is set to either destination-based forwarding or host-flow based forwarding. |

## Restrictions

None.

## Example

To clear all out-of-global error statistics:

```
xp(config)# nat clear-err-stats out-of-globals
```

# nat create dynamic

## Purpose

Defines local and global IP address pools for dynamic address binding.

## Format

```
nat create dynamic local-acl-pool <local-acl> global-pool <ip-addr/ip-addr-range/ip-addr-list>
[matches-interface <interface>] [enable-ip-overload]
```

## Mode

Configure.

## Description

The **nat create dynamic** command lets you specify the local-acl pool and global IP address pool that are to be used for dynamic address binding. With dynamic address translation, IP address bindings last only until the data flow ages out or the dynamic binding is manually deleted. Global IP addresses defined for dynamic translation are reassigned whenever they become free. The local address pool for dynamic bindings are defined via an ACL profile, while the global address pool must be specified as a single IP address, an address range, an IP address and mask, or an IP list. You can also specify multiple global pools for the same local-acl pool, if you have more than one connection to the Internet on different interfaces.

## Parameters

|   |   |
|---|---|
| <b>local-acl-pool</b><br><local-acl>                    | The ACL that corresponds to the local IP address pool. The ACL may contain either <b>permit</b> or <b>deny</b> keywords. Note that only the source IP address information in the ACL is used; other ACL parameters are ignored. Used in the case of address translation from an inside private to an outside public network.  |
| <b>global-pool</b> <ip-addr/ip-addr-range/ip-addr-list> | <p>The global address pool, defined in one of the following ways:</p> <ul style="list-style-type: none"><li>• A single IP address in the form a.b.c.d</li><li>• An IP address range in the form 10.10.1.1-10.10.1.50</li><li>• IP address and mask in the form 1.2.0.0/255.255.0.0 or 1.2.3.0/16</li><li>• A list of IP addresses, separated by spaces and enclosed in quotation marks.</li><li>• Used in the case of address translation from an inside private to an outside public network.</li></ul> <p><b>Note:</b> Do not specify more than 64K global addresses.</p> |

|   |  |
|---|--|
| <b>matches-interface</b><br><interface> | Specifies the interface to use for multiple global pools. Used in the case of address translation from an inside private to an outside public network.   |
| <b>enable-ip-overload</b>               | Enables Port Address Translation (PAT) if no global addresses are available from the pool. This allows many local addresses to be bound to a single global address using port numbers 1024 through 4999 (port numbers are not configurable). With PAT, multiple IP addresses can map to a single IP address with multiple numbers. Used in the case of address translation from an inside private to an outside public network.<br><br><b>Note:</b> Protocols like ICMP do not work with the <b>enable-ip-overload</b> option. Thus, the <b>ping</b> command will not work if this option is used. |

## Restrictions

None.

## Examples

To configure address pools for dynamic address bindings, first configure the ACL that corresponds to the local IP address pool. In the following example, the ACL 'lcl' corresponds to IP addresses from 10.1.1.1 to 10.1.1.254:

```
xp(config)# acl lcl permit ip 10.1.1.0/24
```

Then, specify this ACL for the local IP address pool for dynamic address bindings with global addresses 136.1.1.1 to 136.1.1.254:

```
xp(config)# nat create dynamic local-acl-pool lcl global-pool 136.1.1.0/24
```

The following examples show the use of Port Address Translation, where the global pool consists of only two specified IP addresses. In the following example, the ACL 'lcl' corresponds to IP addresses from 10.1.1.1 to 10.1.1.254:

```
xp(config)# acl lcl permit ip 10.1.1.0/24
```

Then, specify this ACL for the local IP address pool for dynamic address bindings with global addresses 136.1.1.1 and 136.1.1.2 with Port Address Translation enabled:

```
xp(config)# nat create dynamic local-acl-pool lcl global-pool 136.1.1.1-136.1.1.2 enable-ip-overload
```

Port numbers 1024 through 4999 can be used for global addresses 136.1.1.1 and 136.1.1.2, so you can have a maximum of about 4000 bindings per global address.

# nat create static

## Purpose

Defines one-to-one binding between a local address and global address.

## Format

```
nat create static protocol ip|tcp|udp local-ip <local-ip-addr/address range>  
global-ip <global-ip-addr/address range> [local-port <tcp/udp-local-port>|any]  
[global-port <tcp/udp-global-port>|any]
```

## Mode

Configure.

## Description

The **nat create static** command lets you define fixed address translation from the local network to the global network. The binding of the local to the global address does not expire until this command is negated. If the protocol used is TCP or UDP, you can also specify port address translation (PAT).

## Parameters

|  |  |
|--|--|
| <b>ip tcp udp</b>                                    | Specifies either only IP address translation, IP and TCP port address translation, or IP and UDP port address translation.   |
| <b>local-ip</b> <local-ip-addr/address range>        | Either a single IP address, in the form a.b.c.d, or an address range, in the form 10.10.1.1-10.10.1.50.  |
| <b>global-ip</b> <global-ip-addr/address range>      | Either a single IP address, in the form a.b.c.d, or an address range, in the form 10.10.1.1-10.10.1.50.  |
| <b>local-port</b> <tcp/udp-local-port>  <b>any</b>   | The local TCP or UDP port number. Specify a number between 1-65535, or <b>any</b> for no port translation. This parameter is only valid if you specified <b>tcp</b> or <b>udp</b> .<br><br><b>Note:</b> The number of IP addresses in the local range should be equal to the number of IP addresses in the global range. |
| <b>global-port</b> <tcp/udp-global-port>  <b>any</b> | The global TCP or UDP port number. Specify a number between 1-65535, or <b>any</b> for no port translation. This parameter is only valid if you specified <b>tcp</b> or <b>udp</b> .   |

## Restrictions

None.

## Examples

To configure a static binding of a local and a global IP address:

```
xp(config)# nat create static protocol ip local-ip 10.1.1.13 global-ip 136.1.1.13
```

To configure a static binding of local and global IP address ranges:

```
xp(config)# nat create static protocol ip local-ip 10.1.1.1-10.1.1.50 global-ip 136.1.1.1-136.1.1.50
```

To configure a static binding of local and global IP and UDP port addresses:

```
xp(config)# nat create static local-ip 10.1.1.13 global-ip 136.1.1.13 local-port 18 global-port 36  
protocol udp
```

# nat flush-dynamic-binding

## Purpose

Deletes dynamic NAT bindings.

## Format

```
nat flush-dynamic-binding all| pool-specified [local-acl-pool <local-acl>]  
[global-pool <ip-addr/ip-addr-range/ ip-addr-list>] |  
[type-specified dynamic | overloaded-dynamic] | owner-specified [dns| ftp-control| ftp-data]
```

## Mode

Enable.

## Description

The **nat flush-dynamic-binding** command deletes dynamic address bindings. You can delete the dynamic address bindings for specific address pools or delete all dynamic bindings.

## Parameters

|   |  |   |
|---|--|---|
| <b>all</b>                                    | Deletes all NAT dynamic bindings.                                  |   |
| <b>pool-specified</b>                         | Deletes NAT dynamic bindings based on local and global acl pools.  |   |
|   | <b>local-acl-pool</b> <local-acl>                                  | The ACL that corresponds to the local IP address pool.  |
|   | <b>global-pool</b><br><ip-addr/ip-addr-range>                      | The global address pool, defined in one of the following ways: <ul style="list-style-type: none"><li>• A single IP address in the form a.b.c.d</li><li>• An IP address range in the form 10.10.1.1-10.10.1.50</li><li>• IP address and mask in the form 1.2.0.0/255.255.0.0 or 1.2.3.0/16</li></ul> |
| <b>type-specified</b>                         | Deletes NAT dynamic bindings based on the type of dynamic binding. |   |
| <b>dynamic</b>  <br><b>overloaded-dynamic</b> | <b>dynamic</b>   | Flushes wildcarded dynamic translations   |
|   | <b>overloaded-dynamic</b>  | Flushes IP overloaded dynamic translations  |

|                        |   |   |
|------------------------|---|---|
| <b>owner-specified</b> | Deletes NAT dynamic bindings based on the type of application utilizing the bindings. |   |
|                        | <b>dns</b>  | Deletes NAT dynamic bindings created by DNS (domain name server). |
|                        | <b>ftp-control</b>  | Deletes NAT dynamic bindings created by FTP control connection.   |
|                        | <b>ftp-data</b>   | Deletes NAT dynamic bindings created by FTP data connection.      |

## Restrictions

None.

## Examples

To delete dynamic address bindings for the local address pool that corresponds to the ACL 'lcl' and the global address pool that corresponds to 136.1.1.1-136.1.1.254:

```
xp# nat flush-dynamic-binding pool-specified local-acl-pool lcl global-pool 136.1.1.0/24
```

To delete all dynamic address bindings:

```
xp# nat flush-dynamic-binding all
```

# nat set dns-name-extension-error

## Purpose

Enable or disable the error message associated with DNS name extensions.

## Format

**nat set dns-name-extension-error on|off**

## Mode

Configure.

## Description

The **nat set dns-name-extension-error** command allows you to enable or disable the router's ability to display the DNS name extension error message.

## Parameters

|               |   |
|---------------|---|
| <b>on off</b> | Select <b>on</b> or <b>off</b> to enable or disable this error message. If you negate a command that specifies the option to be off (i.e., <b>nat set dns-name-extension-error off</b> ), the command is enabled automatically. |
|---------------|---|

## Restrictions

None.

## Example

To *enable* the router's ability to display the DNS name extension error message, enter the following:

```
xp(config)# nat set dns-name-extension-error on
```

To *disable* the router's ability to display the DNS name extension error message, enter the following:

```
xp(config)# nat set dns-name-extension-error off
```



# nat set dns-session-timeout

## Purpose

Specifies the timeout for the DNS session.

## Format

**nat set dns-session-timeout** *<num>*

## Mode

Configure.

## Description

The **nat set dns-session-timeout** command sets the timeout for DNS application-specific sessions.

The default DNS session timeout is **30** minutes.

## Parameters

|                    |   |
|--------------------|---|
| <i>&lt;num&gt;</i> | The timeout for the DNS session, in minutes. Specify a value between 3-2880. Default is 30 minutes. |
|--------------------|---|

## Restrictions

None.

## Example

To set the DNS session timeout to 60 minutes:

```
xp(config)# nat set dns-session-timeout 60
```

# nat set dynamic-binding-timeout

## Purpose

Sets the timeout for dynamic NAT binding.

## Format

**nat set dynamic-binding-timeout** *<minutes>*|**disable**

## Mode

Configure.

## Description

Dynamic address bindings time out after a period of non-use. The **nat set dynamic-binding-timeout** command lets you set the timeout for dynamic address bindings. The default is 1440 minutes (24 hours).

## Parameters

|                        |  |
|------------------------|--|
| <i>&lt;minutes&gt;</i> | The number of minutes before an dynamic address binding times out. Specify a value between 3-2880. |
| <b>disable</b>         | Disables timeout of dynamic address bindings.  |

## Restrictions

None.

## Example

To set the timeout for dynamic address bindings to 3 minutes:

```
xp(config)# nat set dynamic-binding-timeout 3
```

To disable timeout of dynamic address bindings:

```
xp(config)# nat set dynamic-binding-timeout disable
```

# nat set ftp-control-port

## Purpose

Specifies the port for FTP control.

## Format

**nat set ftp-control-port** *<port number>*

## Mode

Configure.

## Description

File Transfer Protocol (FTP) packets require special handling with NAT, because IP address information is contained within the FTP packet data. You can use the **nat set ftp-control-port** command to specify the port number that is used for FTP control.

The default port for FTP control is port **21**.

The X-Pedition router's current ACL/NAT implementation does not make provisions for running standard or PASV FTP sessions across a translated interface when only ports 20 (FTP data port) and 21 (FTP control port) are open for communication. Because FTP will use other higher-numbered ports to establish TCP sessions, FTP sessions established across a NAT-translated interface may hang if these other TCP ports are not open for communication. In order to allow FTP to establish a TCP session on higher-numbered ports, the NAT-associated ACL must be set up to allow incoming traffic from any port. When running this configuration, it is suggested that NAT secure-plus is enabled (**nat set secure-plus on**) in order to increase security and prevent private address leaks. For more information, please reference RFC 1579 ("Firewall-Friendly FTP").

## Parameters

|                            |  |
|----------------------------|--|
| <i>&lt;port number&gt;</i> | Specifies the port number used for FTP control. Specify a value between 1 and 65535. |
|----------------------------|--|

## Restrictions

None.

## Example

To set the FTP control port to 100:

```
xp(config)# nat set ftp-control-port 100
```

# nat set ftp-session-timeout

## Purpose

Specifies the timeout for the FTP session.

## Format

**nat set ftp-session-timeout** *<minutes>*

## Mode

Configure.

## Description

The **nat set ftp-session-timeout** command sets the timeout for the FTP session.

The default FTP session timeout is **30** minutes.

## Parameters

---

|                        |  |
|------------------------|--|
| <i>&lt;minutes&gt;</i> | The timeout for the FTP session. Specify a value between 3-2880. |
|------------------------|--|

---

## Restrictions

None.

## Example

To set the FTP session timeout to 60 minutes:

```
xp(config)# nat set ftp-session-timeout 60
```

# nat set interface

## Purpose

Defines an interface as inside or outside for NAT address translation.

## Format

**nat set interface** *<name>* **inside|outside**

## Mode

Configure.

## Description

The **nat set interface** command allows you to define an interface as inside or outside. When NAT is enabled using the **nat create static** or **nat create dynamic** command, address translation is applied only to packets that arrive on these interfaces.

## Parameters

|                       |  |
|-----------------------|--|
| <i>&lt;name&gt;</i>   | Name of the interface to which address translation will apply.<br><br><b>Note:</b> The X-Pedition router displays interface names up to 32 characters in length. |
| <b>inside outside</b> | Specifies the interface(s) as inside or outside.   |

## Restrictions

None.

## Examples

To create the interface '10-net' and define it as an inside interface for NAT:

```
xp(config)# interface create ip 10-net address-netmask 10.1.1.1/24 port et.2.1
xp(config)# nat set interface 10-net inside
```

To create the interface '192-net' and define it as an outside interface for NAT:

```
xp(config)# interface create ip 192-net address-netmask 192.50.20.1/24 port et.2.2  
xp(config)# nat set interface 192-net outside
```

## nat set secure-plus

### Purpose

Block IP addresses defined as *inside* addresses from ever appearing on an *outside* interface.

### Format

**nat set secure-plus on|off**

### Mode

Configure.

### Description

The **nat set secure-plus** command forces all flows from the *inside* network or the *outside* network to go through network address translation. Packets that would otherwise bypass NAT and transmit untranslated are dropped.

### Parameters

|               |   |
|---------------|---|
| <b>on off</b> | Specify on to enable secure-plus feature. Specify off to disable secure-plus feature. |
|---------------|---|

### Restrictions

None.



# nat show

## Purpose

Displays NAT information.

## Format

**nat show** [**translations** <type>] [**timeouts**] [**statistics**]

## Mode

Enable.

## Description

The **nat show** command allows you to display NAT address translations, timeouts, and statistics.

## Parameters

|   |   |
|---|---|
| <b>translations</b> <type>                    | Displays NAT translations. Specify one of the following keywords:   |
| <b>all</b>                                    | Shows all translations.   |
| <b>type static dynamic overloaded-dynamic</b> | Shows static, dynamic, or IP overloaded dynamic translations.   |
| <b>owner dns ftp-control ftp-data</b>         | Shows dynamic translation created by dns, overloaded dynamic ftp control connection translations, or overloaded dynamic ftp data connection translations. |
| <b>local-filter-in</b><br><local-ip-addr>     | Shows translations of the specified local IP address. The IP address must be in the form a.b.c.d.   |
| <b>global-filter-in</b><br><global-ip-addr>   | Shows translations of the specified global IP address. The IP address must be in the form a.b.c.d.  |
| <b>timeouts</b>                               | Displays the current set of timeouts.   |
| <b>statistics</b>                             | Displays NAT statistics.  |
| <b>verbose</b>                                | Displays NAT translations in greater detail.  |

## Restrictions

None.

## Examples

To display active NAT translations:

| xp# nat show translations all |                  |                   |           |              |
|-------------------------------|------------------|-------------------|-----------|--------------|
| Proto                         | Local/Inside     | Global/Outside IP | Type      | No. of flows |
| -----                         | -----            | -----             | -----     | -----        |
| TCP                           | 15.15.15.15:1896 | 100.1.1.1:1026    | Dyn. ovr. | 2            |
| TCP                           | 15.15.15.15:1897 | 100.1.1.1:1028    | Dyn. ovr. | 0            |
| TCP                           | 15.15.15.15:1894 | 100.1.1.1:1024    | Dyn. ovr. | 2            |
| TCP                           | 15.15.15.15:1895 | 100.1.1.1:1025    | Dyn. ovr. | 2            |
| TCP                           | 15.15.15.15:1892 | 100.1.1.1:1027    | Dyn. ovr. | 0            |
| IP                            | 10.10.10.10:*    | 200.1.1.1:*       | Dynamic   | 20           |
| IP                            | 4.4.4.4:*        | 202.1.1.1:*       | Static    | 789          |

If there are many active NAT translations, you can filter the display by specifying **local-filter-in**, **global-filter-in**, or **type** parameters for the **nat show translations** command.

To display NAT timeouts:

| xp# nat show timeouts |           |           |            |
|-----------------------|-----------|-----------|------------|
| All values in minutes |           |           |            |
| Flow                  | FTP Sess. | DNS Sess. | Dyn. Sess. |
| -----                 | -----     | -----     | -----      |
| 2                     | 30        | 30        | 1440       |

To display NAT statistics:

|  |              |              |            |            |                      |
|--|--------------|--------------|------------|------------|----------------------|
| NAT current status                           |              |              |            |            |                      |
| -----  |              |              |            |            |                      |
| active                                       |              |              |            |            |                      |
|  |              |              |            |            |                      |
| NAT secure-plus status                       |              |              |            |            |                      |
| -----  |              |              |            |            |                      |
| inactive                                     |              |              |            |            |                      |
|  |              |              |            |            |                      |
| Interface Information                        |              |              |            |            |                      |
| -----  |              |              |            |            |                      |
| No. of Interfaces: 1                         |              |              |            |            |                      |
| Interface: 20net, configured as nat: outside |              |              |            |            |                      |
|  |              |              |            |            |                      |
| STATIC Binding Information                   |              |              |            |            |                      |
| -----  |              |              |            |            |                      |
| No. of Static Bindings: 1                    |              |              |            |            |                      |
|  |              |              |            |            |                      |
| DYNAMIC Binding Information                  |              |              |            |            |                      |
| -----  |              |              |            |            |                      |
| No. of Dynamic Bindings: None                |              |              |            |            |                      |
|  |              |              |            |            |                      |
| Local Acl pool                               | Max. globals | Globals used | Max. ports | Ports Used | Out of globals/ports |
| -----  |              |              |            |            |                      |
| local  | 1            | 0            | 3975       | 0          | 0                    |



# Chapter 42

## ndisc Commands

The **ndisc** commands allow you to configure the Neighbor Discovery protocol for IPv6 and the IPv6 Stateless Address Autoconfiguration protocol on the X-Pedition router.

Neighbor Discovery uses ICMPv6 messages to discover the link-layer addresses of neighbors on the same link, to detect changed link-layer addresses, to discover routers, and to keep track of the reachability of neighbors. The Neighbor Discovery protocol for IPv6 is described in RFC 2461.

IPv6 Stateless Autoconfiguration specifies how IPv6 hosts can generate their own IPv6 addresses using network parameters advertised by an IPv6 router as well as their own information such as their MAC address. The IPv6 Stateless Address Autoconfiguration protocol is described in RFC 2462. The X-Pedition software implements the IPv6 Stateless Address Auto-configuration protocol from the perspective of a router (as opposed to a host) only.

### Command Summary

[Table 37](#) lists the **ndisc** commands. The sections following the table describe the command syntax.

**Table 37. ndisc commands**

|   |
|---|
| <b>ndisc set interface</b> <interfacename-or-ipv6addr> <b>all</b> [ <b>suppress-ra</b> ] [ <b>max-ra-interval</b> <num>] [ <b>min-ra-interval</b> <num>] [ <b>managed-config-flag</b> ] [ <b>other-config-flag</b> ] [ <b>ra-lifetime</b> <num>] [ <b>reachable-time</b> <num>] [ <b>ns-interval</b> <num>] |
| <b>ndisc show interface</b> <interfacename-or-ipv6addr>   <b>all</b>  |
| <b>ndisc add prefix</b> <ipv6-prefix>/<length> <b>interface</b> <interfacename-or-ipv6addr> [ <b>valid-lifetime</b> <num>] <date-time>   <b>infinite</b> ] [ <b>preferred-lifetime</b> <num>] <date-time>   <b>infinite</b> ] [ <b>no-advertise</b> ] [ <b>off-link</b> ] [ <b>no-autoconfig</b> ]          |
| <b>ndisc show prefix</b> {<ipv6-prefix>/<length>   <b>all</b> } } [ <b>interface</b> <interfacename-or-ipv6addr>]   |
| <b>ndisc add neighbor</b> <host> <b>mac-addr</b> <MAC-addr>   |

**Table 37. ndisc commands (Continued)**

|  |
|--|
| <b>ndisc clear neighbor</b> <i>&lt;host&gt;</i>   <b>all</b> |
| <b>ndisc show neighbor</b> <i>&lt;host&gt;</i>   <b>all</b>  |
| <b>ndisc set dad-attempts</b> <i>&lt;num&gt;</i>             |
| <b>ndisc show dad-attempts</b>                               |

# ndisc set interface

## Purpose

Configure IPv6 Neighbor Discovery parameters on a single interface or all interfaces.

## Format

```
ndisc set interface <interfacename-or-ipv6addr>|all [suppress-ra]  
[max-ra-interval <num>] [min-ra-interval <num>] [managed-config-flag] [other-config-flag]  
[ra-lifetime <num>] [reachable-time <num>] [ns-interval <num>]
```

## Mode

Configure.

## Description

This command lets you configure the following parameters associated with the IPv6 Neighbor Discovery protocol on a single interface or all interfaces of the X-Pedition router.

- Whether or not IPv6 Router Advertisements are transmitted on an interface
- Minimum and maximum lengths for the interval between IPv6 Router Advertisements
- The “Managed address configuration” flag in IPv6 Router Advertisements
- The “Other stateful configuration” flag in IPv6 Router Advertisements
- The “Router Lifetime” value in IPv6 Router Advertisements
- The “Reachable Time” value in IPv6 Router Advertisements
- The “Retrans Timer” value in IPv6 Router Advertisements

Refer to the parameter descriptions below for more information about these parameters.

When a parameter is left unspecified, the default value associated with the parameter is used. The **no** form of the command is used to delete the configuration previously specified by a matching command that did not include the **no** keyword.

## Parameters

|   |   |
|---|---|
| <i>&lt;interfacename-or-IPv6addr&gt;</i>   <b>all</b> | The interface name or IPv6 address of the interface for which you are setting Neighbor Discovery parameters.          |
|   | Use the <b>all</b> keyword if you want to set Neighbor Discovery parameters for all IPv6 interfaces on the X-Pedition |

|                                 |   |
|---------------------------------|---|
| <b>suppress-ra</b>              | <p>When this option is specified, no IPv6 Router Advertisements are transmitted on the specified interface(s).</p> <p>By default, IPv6 Router Advertisements are transmitted on all interfaces.</p>   |
| <b>max-ra-interval</b><br><num> | <p>Specifies, in seconds, the maximum time allowed between sending unsolicited multicast Router Advertisements from the specified interface(s).</p> <p>The value of &lt;num&gt; must be no less than 4 seconds and no greater than 1800 seconds. The default value is 3 times the value of the <b>min-ra-interval</b> parameter, or 600 seconds if <b>min-ra-interval</b> is not specified.</p>   |
| <b>min-ra-interval</b><br><num> | <p>Specifies, in seconds, the minimum time allowed between sending unsolicited multicast Router Advertisements from the specified interface(s).</p> <p>The value of &lt;num&gt; must be no less than 3 seconds and no greater than 0.75 times the value of the <b>max-ra-interval</b> parameter. The default value is 0.33 times the value of the <b>max-ra-interval</b> parameter, or 200 seconds if <b>max-ra-interval</b> is not specified.</p>  |
| <b>managed-config-flag</b>      | <p>When this option is specified, the “Managed address configuration” bit is set in IPv6 Router Advertisements transmitted on the specified interface(s).</p> <p>When this bit is set, receiving hosts use the administered (stateful) protocol for address configuration, in addition to any addresses autoconfigured using stateless address autoconfiguration.</p> <p>When this bit is not set (that is, cleared), receiving hosts use stateless autoconfiguration.</p> <p>By default, the “Managed address configuration” bit is cleared in IPv6 Router Advertisements.</p> |
| <b>other-config-flag</b>        | <p>When this option is specified, the “Other stateful configuration” bit is set in IPv6 Router Advertisements transmitted on the specified interface(s).</p> <p>When this bit is set, receiving hosts use the administered (stateful) protocol for configuration of other, non-address-related information. When this bit is not set (that is, cleared), receiving hosts use stateless autoconfiguration for other information.</p> <p>By default, the “Other address configuration” bit is cleared in IPv6 Router Advertisements.</p>  |



---

|                             |   |
|-----------------------------|---|
| <b>ra-lifetime</b> <num>    | <p>Specifies the “Router Lifetime” value in IPv6 Router Advertisements transmitted on the specified interface(s).</p> <p>A value of 0 indicates that the router is not a default router. A non-zero value indicates that this router should be considered a default router on the specified interface(s).</p> <p>The value indicates how long the router is useful as a default router on the specified interface(s), and should not be less than the value of the <b>max-ra-interval</b> parameter.</p> <p>The value is specified in seconds in the range 0 to 65535. The maximum value corresponds to 18.2 hours. The default value of this parameter is 1800 seconds.</p>  |
| <b>reachable-time</b> <num> | <p>Specifies the “Reachable Time” value in IPv6 Router Advertisements transmitted on the specified interface(s). This 32-bit value is the length of time, in milliseconds, that a node assumes a neighbor remains reachable after receiving some reachability confirmation from the neighbor.</p> <p>This value is used by the Neighbor Unreachability Detection algorithm. A value of 0 means the “Reachable Time” is unspecified (by this router).</p> <p>The value of this parameter is also used by this router to detect unreachability of its own neighbors. A smaller value allows neighbor unreachability to be detected more quickly, but consumes more network resources.</p> <p>By default, a value of 0 milliseconds is placed in Router Advertisements, and a value of 30000 milliseconds is used for neighbor unreachability detection by this router itself.</p> |
| <b>ns-interval</b> <num>    | <p>Specifies the “Retrans Timer” value in IPv6 Router Advertisements transmitted on the specified interface(s). This 32-bit value is the length of time, in milliseconds, between retransmitted Neighbor Solicitation messages.</p> <p>A default value of 0 (unspecified) is advertised in Router Advertisements. A default value of 1000 milliseconds is used by this router for its own neighbor discovery activity.</p>  |

---

## Restrictions

None.

## Example

The following example changes the interval for unsolicited multicast Router Advertisements by setting the minimum interval to 4 minutes (240 seconds) for all IPv6 interfaces on the X-Pedition router.

```
xp(config)# ndisc set interface all min-ra-interval 240
```

The following example configures the existing IPv6 interface named “IPv6\_1” to advertise itself as not being available as a default router. The example also sets the “Reachable Time” value sent in Router Advertisements to 10,000 milliseconds. This parameter is used by the Neighbor Unreachability Detection algorithm by the on-link hosts receiving advertisements from this router and also by the router itself.

```
xp(config)# ndisc set interface IPv6_1 ra-lifetime 0 reachable-time 10000
```

# ndisc show interface

## Purpose

Display configured IPv6 Neighbor Discovery protocol information for a single interface or all interfaces.

## Format

**ndisc show interface** < *interfacename-or-ipv6addr* >| **all**

## Mode

Enable.

## Description

This command lets you display the IPv6 Neighbor Discovery configuration information associated with IPv6 interfaces. The configuration information displayed consists of:

- Whether or not IPv6 Router Advertisements are transmitted on an interface
- Minimum and maximum lengths of interval between IPv6 Router Advertisements
- The state of the “Managed address configuration” flag in IPv6 Router Advertisements
- The state of the “Other stateful configuration” flag in IPv6 Router Advertisements
- The “Router Lifetime” value in IPv6 Router Advertisements
- The “Reachable Time” value in IPv6 Router Advertisements
- The “Retrans Timer” value in IPv6 Router Advertisements

Refer to the parameter descriptions for the **ndisc set interface** command for more information about the information displayed.

## Parameters

---

|                                      |   |
|--------------------------------------|---|
| < <i>interfacename-or-IPv6addr</i> > | The interface name or IPv6 address of the interface for which you are displaying Neighbor Discovery parameters.           |
| <b>all</b>                           | Use the <b>all</b> keyword if you want to display Neighbor Discovery parameters for all IPv6 interfaces on the X-Pedition |

---

## Restrictions

None.

## Example

The following example displays information about all prefixes configured on the X-Pedition router:

```
xp# ndisc show interface all
IPv6 Neighbor Discovery interface configuration:
  Interface default
    IPv6 Advertisements are not suppressed
    min-ra-interval 200
    max-ra-interval 600
    managed-config-flag not set
    other-config-flag not set
    ra-lifetime 1800
    reachable-time 0
    ns-interval 0
  Interface 0023:0000:0000:0000:02e0:63ff:fe13:2043(intf3)
    IPv6 Advertisements are not suppressed
    min-ra-interval 200
    max-ra-interval 600
    managed-config-flag not set
    other-config-flag not set
    ra-lifetime 1800
    reachable-time 0
    ns-interval 0
  Interface 0020:0000:0000:0000:02e0:63ff:fe13:2043(intf1)
    IPv6 Advertisements are not suppressed
    min-ra-interval 200
    max-ra-interval 600
    managed-config-flag not set
    other-config-flag not set
    ra-lifetime 1800
    reachable-time 0
    ns-interval 0
```

# ndisc add prefix

## Purpose

Configure prefixes to be included in IPv6 Router Advertisements.

## Format

```
ndisc add prefix <ipv6-prefix>/<length> interface <interfacename-or-ipv6addr>  
[valid-lifetime <num>| <date-time> | infinite] [preferred-lifetime <num>| <date-time> | infinite]  
[no-advertise] [off-link] [no-autoconfig]
```

## Mode

Configure.

## Description

The **ndisc add prefix** command lets you configure prefixes to be included in IPv6 Router Advertisements transmitted on the specified interface. By default, the prefixes configured as addresses on an interface using the **interface create ipv6** or **interface add ipv6** commands are advertised in IPv6 Router Advertisements. If you configure prefixes for advertisement using the **ndisc add prefix** command, then only these prefixes are advertised.

The following pieces of information associated with a prefix may be configured:

- The value of the prefix
- The interface on which the prefix is advertised
- The “Valid Lifetime” value for the prefix in IPv6 Router Advertisements
- The “Preferred Lifetime” value for the prefix in IPv6 Router Advertisements
- Whether or not the prefix is included in IPv6 Router Advertisements
- The status of the “on-link” flag for the prefix in IPv6 Router Advertisements
- The status of the “autonomous address-configuration” flag for the prefix in IPv6 Router Advertisements

Refer to the parameter descriptions below for more information about these parameters.

When a parameter is left unspecified, the default value associated with the parameter is used. The **no** form of the command is used to delete a prefix previously configured by a matching command that did not include the **no** keyword.

## Parameters

|   |  |
|---|--|
| <code>&lt;ipv6-prefix&gt;/&lt;length&gt;</code>   | <p>An IPv6 prefix to be advertised on the specified interface, entered in RFC 2373-compliant IPv6 address/prefix length (CIDR) notation.</p> <p>The value of the prefix <code>&lt;length&gt;</code> can be in the range 0 to 128.</p>  |
| <b>interface</b><br><code>&lt;interfacename-or-ipv6addr&gt;</code>                                | <p>The interface name or IPv6 address of the interface on which the specified prefix is to be advertised.</p>  |
| <b>valid-lifetime</b> <code>&lt;num&gt;</code>   <code>&lt;date-time&gt;</code>   <b>infinite</b> | <p>Specifies the “Valid Lifetime” value included for the prefix in IPv6 Router Advertisements. This value defines the period of validity of the prefix for the purpose of on-link determination. It also defines the period of validity of any host address derived from the prefix via stateless autoconfiguration.</p> <p>This value may be specified as one of the following:</p> <ul style="list-style-type: none"><li>• A 32-bit unsigned number (<code>&lt;num&gt;</code>) that represents the time until expiration in seconds</li><li>• As an expiration date, where (<code>&lt;date-time&gt;</code>) is entered as a quoted string in the format:<br/><br/>‘[YYYY] DD MM HH:MM’ (year is optional). For example:<br/>‘2004 23 12 13:13’ or ‘23 12 13:13’</li><li>• As being indefinitely valid (<b>infinite</b>)</li></ul> <p>This parameter defaults to a <code>&lt;num&gt;</code> value of 2592000 seconds (30 days).</p> |

|   |   |
|---|---|
| <b>preferred-lifetime</b><br><code>&lt;num&gt;  &lt;date-time&gt;  </code><br><b>infinite</b> | <p>Specifies the “Preferred Lifetime” value included for the prefix in IPv6 Router Advertisements. This value defines the period of time that an address derived from the prefix via stateless autoconfiguration remains in a preferred state. An address goes from the preferred state to the deprecated state when its preferred lifetime expires. The preferred lifetime of an address always expires before or at the same time as its valid life time.</p> <p>The value of this parameter may be specified as one of the following:</p> <ul style="list-style-type: none"> <li>• A 32-bit unsigned number (<code>&lt;num&gt;</code>) that represents the time until expiration of the preferred state in seconds</li> <li>• As an expiration date, where (<code>&lt;date-time&gt;</code>) is entered as a quoted string in the format:<br/> ‘[YYYY] DD MM HH:MM’ (year is optional). For example:<br/> ‘2004 23 12 13:13’ or ‘23 12 13:13’</li> <li>• As being indefinitely preferred (<b>infinite</b>).</li> </ul> <p>This parameter defaults to a <code>&lt;num&gt;</code> value of 604800 seconds (7 days).</p> |
| <b>no-advertise</b>   | <p>This flag specifies that this prefix is not advertised in IPv6 Router Advertisements. By default, prefixes are advertised.</p>   |
| <b>off-link</b>   | <p>Determines the value of the “on-link” flag (L-bit) for the prefix in IPv6 Router Advertisements. When this option is specified, the “on-link” flag <i>is cleared</i>. By default, the “on-link” flag <i>is set</i>.</p> <p>When set, the “on-link” flag indicates that the addresses implied by the prefix are available on the specified interface. When this flag is cleared, a receiving host may not assume that the addresses implied by the prefix are available on the receiving interface.</p>   |
| <b>no-autoconfig</b>  | <p>Determines the value of the “autonomous address-configuration” flag (A-bit) for the prefix in IPv6 Router Advertisements. When this option is specified, the flag <i>is cleared</i>. By default, the “autonomous address-configuration” flag <i>is set</i>.</p> <p>When set, the “autonomous address-configuration” flag indicates that this prefix can be used by a receiving host for stateless address autoconfiguration. When cleared, a host may not use this prefix for stateless address autoconfiguration</p>  |

## Restrictions

None

## Example

The following example adds two prefixes to two different IPv6 interfaces, setting the valid lifetime to 20 days (1828000 seconds), and then displays the configured prefixes.:

```
xp(config)# ndisc add prefix 33::/64 interface intf3 valid-lifetime 1828000
xp(config)# ndisc add prefix 44::/64 interface intf1 valid-lifetime 1828000
xp(config)# Exit
```

```
xp# ndisc show prefix all
```

```
IPv6 Neighbor Discovery prefix configuration:
```

```
Prefix 0044:0000:0000:0000:0000:0000:0000:0000/64
```

```
Interface 0020:0000:0000:0000:02e0:63ff:fe13:2043(intf1)
```

```
valid-lifetime 1828000
```

```
preferred-lifetime 604800
```

```
no-advertise not set
```

```
off-link not set
```

```
no-autoconfig not set
```

```
Prefix 0033:0000:0000:0000:0000:0000:0000:0000/64
```

```
Interface 0023:0000:0000:0000:02e0:63ff:fe13:2043(intf3)
```

```
valid-lifetime 1828000
```

```
preferred-lifetime 604800
```

```
no-advertise not set
```

```
off-link not set
```

```
no-autoconfig not set
```



# ndisc show prefix

## Purpose

Displays information about prefixes that are configured for inclusion in IPv6 Router Advertisements.

## Format

**ndisc show prefix** {<ipv6-prefix>/<length> | **all**} [**interface** <interfacename-or-ipv6addr>]

## Mode

Enable.

## Description

The **ndisc show prefix** command lets you display information about prefixes previously configured with the **ndisc add prefix** command for inclusion in IPv6 Router Advertisements transmitted on a specific interface or on all IPv6 interfaces. By default, the prefixes configured as addresses on an interface using the **interface create ipv6** or **interface add ipv6** commands are advertised in IPv6 Router Advertisements. However, these prefixes are not listed in the output of this command. Only prefixes configured using the **ndisc add prefix** command are listed.

The following information associated with a prefix is displayed by this command:

- The value of the IPv6 prefix and its length.
- The “Valid Lifetime” value for the prefix in IPv6 Router Advertisements.
- The “Preferred Lifetime” value for the prefix in IPv6 Router Advertisements
- Whether or not the prefix is included in IPv6 Router Advertisements
- The status of the “on-link” flag for the prefix in IPv6 Router Advertisements
- The status of the “autonomous address-configuration” flag for the prefix in IPv6 Router Advertisements.

For more detailed descriptions of the information displayed by this command, see the parameter descriptions of the **ndisc add prefix** command.

## Parameters

|  |   |
|--|---|
| <code>&lt;ipv6-prefix&gt;/&lt;length&gt;   all</code>    | <p>The IPv6 prefix for which information is to be displayed. The value is specified in RFC2373-compliant IPv6 address/prefix length (CIDR) notation. The value of prefix <code>&lt;length&gt;</code> is in the range 0 to 128.</p> <p>If the <b>all</b> keyword is entered, information is displayed for all prefixes configured on the X-Pedition router, if no interface is specified, or for all the prefixes associated with a specified interface.</p> <p>If you enter a specific prefix value with <code>&lt;ipv6-prefix&gt;/&lt;length&gt;</code>, you cannot include the <b>interface</b> option, since a prefix can be associated with only one interface.</p> |
| <code>interface &lt;interfacename-or-ipv6addr&gt;</code> | <p>The interface name or IPv6 address of the interface for which prefix information is to be displayed.</p> <p>This option may not be specified if the <code>&lt;ipv6-prefix&gt;/&lt;length&gt;</code> value is specified.</p>  |

## Restrictions

None.

## Example

The following example displays information for the prefix 55:44:33:22::/64, which was assigned to the IPv6 interface named IPv6\_2:

```
xp# ndisc show prefix 55:44:33:22::/64

Prefix 0055:0044:0033:0022:0000:0000:0000:0000/64
  Interface 00aa:00bb:00cc:00dd:00ee:0000:0000:0000(IPv6_2)
  valid-lifetime 2592000
  preferred-lifetime 40000
  no-advertise not set
  off-link not set
  no-autoconfig not set
```

The following example displays information about all the prefixes configured on the IPv6 interface named intf3:

```
xp# ndisc show prefix all interface intf3
IPv6 Neighbor Discovery prefix configuration:
  Prefix 0075:0000:0000:0000:0000:0000:0000/64
    Interface 0023:0000:0000:0000:02e0:63ff:fe13:2043(intf3)
    valid-lifetime 2592000
    preferred-lifetime 604800
    no-advertise not set
    off-link not set
    no-autoconfig not set
  Prefix 0033:0000:0000:0000:0000:0000:0000/64
    Interface 0023:0000:0000:0000:02e0:63ff:fe13:2043(intf3)
    valid-lifetime 1828000
    preferred-lifetime 604800
    no-advertise not set
    off-link not set
    no-autoconfig not set
```

# ndisc add neighbor

## Purpose

Configure static entries in the IPv6 Neighbor Discovery Cache.

## Format

**ndisc add neighbor** <host> **mac-addr** <MAC-addr>

## Mode

Configure.

## Description

The IPv6 Neighbor Cache contains a list of neighbors to which traffic has recently been sent. The **ndisc add neighbor** command allows you to configure static entries in the IPv6 Neighbor Cache. The IPv6 address of the specified host is associated with the specified MAC address in the cache. This command is similar to the IPv4 **arp add** command. If a dynamic entry for the specified host (learned through the IPv6 Neighbor Discovery process) already exists in the Neighbor Cache, the entry is converted to a static entry. Static entries in the cache are not modified by the Neighbor Discovery process. Neighbor unreachability detection is not performed on static entries in the Neighbor Discovery Cache.

Use the **no** form of this command to delete a static entry that was previously configured using a matching command that did not include the **no** prefix. The **ndisc clear neighbor** command clears dynamic entries only, and cannot be used to delete static entries in the Neighbor Cache.

Use the **ndisc show neighbor** command to view both static and dynamic entries in the IPv6 Neighbor Cache.

## Parameters

|                            |   |
|----------------------------|---|
| <host>                     | Hostname or IPv6 address of neighbor being added to Neighbor Cache. |
| <b>mac-addr</b> <MAC-addr> | MAC address of the host.  |

## Restrictions

None.

## Example

The following example adds a permanent entry to the neighbor cache, then displays the contents of the cache with the new entry. The new entry is marked with the S flag, to denote a static entry.

```
xp(config)# ndisc add neighbor 20::2 mac-addr 00:e0:63:13:20:43

xp# ndisc show neighbor all
Neighbor          Linklayer Address  Netif    Expire    S    Flags
20::1             00:e0:63:13:20:03  intf1    permanent R
20::2             00:e0:63:13:20:43  intf1    permanent R    S
22::1             00:e0:63:13:20:03  intf3    permanent R
fe80::2e0:63ff:fe13:2003%intf1 00:e0:63:13:20:03  intf1    permanent R
fe80::2e0:63ff:fe13:2003%intf3 00:e0:63:13:20:03  intf3    permanent R
5 entries found in neighbor cache
```

# ndisc clear neighbor

## Purpose

Purge dynamic entries from the IPv6 Neighbor Discovery Cache.

## Format

**ndisc clear neighbor** *<host>* | **all**

## Mode

Enable.

## Description

The **ndisc clear neighbor** command lets you delete one or all of the dynamic entries currently in the IPv6 Neighbor Discovery Cache. Static entries are not affected by this command. To delete a static entry use the **no ndisc add neighbor** command.

Use the **ndisc show neighbor** command to view both static and dynamic entries in the IPv6 Neighbor Discovery Cache.

## Parameter

---

|                                  |   |
|----------------------------------|---|
| <i>&lt;host&gt;</i>   <b>all</b> | Hostname or IPv6 address of dynamic neighbor cache entry to be deleted.                   |
|                                  | If the keyword <b>all</b> is specified, all the dynamic entries in the cache are deleted. |

---

## Restrictions

None.

## Example

The following example first shows the neighbor cache, with one dynamic entry. Then the **ndisc clear neighbor** command is invoked to remove dynamic entries, and the **ndisc show neighbor** command shows that the dynamic entry was deleted.

```

xp# ndisc show neighbor all
Neighbor                Linklayer Address  Netif    Expire    S      Flags
20::1                   00:e0:63:13:20:03 intf1     permanent R
20::2                   00:e0:63:13:20:43 intf1     28s      R      R
22::1                   00:e0:63:13:20:03 intf3     permanent R
fe80::2e0:63ff:fe13:2003%intf1 00:e0:63:13:20:03 intf1     permanent R
fe80::2e0:63ff:fe13:2003%intf3 00:e0:63:13:20:03 intf3     permanent R
5 entries found in neighbor cache

xp# ndisc clear neighbor all

xp# ndisc show neighbor all
Neighbor                Linklayer Address  Netif    Expire    S      Flags
20::1                   00:e0:63:13:20:03 intf1     permanent R
22::1                   00:e0:63:13:20:03 intf3     permanent R
fe80::2e0:63ff:fe13:2003%intf1 00:e0:63:13:20:03 intf1     permanent R
fe80::2e0:63ff:fe13:2003%intf3 00:e0:63:13:20:03 intf3     permanent R
4 entries found in neighbor cache

```

# ndisc show neighbor

## Purpose

Display Neighbor Discovery Cache information.

## Format

**ndisc show neighbor** *<host>* | **all**

## Mode

Enable.

## Description

The **ndisc show neighbor** command displays IPv6 Neighbor Discovery Cache information for a specific neighbor or for all known neighbors.

Some of the important fields in the Neighbor Discovery Cache that are displayed include:

- IPv6 address of neighbor
- MAC (link layer) address of neighbor. A — is displayed if MAC address is not known.
- State of neighbor cache entry
- The time until expiration of the current state.

## Parameter

|                                  |   |
|----------------------------------|---|
| <i>&lt;host&gt;</i>   <b>all</b> | Hostname or IPv6 address of dynamic neighbor cache entry to be displayed. If the keyword <b>all</b> is specified, all the entries in the cache are displayed. |
|----------------------------------|---|

## Restrictions

None.



## Example

The following example illustrates the contents of the Neighbor Cache showing the local interfaces and two neighbors. One neighbor entry is in Reachable state while the other is in Stale state. See the descriptions of the output fields below.

| xp# ndisc show neighbor all       |                   |       |           |   |       |
|-----------------------------------|-------------------|-------|-----------|---|-------|
| Neighbor                          | Linklayer Address | Netif | Expire    | S | Flags |
| 23::2e0:63ff:fe13:2003            | 00:e063:13:20:03  | intf3 | 28s       | R | R     |
| 20::2e0:63ff:fe13:2003            | 00:e0:63:13:20:03 | intf1 | 23h59m18s | S | R     |
| 20::2e0:63ff:fe13:2043            | 00:e0:63:13:20:43 | intf1 | permanent | R |       |
| 23::2e0:63ff:fe13:2043            | 00:e0:63:13:20:43 | intf3 | permanent | R |       |
| fe80::2e0:63ff:fe13:2043%intf1    | 00:e0:63:13:20:43 | intf1 | permanent | R |       |
| fe80::2e0:63ff:fe13:2043%intf3    | 00:e0:63:13:20:43 | intf3 | permanent | R |       |
| 6 entries found in neighbor cache |                   |       |           |   |       |

### Field Definitions

| Field             | Definition   |
|-------------------|--|
| Linklayer Address | MAC address of interface   |
| Netif             | Interface name   |
| Expire            | Indicates the time until expiration of the current state. See the description of States below for more information.<br><br>For static entries and local interfaces, this column displays a value of “permanent.” If the state is in transition, “nextState” will be displayed. |

|           |   |
|-----------|---|
| S (State) | <p>Indicates the state of the entry. The value can be one of the following:</p> <ul style="list-style-type: none"> <li>• N — No state.</li> <li>• I — Incomplete. Address resolution being performed but not completed yet.</li> <li>• R — Reachable. Positive confirmation was received within the last ReachableTime milliseconds that the forward path to neighbor was functioning properly.</li> <li>• S — Stale. More than ReachableTime milliseconds have elapsed since the last positive confirmation was received that forward path was functioning properly.</li> <li>• D — Delay. More than ReachableTime milliseconds have elapsed since the last positive confirmation was received that forward path was functioning properly and a packet was sent within the last DELAY_FIRST_PROBE_TIME seconds. If no reachability confirmation is received within DELAY_FIRST_PROBE_TIME seconds of entering the Delay state, send a Neighbor Solicitation and change the state to Probe.</li> <li>• P — Probe. A reachability confirmation is actively sought by retransmitting Neighbor Solicitations every RetransTimer milliseconds until a reachability confirmation is received.</li> <li>• ? — other</li> </ul> <p><b>Note:</b> When a neighbor is an active destination, its entry in the cache will cycle through the Neighbor Unreachability state machine (Reachable &gt; Delay &gt; Probe &gt; Reachable) approximately every 35 seconds.</p> <p>When a neighbor is not an active destination, its entry will transition into the Stale state approximately 30 seconds after becoming Reachable, and will stay in Stale state until a packet is sent to the neighbor or until the entry is garbage collected in 24 hours.</p> |
| Flags     | <p>The Flags column displays one of the following:</p> <ul style="list-style-type: none"> <li>• S — Static (configured) entry</li> <li>• R — Neighbor is a router</li> <li>• p — Proxy. A router may proxy for other nodes, by indicating via Neighbor Advertisements that it is willing to accept packets not explicitly addressed to itself.</li> </ul> <p>A number may appear after the flags field. This number represents the number of neighbor solicitation probes sent to the neighbor when in the Probe state.</p>   |

# ndisc set dad-attempts

## Purpose

Configure the number of consecutive IPv6 neighbor solicitation messages sent by an interface when duplicate address detection (DAD) is performed on a unicast IPv6 interface address assigned to that interface.

## Format

**ndisc set dad-attempts** *<num>*

## Mode

Configure.

## Description

This command lets you configure the “dad-attempts” parameter associated with the IPv6 Neighbor Discovery protocol for all interfaces on the box. The *num* parameter specifies the number of consecutive neighbor solicitation messages that are sent on an interface when duplicate address detection is performed on a unicast IPv6 address assigned to that interface.

The **no** form of the command is used to delete the configuration previously specified by a matching command that did not include the **no** keyword.

## Parameters

---

|                    |  |
|--------------------|--|
| <i>&lt;num&gt;</i> | Specifies the number of consecutive Neighbor Solicitation messages transmitted on an interface, when duplicate address detection (DAD) is performed on a unicast IPv6 address assigned to an interface.<br><br>This value may be specified in the range 0 to 600. A value of 0 disables duplicate address detection on all IPv6 interfaces. A value of 1, which is the default, specifies a single transmission with no follow-up transmissions. |
|--------------------|--|

---

## Restrictions

None

## Example

The following example sets the DAD attempts parameter to 4 with the **ndisc set dad-attempts** command, and then shows the changed value with the **ndisc show dad-attempts** command.

```
xp(config)# ndisc set dad-attempts 4
xp(config)# Exit
Do you want to make the changes Active [yes]? yes
xp# ndisc show dad-attempts
IPv6 Duplicate Address Detection (IPV6CTL_DAD_COUNT): 4 attempts
```

# ndisc show dad-attempts

## Purpose

Display the value of the IPv6 neighbor discovery “dad-attempts” parameter.

## Format

**ndisc show dad-attempts**

## Mode

Enable.

## Description

This command allows you to display the configured value of the DAD attempts parameter, which can be set with the **ndisc set dad-attempts** command.

## Parameters

None.

## Restrictions

None.

## Example

The following example displays the current value of the DAD attempts parameter, then sets the DAD attempts parameter to 4 with the **ndisc set dad-attempts** command, and then shows the changed value with the **ndisc show dad-attempts** command.

```
xp# ndisc show dad-attempts
IPv6 Duplicate Address Detection (IPV6CTL_DAD_COUNT): 1 attempts
xp# config
xp(config)# ndisc set dad-attempts 4
xp(config)# Exit
Do you want to make the changes Active [yes]? yes
xp# ndisc show dad-attempts
IPv6 Duplicate Address Detection (IPV6CTL_DAD_COUNT): 4 attempts
```



# Chapter 43

## negate Command

The **negate** command negates a command in the scratchpad or the active configuration.

### Format

**negate** <cmd-number> [**scratchpad** | **active-config**]

### Mode

Configure.

### Description

The **negate** command allows you to negate one or more commands by specifying the command number of the commands you want to negate. The command number for each command can be found using the Configure mode **show** command. You can negate commands from the active running system or non-committed commands from the scratchpad. By default, if you do not specify **active-config** or **scratchpad**, the command to negate is assumed to be in the **active-config**.

### Parameters

|                      |  |
|----------------------|--|
| <cmd-number>         | The number of the command(s) you want to negate. Use the <b>show</b> command to display the command numbers. |
| <b>active-config</b> | Negate the specified command from the active running system.   |
| <b>scratchpad</b>    | Negate the specified non-committed command from the scratchpad.  |

### Restrictions

The specified command number must represent a command that exists.

---

## Examples

To negate command 23 from the active configuration:

```
xp# negate 23
```

To negate commands 3, 5, 6 and 7 from the scratchpad:

```
xp# negate 3,5-7 scratchpad
```



# Chapter 44

## netflow Commands

NetFlow data characterizes the movement of IP traffic on a network. NetFlow allows you to collect information about packets sent through the network and to use this data for detailed traffic analysis, network planning, network monitoring, usage-based billing, and for use by third party mediation vendors, network management tools, and billing companies. Combined with a network data analyzer, the NetFlow data you collect can help enterprise engineers, capacity planners, marketing groups, and network management better understand network traffic patterns and isolate areas in need of improvement. NetFlow traffic describes source and destination addresses, autonomous system numbers, port addresses, time of day, number of packets, total bytes, and type of service.

**Note:** To run NetFlow, you must *enable* SNMP.

**Note:** **Do not** run NetFlow and RMON Professional simultaneously.

### Command Summary

[Table 38](#) lists the **NetFlow** commands. The sections following the table describe the command syntax.

**Table 38. NetFlow Commands**

|  |
|--|
| <b>netflow clear statistics</b>  |
| <b>netflow enable</b>  |
| <b>netflow set collector</b> <collector_IPaddr> [ <b>flow-destination-port</b> <number>]                             |
| <b>netflow set engine id</b> <engine id> <b>type</b> <engine type>   |
| <b>netflow set flow-destination-port</b> <port-number>   |
| <b>netflow set interval</b> <minutes>  |
| <b>netflow set memory</b> <kilobytes_size>   |
| <b>netflow set ports</b> <port list>   <b>all-ports</b>  |
| <b>netflow show configuration</b>   <b>collector</b>   <b>ports</b>   <b>statistics</b>   <b>status</b>   <b>all</b> |

## netflow clear statistics

### Purpose

Clear many of the NetFlow statistics kept by the X-Pedition router.

### Format

**netflow clear statistics**

### Mode

Enable.

### Description

The **netflow clear statistics** command clears the NetFlow session statistics kept by the X-Pedition router (displayed by [netflow show on page 732](#)). Clearing statistics does not affect the netflow process or the data packets sent from the X-Pedition router to the collector.

### Parameters

None.

### Restrictions

None.

# netflow enable

## Purpose

Enable NetFlow agent. *Required.*

## Format

**netflow enable**

## Mode

Configure.

## Description

The netflow enable command starts the NetFlow agent.

## Parameters

None.

## Restrictions

- You must configure at least one NetFlow collector before you can execute this command successfully. See [netflow set collector on page 726](#).
- You must configure **netflow set ports** before you can monitor any ports.
- **Do not** run NetFlow and RMON simultaneously.
- To run NetFlow, you must *enable* SNMP.
- NetFlow cannot monitor traffic exits in a multicast environment. If you want to collect statistics on traffic moving through your system, you must monitor the input port(s).
- Hardware restrictions do not allow NetFlow to report a destination port for ICMP flows—the destination port is reported as 0.

# netflow set collector

## Purpose

Sets the IP address of a NetFlow collector and allows you to configure NetFlow-related parameters for the collector. *Required.*

## Format

**netflow set collector** <collector\_IPaddr> [**flow-destination-port** <number>]

## Mode

Configure.

## Description

The **netflow set collector** command allows you to set NetFlow-related parameters—even override the default settings—on a *collector-by-collector* basis only (by using the IP address of a specific NetFlow collector). Although a collector may service multiple routers, you may not enable multiple collectors for the same router.

## Parameters

|  |   |
|--|---|
| <b>collector</b><br><collector_IPaddr> | The IP address of a specific NetFlow collector. You can define only one NetFlow collector per <b>netflow set collector</b> command.<br><br><b>Note:</b> Because NetFlow packets are UDP packets, packet delivery is a best effort delivery—the system will not attempt retries if delivery fails. |
| <b>flow-destination-port</b> <number>  | The destination port number. The default NetFlow destination port number is 2055.<br><br><b>Note:</b> If you change the default value for the flow-destination port, the new value must correspond with the port ID on the collector you will use.  |

## Restrictions

None.

# netflow set engine

## Purpose

Allows you to modify the engine identification and type sent with a NetFlow packet header.  
*Optional.*

## Format

**netflow set engine id** *<engine id>* **type** *<engine type>*

## Mode

Configure.

## Description

The **netflow set engine** command allows the modification of the engine identification and type sent with a NetFlow packet header, affecting those NetFlow collectors that require specific engine values.

## Parameters

|                            |   |
|----------------------------|---|
| <i>&lt;engine id&gt;</i>   | The NetFlow engine ID (0-255 inclusive). By default, this value is 0. |
| <i>&lt;engine type&gt;</i> | The engine type (0-255 inclusive). By default, this value is 0.       |

## Restrictions

None.

## Example

To set the engine id to 4 and the engine type to 15, enter the following:

```
xp# netflow set engine id 4 type 15
```

# netflow set flow-destination-port

## Purpose

Sets the flow destination port of a specific NetFlow collector. *Optional.*

## Format

**netflow set flow-destination-port** <port-number>

## Mode

Configure.

## Description

The **netflow set flow-destination-port** command sets the default flow destination port through which the X-Pedition router will send its data. The default netflow flow-destination port number is 2055.

**Note:** If you change the default value for the flow-destination port, the new value must correspond with the port ID on the collector you will use.

## Parameters

---

|               |   |
|---------------|---|
| <port-number> | The port through which to send the NetFlow packets. |
|---------------|---|

---

## Restrictions

None.

# netflow set interval

## Purpose

Changes the default interval parameter for NetFlow. *Optional.*

## Format

**netflow set interval** <minutes>

## Mode

Configure.

## Description

The **netflow set interval** command allows you to set the time interval at which all currently monitored flows will report updated information to the collector. NetFlow staggers the packet reporting throughout the entire period of the interval to reduce congestion and prevent packet loss. As flows *expire*, they will report to the collector regardless of the time interval specified.

## Parameters

---

|                           |   |
|---------------------------|---|
| <b>Interval</b> <minutes> | The time in minutes (1-1440) for an interval. The default interval is 30 minutes. |
|---------------------------|---|

---

## Restrictions

None.

# netflow set memory

## Purpose

Changes the default memory limit for NetFlow. *Optional.*

## Format

**netflow set memory** <kilobytes\_size>

## Mode

Configure.

## Description

The **netflow set memory** command allows you to set the maximum amount of memory used by the NetFlow agent. This limits the maximum number of flows and buffered datagrams supported by the NetFlow agent. The default value is 450k.

The system will periodically calculate the NetFlow maximum memory limit. Use the **netflow show statistics** command to see the calculated value. Factors that affect the value it calculates are the amount memory being used by the system excluding memory NetFlow is using to track flows, and the amount of memory installed in the system.

## Parameters

---

|                  |  |
|------------------|--|
| <kilobytes_size> | Amount of memory for NetFlow operations the NetFlow agent will be limited to (from 100k to a system imposed limit). The default value is 450k. |
|------------------|--|

---

## Restrictions

None.



# netflow set ports

## Purpose

Configure the ports that will participate in the NetFlow accounting. *Required.*

## Format

**netflow set ports** <port list> | **all-ports**

## Mode

Configure.

## Description

The **netflow set ports** command is used to identify which ports the NetFlow agent will monitor.

## Parameters

|                          |   |
|--------------------------|---|
| <b>ports</b> <port list> | Specifies the ports participating in the NetFlow feature. |
| <b>all-ports</b>         | Enables all ports.  |

## Restrictions

None.

## Example

```
xp# netflow set ports et.3.1-4
```

# netflow show

## Purpose

Displays all pertinent NetFlow agent data including configuration, collector, statistics, and status.

## Format

**netflow show configuration| collector| ports| statistics| status| all**

## Mode

Enable.

## Description

The **netflow show** command allows you to show the configuration, collector, ports, statistics, and status, of the NetFlow agent.

## Parameters

|                      |  |
|----------------------|--|
| <b>configuration</b> | Show configured values: <ul style="list-style-type: none"><li>• NetFlow engine ID and type</li><li>• Interval at which all active flow will be sent to the collector</li><li>• UDP port on the collector where the accounting data is sent</li><li>• Priority of the NetFlow tasks</li></ul> <p><b>Note:</b> The port configuration is with the Ports information, collector configuration is with the Collector information, and memory configuration is with the Statistics information.</p> |
| <b>collector</b>     | Show collector information: <ul style="list-style-type: none"><li>• IP Address</li><li>• UDP port number</li></ul>   |
| <b>ports</b>         | Show accounting information for: <ul style="list-style-type: none"><li>• SNMP interfaces index</li><li>• Port name</li><li>• In bound flow counts on the port</li><li>• Out bound flow counts on the port</li></ul>  |

|                   |   |
|-------------------|---|
| <b>statistics</b> | Show NetFlow statistics: <ul style="list-style-type: none"> <li>• Previous and next active flow interval times</li> <li>• Memory limit the system calculated</li> <li>• Configured memory limit</li> <li>• Operating memory limit for NetFlow (smaller of the two previous items)</li> <li>• Amount of memory NetFlow is using</li> <li>• Percentage of memory limit being used</li> <li>• Peak memory information</li> <li>• Number of active flows</li> <li>• Number of reported flows (deleted flows)</li> <li>• Number of created flows (all active and deleted flows)</li> </ul> |
| <b>status</b>     | Show NetFlow status: <ul style="list-style-type: none"> <li>• State of the NetFlow agent (on/off)</li> <li>• Agent start time</li> </ul>  |
| <b>all</b>        | Show all of the above.  |

## Restrictions

None.

## Example

For detailed information about the contents of each field, see the *Enterasys X-Pedition User Reference Manual*.

```
xp# netflow show all

NetFlow Status:
  NetFlow is ENABLED
  NetFlow Started at      : 2004-03-17 23:52:31

NetFlow Default Configuration:
  NetFlow Version        : 5
  NetFlow Engine ID      : 0
  NetFlow Engine Type     : 0
  Active Flows Polling Interval : 30
  Default Port           : 2055

(Continued on next page....)
```

Continued from previous page:

NetFlow Statistics:

-Intervals:

Time of Last Reporting Interval:

Interval has not expired

Time of Next Reporting Interval:

2004-03-18 00:22:31

-Memory:

System limit on flow tracking memory:

92259 K

Configured limit on flow tracking memory:

27500 K

Current limit on flow tracking memory:

27500 K

Amount of flow tracking memory in use:

7704 K

Percent of flow tracking memory in use:

28 %

Limit on flow tracking memory at peak:

27500 K

Flow tracking memory used at peak:

7704 K

Percent of flow tracking memory used at peak:

28 %

Time of peak flow tracking memory usage:

2004-03-17 23:54:12

Number of times NetFlow failed to get requested memory:

0

-Counters:

Current number of active flows:

54784

Number of times netflow has sent reports:

31

Number of packets used to send reports:

603

Number of flows created in NetFlow:

72890

Number of flows deleted in NetFlow:

18106

Number of flows pending delete:

0

Number of flows not reported by NetFlow (discarded):

0

Number of reported records (flows):

18090

Ports Enabled for NetFlow:

| ifIndex                             | Port Name | Tracked In Flows | Tracked Out Flows | Monitored |
|-------------------------------------|-----------|------------------|-------------------|-----------|
| 1                                   | et.6.1    | 18935            | 53958             | ON        |
| 9                                   | et.7.1    | 53958            | 18935             | ON        |
| Unknown Ports Flows:                |           |                  | 0                 |           |
| Total Flows Count                   |           | : 72893          | 72893             |           |
| Number of Ports Being Monitored : 2 |           |                  |                   |           |

NetFlow Collector:

IP Address:

10.136.2.9

Accounting Port:

<Default>

# Chapter 45

## no Command

The **no** command removes a configuration command from the active configuration of the running system.

### Format

**no** *<command-to-negate>*

### Mode

Configure.

### Description

The **no** command allows you to negate a previously executed command. Following the keyword **no**, one can specify the command to negate in its entirety or use the wildcard character (\*) to negate a group of commands. In addition to the **no** command, one can also use the **negate** command to negate a group of commands using the command number.

### Parameters

---

*<command-to-negate>*

The CLI command you want to negate. You do not have to enter the entire command. You can use the wildcard character, \*, to negate matching commands. For example, if you specify “no acl 100 \*” then all commands starting with the words “acl 100” will be negated.

---

---

## Restrictions

The command to negate must already be in the active configuration. You cannot negate a command that hasn't been entered.

## Examples

To negate the specified **arp add** command, enter the following. By negating this command, the system removes the ARP entry for *nfs2* from the ARP table.

```
xp# no arp add nfs2 macaddr 080020:13a09f exit-port et.3.1
```

To negate all commands starting with the word "acl":

```
xp# no acl *
```

# Chapter 46

## ntp Commands

The **ntp** commands configure and display the characteristics of the NTP (Network Time Protocol) client.

### Command Summary

[Table 39](#) lists the **ntp** commands. The sections following the table describe the command syntax.

**Table 39. ntp Commands**

|   |
|---|
| <b>ntp set server</b> <nameiplist> [ <b>interval</b> <minutes>] [ <b>source</b> <ipaddr>] [ <b>version</b> <num>] |
| <b>ntp show all</b>   |
| <b>ntp synchronize server</b> <host>  |

# ntp set server

## Purpose

Specifies the NTP server against which the X-Pedition router is to synchronize its clock.

## Format

**ntp set server** <nameiplist> [**interval** <minutes>] [**source** <ipaddr>] [**version** <num>]

## Mode

Configure.

## Description

The **ntp set server** command instructs the X-Pedition router's NTP client to periodically synchronize its clock. By default, the X-Pedition router specifies an NTPv3 client that sends a synchronization packet to the server every 60 minutes. This means the X-Pedition router will attempt to set its own clock against the server once every hour. The synchronization interval as well as the NTP version number can be changed. To ensure that NTP has the correct time, you need to specify the time zone, as well. You can set the time zone by using the **system set timezone** command. When specifying daylight saving time, you'll need to use the **system set daylight-saving** command.

**Note:** If you configured the **ntp set server** command in the startup file and the X-Pedition router does not receive a valid response from the configured NTP servers after startup, the router will send an NTP request to each NTP server every minute until: (a) the router receives a valid response from an NTP server; (b) the router reaches the configured NTP query interval; or (c) you reconfigure the **ntp set server** command. During this time, the router will not display any NTP related message. After it meets one of the above conditions, the router returns to the normal NTP mode—this mode sends requests at configured query intervals and displays NTP messages.

## Parameters

|                            |   |
|----------------------------|---|
| <b>server</b> <nameiplist> | Specifies a list of host names or/and ip addresses of NTP servers. The maximum number of servers is 3. Specify each ip address in dotted-decimal-notation. If more than one servers are configured, they need to be separated by space and are surrounded with a set of quotes. |
| <b>interval</b> <minutes>  | Specifies how often (in minutes) the X-Pedition router should synchronize with the server. The default synchronization interval is 60 minutes. Valid interval is between 1 minute to 10080 minutes (7 days).  |



|                        |   |
|------------------------|---|
| <b>source</b> <ipaddr> | Specifies the source IP address to be used by the X-Pedition router for sending the NTP packet. The IP address must belong to one of the interfaces on the X-Pedition router. |
| <b>version</b> <num>   | Specifies the NTP version number of the packet. The default version number is 3 (NTPv3). Valid value is 1-3.  |

## Restrictions

None.

## Examples

To send NTP packets to the NTP server 10.13.1.1 with default parameters:

```
xp(config)# ntp set server 10.13.1.1
```

To synchronize with a NTP server every 15 minutes with a specific source IP address:

```
xp(config)# ntp set server 10.13.1.1 interval 15 source 10.15.3.3
```

To configure three NTP servers with default parameters:

```
xp(config)# ntp set server "ntpserver1.org ntpserver2.org 10.17.5.5"
```

# ntp show all

## Purpose

Display NTP information about the X-Pedition router.

## Format

**ntp show all**

## Mode

Enable.

## Description

The **ntp show all** command displays various NTP information about the XP. This information may include the last time a successful synchronization was made, the synchronization interval, the NTP version number, the NTP server list, and so on.

## Parameters

None.

## Restrictions

None.

## Example

```
xp# ntp show all
NTP status:
  Synchronization interval: 60 mins
  Version: NTPv3
  Servers:
    ntpserver1.org
    ntpserver2.org
    10.17.5.5
  Last successful contact: 2001-09-04 16:46:40
```

# ntp synchronize server

## Purpose

Manually force the X-Pedition router to immediately synchronize with a NTP server.

## Format

**ntp synchronize server** <host>

## Mode

Enable.

## Description

The **ntp synchronize server** command forces the X-Pedition router to immediately synchronize its clock with the NTP server. Unlike the Configuration mode **ntp set server** command, this Enable mode command does not send periodic synchronization packets to the server. Instead, each time this command is executed, the X-Pedition router synchronizes itself with the server. To have the X-Pedition router synchronize itself periodically, use the **ntp set server** command.

## Parameters

---

|        |   |
|--------|---|
| <host> | Specifies the hostname or the IP address of the NTP server. |
|--------|---|

---

## Restrictions

None.

## Examples

To synchronize the X-Pedition router against the NTP server 10.13.1.1:

```
xp(config)# ntp synchronize server 10.13.1.1
%NTP-I-TIMESYNC, Time synchronized to Mon Jan 22 23:11:28 2001
```



# Chapter 47

## ospf Commands

The **ospf** commands let you display and set parameters for the Open Shortest Path First (OSPF) routing protocol.

### Command Summary

[Table 40](#) lists the **ospf** commands. The sections following the table describe the command syntax.

**Table 40. ospf Commands**

|  |
|--|
| <b>ospf add interface</b> [<interfacename-or-IPaddr>  <b>all</b> ] <b>to-area</b> <area-addr>  <b>backbone</b><br>[ <b>type broadcast non-broadcast point-to-multipoint</b> ]                    |
| <b>ospf add nbma-neighbor</b> <IPaddr> <b>to-interface</b> <interfacename-or-IPaddr> [ <b>eligible</b> ]   |
| <b>ospf add network</b>   <b>summary-range</b> <IPaddr/mask> <b>to-area</b> <area-addr> [ <b>restrict</b> ] [ <b>host-net</b> ]  |
| <b>ospf add nssa-network</b> <IPADDR_MASK> [ <b>to-area</b> <IPaddr>  <b>restrict</b> ] <b>host-net</b> ]  |
| <b>ospf add pmp-neighbor</b> <IPaddr> <b>to-interface</b> <interfacename-or-IPaddr>  |
| <b>ospf add stub-host</b> <IPaddr> <b>to-area</b> [<area-addr>  <b>backbone</b> ] [ <b>cost</b> <num>]   |
| <b>ospf add stub-network</b> <IPADDR_MASK> [ <b>to-area</b> <IPaddr>  <b>host-net</b> ] <b>cost</b> <num>]   |
| <b>ospf add summary-filter</b> [ <b>network</b> <IPADDR_MASK>  <b>all</b> ] <b>default</b>   <b>to-area</b> <IPaddr>  <b>exact</b> ]<br><b>refines</b>   <b>between</b> <num>  <b>host-net</b> ] |
| <b>ospf add virtual-link</b> <number-or-string> <b>neighbor</b> <IPaddr> <b>transit-area</b> <area-num>  |
| <b>ospf create area</b> <area-num> [ <b>backbone</b> ]   |
| <b>ospf log router-lsas</b> <b>on</b>   <b>off</b>   <b>on detail</b>  |
| <b>ospf set advertise-subnet</b> <b>on</b>   <b>off</b>  |

Table 40. ospf Commands (Continued)

|  |
|--|
| <b>ospf set always-update-summary on off</b>   |
| <b>ospf set area</b> <area-num> <option-list>  |
| <b>ospf set ase-defaults</b> {[preference <num>]  [cost <num>]  [type <num>]  [inherit-metric]  <br>[tag [as] <num>]  [multicast]}   |
| <b>ospf set authentication-method</b> [none simple md5 [keychain <num> <string>]]  |
| <b>ospf set hello-interval</b> <num>   |
| <b>ospf set interface</b> <name-or-IPaddr> all [state disable enable] [cost <num>] [no-multicast]  <br>[retransmit-interval <num>] [transit-delay <num>] [priority <num>]  <br>[hello-interval <num>] [router-dead-interval <num>] [poll-interval <num>]  <br>[key-chain <num-or-string>] [authentication-method none  simple  md5] [passive]  <br>[advertise-subnet on off] [strict-routers on off] |
| <b>ospf set nssa-defaults</b> [preference <num>] [cost <num>] [type <num>] [inherit-metric]  |
| <b>ospf set opaque-capability on off</b>   |
| <b>ospf set poll-interval</b> <num>  |
| <b>ospf set priority</b> <num>   |
| <b>ospf set retransmit-interval</b> <num>  |
| <b>ospf set rfc1583 on</b>   |
| <b>ospf set router-dead-interval</b> <num>   |
| <b>ospf set transit-delay</b> <num>  |
| <b>ospf set-trap all none [&lt;option-list&gt; on off]</b>   |
| <b>ospf set virtual-link</b> <number-or-string> [no-multicast] [retransmit-interval <num>]  <br>[transit-delay <num>] [priority <num>] [hello-interval <num>]  <br>[router-dead-interval <num>] [poll-interval <num>] [key-chain <num-or-string>]  <br>[authentication-method none  simple  md5] [passive] [advertise-subnet on off]   |
| <b>ospf show</b> <option-list>   |
| <b>ospf start   stop</b>   |
| <b>ospf trace</b> [spf  debug  packets {detail  send  receive}  hello {detail  send  receive} <br>dd {detail  send  receive}  request {detail  send  receive}  update {detail  send  receive} <br>ack {detail  send  receive}  local-options [all  general  state  normal  policy  task  timer <br>route  none]  ospf-state  dr-election  db  flood]   |

# ospf add interface

## Purpose

Associates an interface with an OSPF area.

## Format

**ospf add interface** [*<interfacename-or-IPaddr>* | **all**] **to-area** *<area-addr>* | **backbone**  
**[type broadcast | non-broadcast | point-to-multipoint]**

## Mode

Configure.

## Parameters

|   |   |
|---|---|
| <i>&lt;interfacename-or-IPaddr&gt;</i>   <b>all</b>       | An interface name or an IP address. Use the keyword, <b>all</b> , to specify all interfaces.  |
|   | <b>Note:</b> Enterasys recommends that you use alphabetic characters when defining interface names—purely numeric interfaces will be interpreted as IP addresses. The X-Pedition router will display interface names up to 32 characters in length.                     |
| <b>to-area</b> <i>&lt;area-addr&gt;</i>   <b>backbone</b> | OSPF Area with which this interface is to be associated.  |
| <b>type</b>   | Specifies whether the interface is broadcast, non-broadcast, or point-to-multipoint. Specify one of the following: <ul style="list-style-type: none"> <li>– <b>broadcast</b> (default)</li> <li>– <b>non-broadcast</b></li> <li>– <b>point-to-multipoint</b></li> </ul> |

## Restrictions

None.

# ospf add nbma-neighbor

## Purpose

Specifies an OSPF NBMA Neighbor.

## Format

**ospf add nbma-neighbor** <IPaddr> **to-interface** <interfacename-or-IPaddr> [**eligible**]

## Mode

Configure.

## Parameters

|  |  |
|--|--|
| <b>nbma-neighbor</b><br><IPaddr>                 | The nbma neighbor you will add.  |
| <b>to-interface</b><br><interfacename-or-IPaddr> | Adds the neighbor to the specified OSPF interface.<br><br>Enterasys recommends that you use alphabetic characters when defining interface names—purely numeric interfaces will be interpreted as IP addresses. The X-Pedition router will display interface names up to 32 characters in length. |
| <b>eligible</b>                                  | Specifies whether an OSPF NBMA Neighbor is eligible for becoming a designated router.  |

## Restrictions

None.



## ospf add network | summary-range

**Note:** The **ospf add network** command may use the same syntax as other vendors. Please review the documentation for the proper use of this command.

### Purpose

Configures summary-ranges on Area Border Routers (ABRs). This allows you to reduce the amount of routing information propagated between areas.

On the X-Pedition router, summary ranges are created using the **ospf add summary-range** command. The networks specified using this command describe the scope of an area. Intra-area Link State Advertisement (LSAs) that fall within the specified ranges are aggregated and sent in one summary LSA advertising the summary range only. If you specify the restrict option, the intra-area LSAs that fall within the specified ranges will not be advertised into other areas. Each intra-area LSA that does not fall into the summary ranges is advertised separately in a Summary LSA.

### Format

**ospf add network | summary-range** <IPaddr/mask> **to-area** <area-addr> [**restrict**] [**host-net**]

### Mode

Configure.

### Parameters

|                            |   |
|----------------------------|---|
| <IPaddr/mask>              | IP Address and network mask value representing the summary-range.<br>Example: 16.122.0.0/255.255.0.0 or 16.122.0.0/16.        |
| <b>to-area</b> <area-addr> | OSPF Area with which this summary-range is to be associated.  |
| <b>restrict</b>            | If the restrict option is specified for a network/summary-range, then that network is not advertised in Summary network LSAs. |
| <b>host-net</b>            | Specifies that the network is an OSPF Host Network.   |

### Restrictions

None.

## Example

In the following example, two summary ranges are created:

|   |
|---|
| <pre>ospf add summary-range 207.135.16.0/24 to-area 207.135.0.0 ospf add summary-range 207.135.17.0/24 to-area 207.135.0.0 restrict</pre> |
|---|

All intra-area Link State Advertisements (LSAs) that fall within the range 207.135.16.0/24 will be advertised in one Summary Network LSA rather than advertised in individual Summary Network LSAs.

Because the summary range 207.135.17.0/24 has the restrict option associated with it, intra-area LSAs that fall within it are not advertised to other areas. This can be helpful when “hidden networks” are needed.

# ospf add nssa-network

## Purpose

Specifies the network range that should be translated to a type-5 LSA from a NSSA type-7 LSA. If **restrict** is specified, the network range will not be translated.

## Format

**ospf add nssa-network** <IPADDR\_MASK> [**to-area** <IPaddr>|**restrict**|**host-net**]

## Mode

Configure.

## Description

This command allows the user to decide which type-7 LSAs need to be translated into type-5 LSAs in order to be advertised to the rest of OSPF. Only the NSSA Area Border Router with the highest IP address will perform the type-7 to type-5 translations. Therefore, this command should only be used on NSSA Area Border Routers.

## Parameters

|                         |   |
|-------------------------|---|
| <IPaddr/mask>           | IP Address and network mask value. If a mask is not provided, a natural mask is assigned based on the class of the network. |
| <b>to-area</b> <IPaddr> | Specifies the NSSA area to which this network range should be added.  |
| <b>restrict</b>         | Restricts this NSSA network range from being translated into a type-5 LSA.  |
| <b>host-net</b>         | Specifies that this is a host network.  |

## Restrictions

None.

## Example

To add NSSA network 1.1.0.0/16 to a NSSA Area Border Router for area 0.0.0.1:

```
ospf add nssa-network 1.1.0.0/16 to-area 0.0.0.1
```

To restrict a specific NSSA network:

```
ospf add nssa-network 2.2.0.0/16 to-area 0.0.0.1 restrict
```

# ospf add pmp-neighbor

## Purpose

Specifies an OSPF Point-to-Multipoint Neighbor.

## Format

**ospf add pmp-neighbor** <IPaddr> **to-interface** <interfacename-or-IPaddr>

## Mode

Configure.

## Description

The **ospf add pmp-neighbor** configures a Point-to-Multipoint neighbor router on an interface. A Point-to-Multipoint connectivity is used when the network does not provide full connectivity to all routers in the network. As in the case of NBMA (non-broadcast multiple access) networks, a list of neighboring routers reachable over a PMP network should be configured so that the router can discover its neighbors.

## Parameters

|  |  |
|--|--|
| <b>pmp-neighbor</b><br><IPaddr>                  | Specifies the point-to-multipoint neighbor.  |
| <b>to-interface</b><br><interfacename-or-IPaddr> | Adds the neighbor to the specified OSPF interface.<br><br>Enterasys recommends that you use alphabetic characters when defining interface names—purely numeric interfaces will be interpreted as IP addresses. The X-Pedition router will display interface names up to 32 characters in length. |

## Restrictions

None.

## Example

To add a point-to-multipoint neighbor with IP address 134.141.179.141 to the OSPF interface 134.141.179.152:

```
xp(config)# ospf add pmp-neighbor 134.141.179.141 to-interface 134.141.179.152
```

# ospf add stub-host

## Purpose

Adds a stub-host to an OSPF area.

## Format

**ospf add stub-host** <IPaddr> **to-area** [<area-addr>| **backbone**] [**cost** <num>]

## Mode

Configure.

## Parameters

|   |   |
|---|---|
| <b>to-area</b> <area-addr>  <b>backbone</b> | OSPF Area to which you are adding a stub host.  |
| <b>cost</b> <num>                           | The cost that should be advertised for this directly attached stub host. Specify a number from 0 – 65535. |

## Restrictions

None.

# ospf add stub-network

## Purpose

Adds a directly attached network to be advertised as reachable from this router.

## Format

**ospf add stub-network** <IPaddr/mask> **to-area** <area-addr> [**cost** <num>] [**host-net**]

## Mode

Configure.

## Description

You may add directly-attached networks to OSPF that are reachable from this router. This command should be used for interfaces that are not being added to OSPF.

## Parameters

|                            |   |
|----------------------------|---|
| <IPaddr/mask>              | IP Address and network mask value representing the stub network. If a mask is not provided, a natural mask is assigned based on the class of the network. |
| <b>to-area</b> <area-addr> | Specifies the OSPF area to which you are adding the stub network.   |
| <b>cost</b> <num>          | The cost that should be advertised for this stub-network. Specify a number from 1 to 65535. There is no default cost.                                     |
| <b>host-net</b>            | Specifies that this is a host network.  |

## Restrictions

None.

## Example

To add directly-attached network 1.1.0.0/16 to area 0.0.0.1:

```
ospf add stub-network 1.1.0.0/16 to-area 0.0.0.1
```

# ospf add summary-filter

## Purpose

Specifies which summary-LSAs to filter from a non-transit area.

## Format

**ospf add summary-filter** [**network** <IPADDR\_MASK> | **all** | **default** | **to-area** <IPADDR> | **exact** | **refines** | **between** <num> | **host-net**]

## Mode

Configure.

## Description

Summary filters are used to reduce the amount of summary LSAs stored in a non-transit area. This should only be used in stub and NSSA areas with default routes. Otherwise, it could cause routing problems.

## Parameters

|                                 |   |
|---------------------------------|---|
| <b>network</b><br><IPaddr_mask> | Specifies the network to be filtered by IP address and network mask value. If a mask is not provided, a natural mask is assigned based on the class of the network. |
| <b>all</b>                      | Specifies that all network should be filtered.  |
| <b>default</b>                  | Specifies that the default route should be filtered.  |
| <b>to-area</b> <IPaddr>         | The area, by IP address, in which to add the summary filter.  |
| <b>exact</b>                    | Specifies that the destination mask must match the given mask exactly.  |
| <b>refines</b>                  | Specifies that the destination mask must be more specific than the given mask.  |
| <b>between</b> <num>            | Specifies that the destination mask must be within the upper and lower limits. Specify a range from 1 to 32.  |
| <b>host-net</b>                 | Specifies that this is a host network.  |

## Restrictions

None.

## Example

To add a summary filter for network 1.1.0.0/16 to stub area 0.0.0.1:

|   |
|---|
| <b>ospf add summary-filter network 1.1.0.0/16 to-area 0.0.0.1</b> |
|---|



# ospf add virtual-link

## Purpose

Creates an OSPF Virtual Link.

## Format

**ospf add virtual-link** *<number-or-string>* **neighbor** *<IPaddr>* **transit-area** *<area-num>*

## Mode

Configure.

## Parameters

|   |  |
|---|--|
| <i>&lt;number-or-string&gt;</i>             | A number or character string identifying the virtual link. |
| <b>neighbor</b> <i>&lt;IPaddr&gt;</i>       | The IP address of an OSPF virtual link neighbor.           |
| <b>transit-area</b> <i>&lt;area-num&gt;</i> | The Area ID of the transit area.                           |

## Restrictions

None.

## ospf create area

### Purpose

Create an OSPF area.

### Format

**ospf create area** *<area-num>***|backbone**

### Mode

Configure.

### Parameters

|                         |   |
|-------------------------|---|
| <i>&lt;area-num&gt;</i> | The Area ID. Area IDs are formatted like IP addresses:<br><i>&lt;num&gt;.&lt;num&gt;.&lt;num&gt;.&lt;num&gt;.</i> |
| <b>backbone</b>         | Specifies that the Area you are adding is the backbone area.  |

### Restrictions

None.

# ospf log router-lsas

## Purpose

Logs Router LSAs from incoming link-state update packets to the console and Syslog server.

## Format

**ospf log router-lsas on|off | on detail**

## Mode

Enable.

## Parameters

|                  |  |
|------------------|--|
| <b>off</b>       | Turns logging off (default).   |
| <b>on</b>        | Turns logging on. Gives the user basic information that states which neighbor sent the update and which router advertised each LSA contained within the update packet. |
| <b>on detail</b> | Logs detailed information from the Router LSA.   |

## Restrictions

None.

## Examples

To view basic log information, enter the following command from Enable mode:

```
xp# ospf log router-lsas on
2002-07-25 12:09:40 %OSPF-I-UPDATE, Update received from 50.50.50.23 on interface to23.
2002-07-25 12:09:40 %OSPF-I-ADVRTR, Advertising Router: 15.15.15.15
```

To display detailed log information contained within the Router LSA, enter the following from Enable mode:

```
xp# ospf log router-lsas on detail
2002-07-25 12:09:40 %OSPF-I-UPDATE, Update received from 50.50.50.23 on interface to23.
2002-07-25 12:09:40 %OSPF-I-ADVRTR, Advertising Router: 15.15.15.15
2002-07-25 12:09:40 %OSPF-I-LINK, type: TRANS NET Link Id: 40.40.40.23 LinkData: 40.40.40.15
2002-07-25 12:09:40 %OSPF-I-LINK, type: TRANS NET Link Id: 30.30.30.16 LinkData: 30.30.30.15
2002-07-25 12:09:40 %OSPF-I-LINK, type: STUB Link Id: 80.80.80.0 LinkData: 255.255.255.0
2002-07-25 12:09:40 %OSPF-I-LINK, type: STUB Link Id: 15.15.15.15 LinkData: 255.255.255.255
```

## ospf set advertise-subnet

### Purpose

Specifies whether OSPF should advertise a point-to-point interface as a subnet or a host route. The default is to advertise as a host route.

### Format

**ospf set advertise-subnet on|off**

### Mode

Configure.

### Parameters

|            |   |
|------------|---|
| <b>on</b>  | Advertise the point-to-point interface as a subnet.     |
| <b>off</b> | Advertise the point-to-point interface as a host route. |

### Restrictions

None.

### Example

To advertise point-to-point interfaces as subnets:

```
ospf set advertise-subnet on
```

# ospf set always-update-summary

## Purpose

Specifies whether an SPF calculation should occur when a summary LSA's path type has changed. This command is provided to disable an optimization that can cause OSPF to fail commercially available, component-level tests. The default is on.

## Format

**ospf set always-update-summary on|off**

## Mode

Configure.

## Parameters

|            |   |
|------------|---|
| <b>on</b>  | A new SPF calculation will occur for a changed summary LSA supporting path.     |
| <b>off</b> | A new SPF calculation will not occur for a changed summary LSA supporting path. |

## Restrictions

None.

## Example

To stop SPF calculations from occurring after a summary-LSA change:

```
ospf set always-update-summary off
```

# ospf set area

## Purpose

Sets the parameters for an OSPF area.

## Format

```
ospf set area <area-num> stub | stub-cost <num> | [authentication-method none|simple|md5] |  
nssa | nssa-cost <num> | nssa-type | retransmit-interval <num> | transit-delay <num> |  
priority <num> | hello-interval <num> | router-dead-interval <num> | poll-interval <num> |  
[advertise-subnet on|off] | key-chain <num|string>
```

## Mode

Configure.

## Parameters

|  |   |
|--|---|
| <area-num>                               | The Area ID. Area IDs are formatted like IP addresses:<br><num>.<num>.<num>.<num>.  |
| stub                                     | Makes this area a stub area.  |
| stub-cost <num>                          | Specifies the cost to be used to inject a default route into the area.<br>Specify a number from 1 to 65535.   |
| authentication-method<br>none simple md5 | Specifies the authentication method used within the area. Select one<br>of the following:<br><br><b>none</b> Does not use authentication.<br><br><b>simple</b> Uses a simple string (password) up to 16 characters in<br>length for authentication. If you choose this authentication<br>method, you should also specify a key-chain identifier<br>using the key-chain option.<br><br><b>md5</b> Uses the MD5 algorithm to create a crypto-checksum of an<br>OSPF packet and an authentication key of up to 16<br>characters. |
| nssa                                     | Make this area a Not-So-Stubby Area (NSSA).   |
| nssa-cost <num>                          | Specifies the cost to be used to import non-OSPF routes into the<br>NSSA. The default cost is 1. Specify a number from 1 to 65535.  |
| nssa-type                                | Sets the type of routes exported from the GateD Routing Table into<br>OSPF NSSA. Types can be 1 (default) or 2.   |

|                                      |   |
|--------------------------------------|---|
| <b>retransmit-interval</b><br><num>  | Sets the number of seconds between link state advertisements for adjacencies. Enter a number from 1 to 65535. The default interval is 5 seconds.  |
| <b>transit-delay</b> <num>           | Sets the estimated number of seconds required to transmit a link state update. Enter a value from 1 to 65535. The default delay is 1 second.  |
| <b>priority</b> <num>                | Sets the priority for becoming the Designated Router. Specify a number from 0 to 255. Choosing 0 causes the router to be ineligible for the Designated Router position. The default priority is 1.  |
| <b>hello-interval</b> <num>          | Sets the number of seconds between hello packets that the router sends on an interface. Select a value from 1 to 255. The default interval is 10 seconds for broadcast interfaces and 30 seconds for point-to-point and other non-broadcast interfaces. |
| <b>router-dead-interval</b><br><num> | Sets the number of seconds allowed between hello packets received from a neighbor before that neighbor is declared down. Specify a value from 1 to 65535. The default is 4 times the hello-interval.  |
| <b>poll-interval</b> <num>           | Sets the minimum number of seconds required between OSPF packets that the router sends to establish neighbor adjacency. Specify a value from 0 to 255. the default interval is 120 seconds.   |
| <b>advertise-subnet on off</b>       | Specifies whether an area should advertise a point-to-point interface as a subnet or a host route. The default is off, where the interface is advertised as a host route.   |
| <b>key-chain</b> <num string>        | Key chain containing the authentication keys. This is defined by the <b>ip-router authentication create key-chain</b> command. An authentication method should be specified using the <b>key-chain</b> option for authentication to work properly.      |

## Restrictions

None.

# ospf set ase-defaults

## Purpose

Sets the defaults used when importing OSPF ASE routes into the routing table and exporting routes from the routing table into OSPF ASEs. The X-Pedition router generates and floods a batch of ASE link state advertisements into OSPF one time per second. Each batch contains 100 ASEs.

## Format

```
ospf set ase-defaults {[preference <num>] | [cost <num>] | [type <num>] | [inherit-metric] | [tag [as] <num>] | [multicast]}
```

## Mode

Configure.

## Parameters

|                         |  |
|-------------------------|--|
| <b>preference</b> <num> | Specifies the preference of OSPF ASE routes. Specify a number between 0 and 255.   |
| <b>cost</b> <num>       | Specifies the cost used when exporting non-OSPF route into OSPF as an ASE. Specify a number from 1 to 65535.   |
| <b>type</b> <num>       | Specifies the ASE type (1 or 2) for routes exported from the routing table into OSPF—the default is type <b>2</b> . You can change the default using the <b>type</b> option, or override the type in OSPF export policies.   |
| <b>inherit-metric</b>   | Allows an OSPF ASE route to inherit the metric of the external route when no metric is specified on the export. A metric specified with the export command takes precedence. The cost specified in the default is used if you do not specify <b>inherit-metric</b> . |
| <b>tag [as]</b> <num>   | Allows an exterior gateway protocol to propagate data through OSPF using a tag value or an AS number if the <b>as</b> option is included.  |
| <b>multicast</b>        | Specifies that OSPF routes should be installed in both unicast and multicast RIBs. Non-ASE OSPF routes as well as ASE OSPF routes will be installed into both RIBs.  |

## Restrictions

None.



# ospf set authentication-method

## Purpose

Sets the authentication method and key values. The default method is none.

## Format

**ospf set authentication-method** [**none**|**simple**|**md5**][**key-chain** <num>|<string>]]

## Mode

Configure.

## Parameters

|                                 |  |
|---------------------------------|--|
| <b>none</b>                     | Does not use authentication.   |
| <b>simple</b>                   | Uses a simple string (password) up to 16 characters in length for authentication.  |
| <b>md5</b>                      | Uses the MD5 algorithm to create a crypto-checksum of an OSPF packet and an authentication key of up to 16 characters.         |
| <b>key-chain</b> <num> <string> | Key chain containing the authentication keys. This is defined by the <b>ip-router authentication create key-chain</b> command. |

## Restrictions

None.

## Example

To add MD5 authentication to OSPF:

```
ip-router authentication create key-chain chain key test id 10
ospf set authentication-method md5 key-chain chain
```

## ospf set hello-interval

### Purpose

Sets the number of seconds between hello packets that the router sends on an interface. The default interval is 10 seconds for broadcast interfaces and 30 seconds for point-to-point and other non-broadcast interfaces.

### Format

**ospf set hello-interval** *<num>*

### Mode

Configure.

### Parameters

|                    |                               |
|--------------------|-------------------------------|
| <i>&lt;num&gt;</i> | Select a value from 1 to 255. |
|--------------------|-------------------------------|

### Restrictions

None.

### Example

To change hello interval to 15 seconds:

|                                   |
|-----------------------------------|
| <b>ospf set hello-interval 15</b> |
|-----------------------------------|

# ospf set interface

## Purpose

Sets parameters for an OSPF interface.

## Format

```
ospf set interface <name-or-IPaddr>|all [state disable|enable] [cost <num>] [no-multicast]
[retransmit-interval <num>] [transit-delay <num>] [priority <num>] [hello-interval <num>]
[router-dead-interval <num>] [poll-interval <num>] [key-chain <num-or-string>]
[authentication-method none|simple|md5] [passive] [advertise-subnet on|off]
[strict-routers on|off]
```

## Mode

Configure

## Parameters

|                                   |   |
|-----------------------------------|---|
| <b>&lt;name-or-IPaddr&gt; all</b> | <p>The OSPF interface for which you are setting OSPF parameters.</p> <p><b>Note:</b> Enterasys recommends that you use alphabetic characters when defining interface names—purely numeric interfaces will be interpreted as IP addresses. The X-Pedition router will display interface names up to 32 characters in length.</p>   |
| <b>state disable enable</b>       | Enables or disables OSPF on the interface.  |
| <b>cost &lt;num&gt;</b>           | <p>The cost associated with this interface. Specify a number from 1 to 65535. The total cost to get to a destination is calculated by adding up the cost of all interfaces that a packet must cross to reach a destination.</p> <p>The default cost of an OSPF interface is calculated using its bandwidth. A VLAN that is attached to an interface could have several ports of differing speeds. The bandwidth of an interface is represented by the highest bandwidth port that is part of the associated VLAN. The cost of an OSPF interface is inversely proportional to this bandwidth. The cost is calculated using the following formula:</p> $Cost = 2000000000 / speed \text{ (in bps)}$ <p><a href="#">Table 41</a> lists the port types and the OSPF default cost associated with each type.</p> |
| <b>no-multicast</b>               | Instructs the X-Pedition router not to send multicast packets to neighbors on point-to-point interfaces.  |

|  |  |
|--|--|
| <b>retransmit-interval</b><br><num>            | The number of seconds between link state advertisement retransmissions for adjacencies belonging to this interface. Specify a number equal to or greater than 1. The default is 5.   |
| <b>transit-delay</b> <num>                     | The estimated number of seconds required to transmit a link state update over this interface. Transit delay takes into account transmission and propagation delays and must be greater than 0. Specify a number equal to or greater than 1. The default is 1.  |
| <b>priority</b> <num>                          | A number between 0 and 255 specifying the priority for becoming the designated router on this interface. When two routers attached to a network both attempt to become the designated router, the one with the higher priority wins. A router whose router priority is set to 0 is ineligible to become designated router. Specify a number from 0 – 255. The default is 1.  |
| <b>hello-interval</b> <num>                    | The length of time, in seconds, between hello packets that the router sends on this interface. Specify a number from 0 – 255. The default is 10 for broadcast interfaces and 30 for point-to-point and other non-broadcast interfaces.   |
| <b>router-dead-interval</b><br><num>           | The number of seconds not hearing a router's Hello packets before the router's neighbors will declare it down. Specify a number from 0 – 255. The default is 4 times the value of the hello interval.  |
| <b>poll-interval</b> <num>                     | Before adjacency is established with a neighbor, OSPF packets are sent periodically at the specified poll interval. Specify a number equal to or greater than 1. The default value for this option is 120 seconds.   |
| <b>key-chain</b><br><num-or-string>            | The identifier of the key-chain containing the authentication keys.  |
| <b>[authentication-method none simple md5]</b> | <p><b>none</b><br/>No authentication method associated with this interface.</p> <p><b>simple</b><br/>The authentication method is a simple password in which an authentication key of up to 16 characters is included in the packet. If you choose this authentication method, you should also specify a key-chain identifier using the key-chain option.</p> <p><b>md5</b><br/>Use MD5 to create a crypto-checksum of an OSPF packet and an authentication key of up to 16 characters. If you choose this authentication method, you should also specify a key-chain identifier using the key-chain option.</p> |
| <b>passive</b>                                 | Specifies that an interface is not to receive or send packets on this interface. By default, the interface is non-passive.   |
| <b>advertise-subnet on off</b>                 | Specifies whether this point-to-point interface should advertise itself as a subnet or host route. The default is off, where the interface advertises itself as a host route.  |

|  |  |
|--|--|
| <b>retransmit-interval</b><br><num>            | The number of seconds between link state advertisement retransmissions for adjacencies belonging to this interface. Specify a number equal to or greater than 1. The default is 5.   |
| <b>transit-delay</b> <num>                     | The estimated number of seconds required to transmit a link state update over this interface. Transit delay takes into account transmission and propagation delays and must be greater than 0. Specify a number equal to or greater than 1. The default is 1.  |
| <b>priority</b> <num>                          | A number between 0 and 255 specifying the priority for becoming the designated router on this interface. When two routers attached to a network both attempt to become the designated router, the one with the higher priority wins. A router whose router priority is set to 0 is ineligible to become designated router. Specify a number from 0 – 255. The default is 1.  |
| <b>hello-interval</b> <num>                    | The length of time, in seconds, between hello packets that the router sends on this interface. Specify a number from 0 – 255. The default is 10 for broadcast interfaces and 30 for point-to-point and other non-broadcast interfaces.   |
| <b>router-dead-interval</b><br><num>           | The number of seconds not hearing a router's Hello packets before the router's neighbors will declare it down. Specify a number from 0 – 255. The default is 4 times the value of the hello interval.  |
| <b>poll-interval</b> <num>                     | Before adjacency is established with a neighbor, OSPF packets are sent periodically at the specified poll interval. Specify a number equal to or greater than 1. The default value for this option is 120 seconds.   |
| <b>key-chain</b><br><num-or-string>            | The identifier of the key-chain containing the authentication keys.  |
| <b>[authentication-method none simple md5]</b> | <p><b>none</b><br/>No authentication method associated with this interface.</p> <p><b>simple</b><br/>The authentication method is a simple password in which an authentication key of up to 16 characters is included in the packet. If you choose this authentication method, you should also specify a key-chain identifier using the key-chain option.</p> <p><b>md5</b><br/>Use MD5 to create a crypto-checksum of an OSPF packet and an authentication key of up to 16 characters. If you choose this authentication method, you should also specify a key-chain identifier using the key-chain option.</p> |
| <b>passive</b>                                 | Specifies that an interface is not to receive or send packets on this interface. By default, the interface is non-passive.   |
| <b>advertise-subnet on off</b>                 | Specifies whether this point-to-point interface should advertise itself as a subnet or host route. The default is off, where the interface advertises itself as a host route.  |

---

|                              |  |
|------------------------------|--|
| <b>strict-routers on off</b> | Specifies whether to ignore packets from neighbors not specified within a non-broadcast or point-to-multipoint interface. The default is on (ignores the packets). |
|------------------------------|--|

---

**Table 41. Port Types and OSPD Default Costs**

| Port Media Type | Speed     | OSPF Default Cost |
|-----------------|-----------|-------------------|
| Ethernet 1000   | 1000 Mbps | 2                 |
| Ethernet 10/100 | 100 Mbps  | 20                |
| Ethernet 10/100 | 10 Mbps   | 200               |
| WAN (T1)        | 1.5 Mbps  | 1333              |
| WAN (T3)        | 45 Mbps   | 44                |

## Restrictions

None.

# ospf set nssa-defaults

## Purpose

Specifies default values to use when importing and exporting NSSA routes.

## Format

**ospf set nssa-defaults** { [**preference** <num>] [**cost** <num>] [**type** <num>] [**inherit-metric**] }

## Mode

Configure.

## Parameters

|                         |   |
|-------------------------|---|
| <b>preference</b> <num> | Specifies the preference of NSSA routes. Specify a number from 0 to 255. The default preference is 150. |
| <b>cost</b> <num>       | Specifies the cost of exporting NSSA routes. Specify a number from 1 to 16777215. The default is 1.     |
| <b>type</b> <num>       | Specifies the type for imported NSSA routes. Types can be 1 or 2. The default type is 2.                |
| <b>inherit-metric</b>   | Allows a NSSA route to inherit the metric of the external route when one is not specified.              |

## Restrictions

None.

## Example

To set NSSA route preference to 100 and cost to 5:

```
ospf set nssa-defaults preference 100 cost 5
```

## **ospf set opaque-capability**

### **Purpose**

Specifies whether to support RFC 2370, Opaque LSAs.

### **Format**

**ospf set opaque-capability on|off**

### **Mode**

Configure

### **Parameters**

|            |  |
|------------|--|
| <b>on</b>  | Turns on support for RFC 2370.                             |
| <b>off</b> | Turns off support for RFC 2370. This is the default value. |

### **Restrictions**

None.



# ospf set poll-interval

## Purpose

Sets the minimum number of seconds required between OSPF packets that the routers sends to establish neighbor adjacency.

## Format

**ospf set poll-interval** *<num>*

## Mode

Configure.

## Parameters

---

|                    |  |
|--------------------|--|
| <i>&lt;num&gt;</i> | Specify an interval from 0 to 255 seconds. The default is 120 seconds. |
|--------------------|--|

---

## Restrictions

None.

## Example

To set poll interval to 100 seconds:

|                                   |
|-----------------------------------|
| <b>ospf set poll-interval 100</b> |
|-----------------------------------|

## ospf set priority

### Purpose

Specifies the priority for becoming the Designated Router. When two routers attached to a network both attempt to become the designated router, the one with the higher priority wins. A router whose router priority is set to 0 is ineligible to become designated router.

### Format

**ospf set priority** *<num>*

### Mode

Configure.

### Parameters

---

*<num>*

Specify a number from 0 to 255. The default is 1.

---

### Restrictions

None.

### Example

To set priority to 10:

|                             |
|-----------------------------|
| <b>ospf set priority 10</b> |
|-----------------------------|

# ospf set retransmit-interval

## Purpose

Specifies the number of seconds between link state advertisement retransmissions for adjacencies.

## Format

**ospf set retransmit-interval** *<num>*

## Mode

Configure.

## Parameters

---

|                    |  |
|--------------------|--|
| <i>&lt;num&gt;</i> | Specify the number of seconds from 1 to 65535. The default is 5. |
|--------------------|--|

---

## Restrictions

None.

## Example

To set retransmit interval to 10 seconds:

|  |
|--|
| <b>ospf set retransmit-interval 10</b> |
|--|

## **ospf set rfc1583 on**

### **Purpose**

Specifies whether OSPF should be RFC 1583 compatible. Set this to on if all of the routers are not based on RFC 2328 or later. The default is off. Use the **no** command to disable support for RFC1583.

### **Format**

**ospf set rfc1583 on**

### **Mode**

Configure

### **Parameters**

None.

### **Restrictions**

None.

# ospf set router-dead-interval

## Purpose

Sets the number of seconds allowed between hello packets received from a neighbor before that neighbor is declared down.

## Format

**ospf set router-dead-interval** *<num>*

## Mode

Configure.

## Parameters

|                    |   |
|--------------------|---|
| <i>&lt;num&gt;</i> | Specify a value from 1 to 65535. The default is 4 times the hello-interval. |
|--------------------|---|

## Restrictions

None.

## Example

To set router dead interval to 20 seconds:

```
ospf set router-dead-interval 20
```

## ospf set transit-delay

### Purpose

Sets the estimated number of seconds required to transmit a link state update.

### Format

**ospf set transit-delay** *<num>*

### Mode

Configure.

### Parameters

---

*<num>*

Enter a value from 1 to 65535. The default delay is 1 second.

---

### Restrictions

None.

### Example

To set transit delay to 5 seconds:

|                                 |
|---------------------------------|
| <b>ospf set transit-delay 5</b> |
|---------------------------------|

# ospf set-trap

## Purpose

Enables or disables RFC1850 traps. All traps are enabled by default.

## Format

**ospf set-trap** [**all**] | [**none**] | [<trap\_name> **on**|**off**]

## Mode

Enable.

## Parameters

|             |  |
|-------------|--|
| <b>all</b>  | Selects all the traps.   |
| <b>none</b> | Deselects all the traps.   |
| <trap_name> | Select one or more of the following traps: <ul style="list-style-type: none"> <li>• ospfIfStateChange</li> <li>• ospfVirtIfStateChange</li> <li>• ospfNbrStateChange</li> <li>• ospfVirtNbrStateChange</li> <li>• ospfIfConfigError</li> <li>• ospfVirtIfConfigError</li> <li>• ospfIfAuthFailure</li> <li>• ospfVirtIfAuthFailure</li> <li>• ospfIfRxBadPacket</li> <li>• ospfVirtIfRxBadPacket</li> <li>• ospfTxRetransmit</li> <li>• ospfVirtIfTxRetransmit</li> <li>• ospfOriginateLsa</li> <li>• ospfMaxAgeLsa</li> </ul> |
| <b>on</b>   | Enables the selected traps.  |
| <b>off</b>  | Disables the selected traps.   |

**Note:** For a description of each trap, refer to RFC1850.

## Restrictions

None

## Example

To set Max Age LSA trap on:

|   |
|---|
| <code>ospf set-trap ospfMaxAgeLsa on</code> |
|---|



# ospf set virtual-link

## Purpose

Sets the parameters for an OSPF virtual link.

## Format

```
ospf set virtual-link <number-or-string> [no-multicast] [retransmit-interval <num>]
[transit-delay <num>] [priority <num>] [hello-interval <num>]
[router-dead-interval <num>] [poll-interval <num>] [key-chain <num-or-string>]
[authentication-method none| simple| md5] [passive] [advertise-subnet on|off]
```

## Mode

Configure.

## Parameters

|   |  |
|---|--|
| <b>&lt;number-or-string&gt;</b>                   | The identifier for this virtual link.  |
| <b>no-multicast</b>                               | Instructs the X-Pedition router to not send multicast packets to neighbors on point-to-point virtual links.  |
| <b>retransmit-interval</b><br><b>&lt;num&gt;</b>  | The number of seconds between link state advertisement retransmissions for adjacencies belonging to this virtual link. Specify a number equal to or greater than 1.  |
| <b>transit-delay</b> <b>&lt;num&gt;</b>           | The estimated number of seconds required to transmit a link state update over this virtual link. Transit delay takes into account transmission and propagation delays and must be greater than 0. Specify a number equal to or greater than 1.   |
| <b>priority</b> <b>&lt;num&gt;</b>                | A number between 0 and 255 specifying the priority for becoming the designated router on this virtual link. When two routers attached to a network both attempt to become the designated router, the one with the higher priority wins. A router whose router priority is set to 0 is ineligible to become designated router. Specify a number from 0 – 255. |
| <b>hello-interval</b> <b>&lt;num&gt;</b>          | The length of time, in seconds, between hello packets that the router sends on this virtual link. Specify a number from 0 – 255. The default is 60 seconds.  |
| <b>router-dead-interval</b><br><b>&lt;num&gt;</b> | The number of seconds not hearing a router's Hello packets before the router's neighbors will declare it down. Specify a number from 0 – 255. The default value for this parameter is 4 times the value of the <b>hello-interval</b> parameter.  |

|  |  |
|--|--|
| <b>poll-interval</b> <num>                   | Sets the minimum number of seconds required between OSPF packets that the router sends to establish neighbor adjacency. Specify a number from 0 – 255. The default is 120 seconds.   |
| <b>key-chain</b><br><num-or-string>          | The identifier of the key chain containing the authentication keys.  |
| <b>authentication-method</b> none simple md5 | <p>Specifies the authentication method used within the area. Specify one of the following:</p> <p><b>none</b> Do not associate an authentication method with this interface.</p> <p><b>simple</b> The authentication-method is a simple password in which an authentication key of up to 16 characters is included in the packet. If you choose this authentication method, you should also specify a key-chain identifier using the key-chain option.</p> <p><b>md5</b> Uses the MD5 algorithm to create a crypto-checksum of an OSPF packet and an authentication key of up to 16 characters. If you choose this authentication method, you should also specify a key-chain identifier using the key-chain option.</p> |
| <b>passive</b>                               | Specifies that an interface is not to receive or send packets on this interface. By default, the interface is non-passive.   |
| <b>advertise-subnet</b><br>on off            | Specifies whether this point-to-point interface should advertise itself as a subnet or host route. The default is off, where the interface advertises itself as a host route.  |

## Restrictions

None.

# ospf show

## Purpose

Show OSPF information.

## Format

**ospf show** *<option-list>*

## Mode

Enable.

## Parameters

*<option-list>* specifies the OSPF information to display. Specify one or more of the following:

|  |  |
|--|--|
| <b>all</b> [ <b>to-file</b>   <b>to-terminal</b> ] | Displays all OSPF tables.<br><b>to-file</b> Saves output in the file <b>/cfg/gated.dmp</b> <b>to-terminal</b> Displays output to the console (the default)   |
| <b>globals</b>                                     | Displays OSPF globals.   |
| <b>timers</b>                                      | Displays OSPF timers.  |
| <b>areas</b>                                       | Displays OSPF areas.   |
| <b>interfaces</b>                                  | Displays OSPF interfaces.  |
| <b>import-policies</b>                             | Displays OSPF import policies.   |
| <b>export-policies</b>                             | Displays OSPF export policies.   |
| <b>statistics</b> <i>&lt;interface&gt;</i>         | Displays OSPF statistics. Enter the interface address for the statistics you want to display. If you do not enter a specific interface address, the X-Pedition router will collect statistics for all interfaces.<br><br>The statistics for the ports specified will reinitialize if you add a previously removed interface to OSPF, add a previously removed area to OSPF (this reinitializes the statistics for that area's interfaces), create a previously removed interface, add a previously removed <b>ospf start</b> command, remove a previously added <b>ospf stop</b> command, or if you change the port status from “down” to “up.” To reset <i>all</i> port statistics, restart OSPF. |

|                              |   |                         |  |                          |   |                           |   |                              |  |                          |  |                         |  |                       |   |                         |   |
|------------------------------|---|-------------------------|--|--------------------------|---|---------------------------|---|------------------------------|--|--------------------------|--|-------------------------|--|-----------------------|---|-------------------------|---|
| <b>errors</b> <interface>    | Displays OSPF errors. Enter an interface address for which errors are displayed. If you do not enter a specific interface address, the X-Pedition router will collect errors for all interfaces.<br><br>The statistics for the ports specified will reinitialize if you add a previously removed interface to OSPF, add a previously removed area to OSPF (this reinitializes the statistics for that area's interfaces), create a previously removed interface, add a previously removed <b>ospf start</b> command, remove a previously added <b>ospf stop</b> command, or if you change the port status from “down” to “up.” To reset <i>all</i> port statistics, restart OSPF.   |                         |  |                          |   |                           |   |                              |  |                          |  |                         |  |                       |   |                         |   |
| <b>virtual-links</b>         | Displays OSPF virtual links.  |                         |  |                          |   |                           |   |                              |  |                          |  |                         |  |                       |   |                         |   |
| <b>as-external-ldsb</b>      | Displays OSPF Autonomous System External database entries.  |                         |  |                          |   |                           |   |                              |  |                          |  |                         |  |                       |   |                         |   |
| <b>lsa</b>                   | Displays the Link State Advertisement. This option requires the <b>Area-id</b> , <b>Adv_Rtr</b> , and <b>Type</b> . <table> <tr> <td><b>area-id</b> &lt;IPaddr&gt;</td><td>Specifies the OSPF area for which the query is directed.</td></tr> <tr> <td><b>type router-links</b></td><td>Request the router link advertisements that describe the collected states of the router interfaces. Ls-id is set to the originating router's router-id.</td></tr> <tr> <td><b>type network-links</b></td><td>Requests network link advertisements that describe the set of routers attached to the network. Ls-id is set to the IP interface address of the designated router for the network.</td></tr> <tr> <td><b>type summary-networks</b></td><td>Requests summary-link advertisements describing routes to networks. Ls-id is set to the IP address of the destination network.</td></tr> <tr> <td><b>type summary-asbr</b></td><td>Requests summary-link advertisements describing routes to AS boundary routers. Ls-id is set to the AS boundary router's router-id.</td></tr> <tr> <td><b>type as-external</b></td><td>Requests AS external link state advertisements. Ls-id is set to the IP address of the destination network.</td></tr> <tr> <td><b>ls-id</b> &lt;IPaddr&gt;</td><td>Specifies the ls-id for the type of link-state advertisement requested.</td></tr> <tr> <td><b>adv-rtr</b> &lt;IPaddr&gt;</td><td>Requests the router ID of the router that originated this link state advertisement.</td></tr> </table> | <b>area-id</b> <IPaddr> | Specifies the OSPF area for which the query is directed. | <b>type router-links</b> | Request the router link advertisements that describe the collected states of the router interfaces. Ls-id is set to the originating router's router-id. | <b>type network-links</b> | Requests network link advertisements that describe the set of routers attached to the network. Ls-id is set to the IP interface address of the designated router for the network. | <b>type summary-networks</b> | Requests summary-link advertisements describing routes to networks. Ls-id is set to the IP address of the destination network. | <b>type summary-asbr</b> | Requests summary-link advertisements describing routes to AS boundary routers. Ls-id is set to the AS boundary router's router-id. | <b>type as-external</b> | Requests AS external link state advertisements. Ls-id is set to the IP address of the destination network. | <b>ls-id</b> <IPaddr> | Specifies the ls-id for the type of link-state advertisement requested. | <b>adv-rtr</b> <IPaddr> | Requests the router ID of the router that originated this link state advertisement. |
| <b>area-id</b> <IPaddr>      | Specifies the OSPF area for which the query is directed.  |                         |  |                          |   |                           |   |                              |  |                          |  |                         |  |                       |   |                         |   |
| <b>type router-links</b>     | Request the router link advertisements that describe the collected states of the router interfaces. Ls-id is set to the originating router's router-id.   |                         |  |                          |   |                           |   |                              |  |                          |  |                         |  |                       |   |                         |   |
| <b>type network-links</b>    | Requests network link advertisements that describe the set of routers attached to the network. Ls-id is set to the IP interface address of the designated router for the network.   |                         |  |                          |   |                           |   |                              |  |                          |  |                         |  |                       |   |                         |   |
| <b>type summary-networks</b> | Requests summary-link advertisements describing routes to networks. Ls-id is set to the IP address of the destination network.  |                         |  |                          |   |                           |   |                              |  |                          |  |                         |  |                       |   |                         |   |
| <b>type summary-asbr</b>     | Requests summary-link advertisements describing routes to AS boundary routers. Ls-id is set to the AS boundary router's router-id.  |                         |  |                          |   |                           |   |                              |  |                          |  |                         |  |                       |   |                         |   |
| <b>type as-external</b>      | Requests AS external link state advertisements. Ls-id is set to the IP address of the destination network.  |                         |  |                          |   |                           |   |                              |  |                          |  |                         |  |                       |   |                         |   |
| <b>ls-id</b> <IPaddr>        | Specifies the ls-id for the type of link-state advertisement requested.   |                         |  |                          |   |                           |   |                              |  |                          |  |                         |  |                       |   |                         |   |
| <b>adv-rtr</b> <IPaddr>      | Requests the router ID of the router that originated this link state advertisement.   |                         |  |                          |   |                           |   |                              |  |                          |  |                         |  |                       |   |                         |   |
| <b>routes</b>                | Displays OSPF routes.   |                         |  |                          |   |                           |   |                              |  |                          |  |                         |  |                       |   |                         |   |
| <b>enabled-traps</b>         | Displays enabled OSPF traps.  |                         |  |                          |   |                           |   |                              |  |                          |  |                         |  |                       |   |                         |   |

|  |   |
|--|---|
| <b>neighbors</b>   | Displays OSPF neighbors.  |
| <b>lsdb area</b><br><IPaddr>  <b>backbone</b>   <b>all</b> | Display OSPF Link State Database for a specific area by specifying the IP address, for the <b>backbone</b> area, or for <b>all</b> areas. |

## Restrictions

None.

## **ospf start|stop**

### **Purpose**

Start or stop the OSPF protocol. OSPF is disabled by default on the X-Pedition router.

### **Format**

**ospf start|stop**

### **Mode**

Configure.

### **Parameters**

|              |              |
|--------------|--------------|
| <b>start</b> | Starts OSPF. |
| <b>stop</b>  | Stops OSPF.  |

### **Restrictions**

None.

# ospf trace

## Purpose

Trace OSPF.

## Format

```
ospf trace [spf| debug| packets {detail| send| receive} |  
hello {detail| send| receive} |  
dd {detail| send| receive} |  
request {detail| send| receive} |  
update {detail| send| receive} |  
ack {detail| send| receive} |  
local-options [all| general| state| normal| policy| task| timer| route| none] |  
ospf-state |  
dr-election |  
db |  
flood]
```

## Mode

Enable and Configure.

## Parameters

|                |   |
|----------------|---|
| <b>spf</b>     | Traces Shortest Path First (SPF) calculations.  |
| <b>debug</b>   | Traces OSPF at the debugging level of detail.   |
| <b>packets</b> | Traces OSPF packets.<br><b>detail</b> Show detailed information about packets.<br><b>send</b> Show OSPF packets sent by the router.<br><b>receive</b> Show OSPF packets received by the router.   |
| <b>hello</b>   | Traces OSPF HELLO packets used to determine neighbor reachability.<br><b>detail</b> Show detailed information about hello packets.<br><b>send</b> Show OSPF hello packets sent by the router.<br><b>receive</b> Show OSPF hello packets received by the router. |

|                      |   |
|----------------------|---|
| <b>dd</b>            | Traces OSPF Database Description packets used in synchronizing OSPF databases.<br><b>detail</b> Show detailed information about database description packets.<br><b>send</b> Show OSPF database description packets sent by the router.<br><b>receive</b> Show OSPF database description packets received by the router.  |
| <b>request</b>       | Traces OSPF Link State Request packets used in synchronizing OSPF databases.<br><b>detail</b> Show detailed information about Link State Request packets.<br><b>send</b> Show OSPF Link State Request packets sent by the router.<br><b>receive</b> Show OSPF Link State Request packets received by the router.  |
| <b>update</b>        | Traces OSPF Link State Update packets used in synchronizing OSPF databases.<br><b>detail</b> Show detailed information about Link State Update packets.<br><b>send</b> Show OSPF Link State Update packets sent by the router.<br><b>receive</b> Show OSPF Link State Update packets received by the router.  |
| <b>ack</b>           | Traces OSPF Link State Acknowledgements:<br><b>detail</b> Show detailed information about link state acknowledgements.<br><b>send</b> Show link state acknowledgements sent by the router.<br><b>receive</b> Show link state acknowledgements received by the router.   |
| <b>local-options</b> | Sets various trace options for this protocol only. By default, these trace-options are inherited from those specified by the <b>ip-router global set trace-options</b> command.<br><b>all</b> Turns on all tracing.<br><b>general</b> Turns on normal and route tracing.<br><b>state</b> Traces state machine transitions.<br><b>normal</b> Traces normal OSPF occurrences—abnormal OSPF occurrences are always traced.<br><b>policy</b> Traces application of OSPF and user-specified policy to routes being imported and exported.<br><b>task</b> Traces system interface and processing.<br><b>timer</b> Traces timer usage.<br><b>route</b> Traces routing table changes for routes installed.<br><b>none</b> All tracing should be turned off. |
| <b>ospf-state</b>    | Traces changes in OSPF states.  |
| <b>dr-election</b>   | Traces Designated Router elections.   |
| <b>db</b>            | Traces link state database changes.   |
| <b>flood</b>         | Traces OSPF flooding.   |



## Restrictions

Users must add the following CLI command(s) in order for tracing to work. From Enable mode:

```
xp# ip-router set trace-state on
```

From Configure mode:

```
xp(config)# ip-router global set trace-state on
```



# Chapter 48

## pim Commands

The **pim** commands allow you to dynamically build a distribution tree for forwarding multicast data on a network. For detailed information about the use of PIM (Protocol Independent Multicast), consult the *Enterasys X-Pedition User Reference Manual*.

The X-Pedition router does not allow users to enable DVMRP and PIM-SM simultaneously. If a user attempts to enable DVMRP and PIM-SM at the same time, one of the following messages will appear:

- %CLI-E-NODVMRPFAC, This command cannot be used when PIM-SM has been configured.
- %CLI-E-NOPIMFAC, This command cannot be used when IGMP or DVMRP has been configured.

To switch between PIM-SM and DVMRP you must remove the protocol's start command from the startup configuration and restart the router.

## Command Summary

[Table 42](#) lists the **pim** commands. The sections following the table describe the command syntax.

**Table 42. pim Commands**

|   |
|---|
| <b>pim global start  stop</b>   |
| <b>pim global set defaults [hello-interval &lt;sec&gt;] [hello-holdtime &lt;sec&gt;] [hello-priority &lt;sec&gt;] [mrt-stale-mult &lt;num&gt;] [mrt-period &lt;sec&gt;] [assert-holdtime &lt;sec&gt;] [jp-interval &lt;sec&gt;] [jp-holdtime &lt;sec&gt;]</b> |
| <b>pim global trace packets  hello  register  bootstrap  jp  assert [detail] [send] [receive]</b>   |
| <b>pim global trace local-options</b>   |
| <b>pim show active-rps [to-terminal  to-file]</b>   |

Table 42. pim Commands (Continued)

|  |
|--|
| <b>pim show all</b> [to-terminal  to-file]   |
| <b>pim show bsr</b> [to-terminal  to-file]   |
| <b>pim show crp</b> [to-terminal  to-file]   |
| <b>pim show errors</b> [to-terminal  to-file]  |
| <b>pim show interface all</b> <IP_address> [to-terminal  to-file]  |
| <b>pim show neighbor all</b> <IP_address> [to-terminal  to-file]   |
| <b>pim show periodic-jp</b> [to-terminal  to-file]   |
| <b>pim show route</b> [all] [detail] [source <IP_address>] [group <IP_address>] [to-terminal  to-file]   |
| <b>pim show rp-hash</b> [to-terminal  to-file]   |
| <b>pim show rp-set</b> [to-terminal  to-file]  |
| <b>pim show timers</b> [to-terminal  to-file]  |
| <b>pim sparse add crp-group</b> <IP-addr-netmask> <b>to-component</b> <name> [priority <num>]  |
| <b>pim sparse add interface</b> <intf> <b>to-component</b> <name>  |
| <b>pim sparse add static-rp</b> <IP-addr> <b>group</b> <IP-addr> <b>to-component</b> <name>  |
| <b>pim sparse create component</b> <name>  |
| <b>pim sparse set component</b> [bsr-on  bsr-off] bsr-address <IP-addr> [bsr-period <sec>] [bsr-priority <num>] [bsr-timeout <sec>] [crp-on  crp-off] crp-address <IP-addr> [crp-adv-period <sec>] [crp-priority <num>] [crp-holdtime <sec>] [threshold <num>] [threshold-dr <num>] [threshold-rp <num>] [reg-sup-timeout <sec>] [probe-period <sec>] [mrt-spt-mult <num>] |
| <b>pim sparse set interface</b> [boundary] [hello-interval <sec>] [hello-holdtime <sec>] [hello-priority <sec>] [assert-holdtime <sec>] [jp-interval <sec>] [jp-holdtime <sec>]  |

# pim global

## Purpose

Start and stop pim protocol processing.

## Format

**pim global start| stop**

## Mode

Configure.

## Description

The **pim global** command allows you to enable and disable PIM protocol processing. PIM will not operate until you enable it.

## Parameters

|              |                               |
|--------------|-------------------------------|
| <b>start</b> | Start pim protocol processing |
| <b>stop</b>  | Stop pim protocol processing  |

## Restrictions

The X-Pedition router does not allow users to enable DVMRP and PIM-SM simultaneously. If a user attempts to enable DVMRP and PIM-SM at the same time, one of the following messages will appear:

- %CLI-E-NODVMRPFAC, This command cannot be used when PIM-SM has been configured.
- %CLI-E-NOPIMFAC, This command cannot be used when IGMP or DVMRP has been configured.

To switch between PIM-SM and DVMRP you must remove the protocol's start command from the startup configuration and restart the router.

**Note:** If a user is running one of the multicast protocols and tries to activate the second protocol, an appropriate error message is displayed and the second protocol is not activated. However, the new configuration is entered into the configuration file without it being marked as being in error.

## pim global set defaults

### Purpose

Specify defaults to apply to all PIM packets.

### Format

```
pim global set defaults [hello-interval <sec>] [hello-holdtime <sec>] [hello-priority <sec>]  
[mrt-stale-mult <num>] [mrt-period <sec>] [assert-holdtime <sec>] [jp-interval <sec>]  
[jp-holdtime <sec>]
```

### Mode

Configure.

### Description

The **pim global set defaults** command allows you to apply specific limitations and values to all PIM packets and multicast routing tables.

### Parameters

|                         |   |
|-------------------------|---|
| [hello-interval <sec>]  | The length of time (in seconds) between hello packets that the router sends on its interfaces. By default, the interval is <b>30</b> seconds.   |
| [hello-holdtime <sec>]  | The length of time (in seconds) that neighbors should wait for hello messages before expiring this router as a neighbor. A value of 65535 specifies that this router should never timeout as a neighbor. By default, the hold time is <b>105</b> seconds. |
| [hello-priority <sec>]  | The priority for becoming Designated Router (DR) on a multiaccess network.  |
| [mrt-stale-mult <num>]  | The number of times to examine the multicast routing table ( <i>MRT</i> ) before removing a stale entry. By default, the number of examination times is <b>14</b> .   |
| [mrt-period <sec>]      | The number of seconds (since the last examination) to wait before examining the MRT for dead (S,G) entries (i.e., entries whose downstream list is null). The default is 15 seconds.  |
| [assert-holdtime <sec>] | The number of seconds between the time an assert is received and the time at which the assert is timed out. The default is 180 seconds.   |
| [jp-interval <sec>]     | The number of seconds between transmissions of a Join/Prune message. The default is <b>60</b> seconds.  |

---

|                                  |  |
|----------------------------------|--|
| <b>[jp-holdtime &lt;sec&gt;]</b> | The Join/Prune hold time advertised in PIM Join/Prune messages. Receivers must wait at least this long after receiving a Join/Prune message before deleting the Join/Prune state associated with the advertiser. The recommended value is <b>3.5 * jp-interval</b> . The default is 210 seconds. |
|----------------------------------|--|

---

## Restrictions

Applies to all interfaces configured for PIM. To set defaults for a specific interface, see [pim sparse set interface on page 816](#).

## Example

To increase the duration between hello messages sent from this router to 60 seconds, enter the following:

```
xp(config)# pim global set hello-interval 60
```

# pim global trace

## Purpose

Trace all PIM, Hello, Register, Register Stop, Bootstrap, Join/Prune, and Assert packets.

## Format

**pim global trace** **packets**| **hello**| **register**| **bootstrap**| **jp**| **assert** [**detail**] [**send**] [**receive**]

## Mode

Configure.

## Description

The **pim global trace** command allows you to trace PIM packet processing. When the X-Pedition router sends or receives a packet, the router displays a message to the console.

## Parameters

|                    |  |
|--------------------|--|
| <b>packets</b>     | Trace all PIM packets.                                 |
| <b>hello</b>       | Trace Hello packets.                                   |
| <b>register</b>    | Trace Register and Register Stop packets.              |
| <b>bootstrap</b>   | Trace Bootstrap packets.                               |
| <b>jp</b>          | Trace Join/Prune packets.                              |
| <b>assert</b>      | Trace Assert packets.                                  |
| [ <b>detail</b> ]  | Show a detailed trace message instead of a brief one.  |
| [ <b>send</b> ]    | Show only those packets that are sent from the router. |
| [ <b>receive</b> ] | Show only those packets received by the router.        |

## Restrictions

Specify each trace target separately. Instead of **pim global trace register jp detail send**, use **pim global trace register detail send** and **pim global trace jp detail send**.



## Example

To trace sent and received hello messages, enter the following

```
xp(config)# pim global trace hello
```

# pim global trace local-options

## Purpose

Sets various trace options for this protocol only. By default, these trace-options are inherited from those specified by the **ip-router global set trace-options** command.

## Format

**pim global trace local-options debug | all | general | state | normal | policy | task | timer | route | none**

## Mode

Configure.

## Description

The **pim global trace local-options** command allows you to trace PIM-specific messages for those options specified by **ip-router global set trace-options**. See [ip-router global set trace-options on page 500](#) for details.

## Parameters

|                |   |
|----------------|---|
| <b>debug</b>   | Enable developer debugging options for trace.   |
| <b>all</b>     | Turn on all tracing.  |
| <b>general</b> | Turn on normal and route tracing.   |
| <b>state</b>   | Traces state machine transitions in protocols.  |
| <b>normal</b>  | Traces normal protocol occurrences. The X-Pedition router always traces abnormal occurrences. |
| <b>policy</b>  | Traces the application of policy to imported and exported routes.                             |
| <b>task</b>    | Traces system interfaces and task processing associated with this protocol or peer.           |
| <b>timer</b>   | Traces timer usage by this protocol or peer.  |
| <b>route</b>   | Traces routing table changes for routes installed by this protocol or peer.                   |
| <b>none</b>    | Specifies that all tracing should be turned off for this protocol or peer.                    |

## Restrictions

None.

## Example

```
xp(config)# pim global trace local-options timer
```

# pim show active-rps

## Purpose

View active group addresses and the RP that hashes to them.

## Format

**pim show active-rps** [**to-terminal**| **to-file**]

## Mode

Enable.

## Description

The **pim show active-rps** command allows you to display a list of active group addresses (i.e., groups that currently have membership information) and the RP that hashes to that group.

## Parameters

|                    |  |
|--------------------|--|
| <b>to-terminal</b> | Displays the information on screen. If you do not specify how to output the information, the X-Pedition router will select the to-terminal option (the default). |
| <b>to-file</b>     | Writes the information to the gated dump file.   |

## Restrictions

None.

## Examples

To display the active group addresses and RP hashing information on screen, enter the following:

```
xp(enable)# pim show active-rps to-terminal
```

To write the active group addresses and RP hashing information to the gated dump file, enter the following:

```
xp(enable)# pim show active-rps to-file
```

# pim show all

## Purpose

Display all PIM-related information.

## Format

**pim show all** [**to-terminal**| **to-file**]

## Mode

Enable.

## Description

The **pim show all** command allows you to display all interfaces, neighbors, routes, bsrs, crps, active-rps, periodic-jps, and errors.

## Parameters

|                    |  |
|--------------------|--|
| <b>to-terminal</b> | Displays the information on screen. If you do not specify how to output the information, the X-Pedition router will select the to-terminal option (the default). |
| <b>to-file</b>     | Writes the information to the gated dump file.   |

## Restrictions

None.

## Examples

To display all pim information on screen, enter the following:

```
xp(enable)# pim show all to-terminal
```

To write all pim information to the gated dump file, enter the following:

```
xp(enable)# pim show all to-file
```

# pim show bsr

## Purpose

Display information about the elected BSR and its priority.

## Format

**pim show bsr** [**to-terminal**| **to-file**]

## Mode

Enable.

## Description

The **pim show bsr** command allows you to display the elected BSR and its priority. If the router is a C-BSR, this command will display the advertised address and priority.

## Parameters

|                    |  |
|--------------------|--|
| <b>to-terminal</b> | Displays the information on screen. If you do not specify how to output the information, the X-Pedition router will select the to-terminal option (the default). |
| <b>to-file</b>     | Writes the information to the gated dump file.   |

## Restrictions

None.

## Examples

To display bsr information on screen, enter the following:

```
xp(enable)# pim show bsr
```

To write bsr information to the gated dump file, enter the following:

```
xp(enable)# pim show bsr to-file
```

# pim show crp

## Purpose

Display advertised address and priority of a C-RP.

## Format

**pim show crp** [to-terminal| to-file]

## Mode

Enable.

## Description

If the current router is configured to be a C-RP, the **pim show crp** command displays the router's advertised address and priority.

## Parameters

|                    |  |
|--------------------|--|
| <b>to-terminal</b> | Displays the information on screen. If you do not specify how to output the information, the X-Pedition router will select the to-terminal option (the default). |
| <b>to-file</b>     | Writes the information to the gated dump file.   |

## Restrictions

None.

## Examples

To display the C-RP advertised address and priority on screen, enter the following:

```
xp(enable)# pim show crp to-terminal
```

To write the C-RP advertised address and priority to the gated dump file, enter the following:

```
xp(enable)# pim show crp to-file
```

# pim show errors

## Purpose

Display the count of bad PIM messages.

## Format

**pim show errors** [**to-terminal**| **to-file**]

## Mode

Enable.

## Description

Display the count of bad Hello and BSR messages.

## Parameters

|                    |  |
|--------------------|--|
| <b>to-terminal</b> | Displays the information on screen. If you do not specify how to output the information, the X-Pedition router will select the to-terminal option (the default). |
| <b>to-file</b>     | Writes the information to the gated dump file.   |

## Restrictions

None.

## Example

To display the bad message count on screen, enter the following:

```
xp(enable)# pim show errors to-terminal
```

To write the bad message count to the gated dump file, enter the following:

```
xp(enable)# pim show errors to-file
```



# pim show interface

## Purpose

Display all interfaces or a specific interface configured to use PIM.

## Format

**pim show interface all** | *<IP\_address>* [**to-terminal** | **to-file**]

## Mode

Enable.

## Description

Display all interfaces or a specific interface (by address) configured to use PIM protocol, along with the configured values for the interface, the neighbor count, and the elected DR.

## Parameters

|                           |  |
|---------------------------|--|
| <b>all</b>                | Show all PIM interfaces.                       |
| <i>&lt;IP_address&gt;</i> | Show a specific PIM interface.                 |
| <b>to-terminal</b>        | Displays the information on the terminal.      |
| <b>to-file</b>            | Writes the information to the gated dump file. |

## Restrictions

None.

## Examples

To display on screen all interfaces configured to use PIM, enter the following:

```
xp(enable)# pim show interface all to-terminal
```

To write the a specific interface configured to use PIM to the gated dump file, enter the following:

```
xp(enable)# pim show interface 10.136.64.5 to-file
```

# pim show neighbor

## Purpose

Display information about PIM-configured neighbors.

## Format

**pim show neighbor all** | *<IP\_address>* [**to-terminal** | **to-file**]

## Mode

Enable.

## Description

Display a neighbor (or all neighbors) by address, the interface it belongs to, how long it has been active, when it expires, and its DR priority.

## Parameters

|                           |  |
|---------------------------|--|
| <b>all</b>                | Show all PIM neighbors.  |
| <i>&lt;IP_address&gt;</i> | Show a specific PIM neighbor.  |
| <b>to-terminal</b>        | Displays the information on screen. If you do not specify how to output the information, the X-Pedition router will select the to-terminal option (the default). |
| <b>to-file</b>            | Writes the information to the gated dump file.   |

## Restrictions

None.

## Example

To display information on screen about a specific neighbor, enter the following:

```
xp(enable)# pim show neighbor 10.136.64.5 to-terminal
```

To write information about all neighbors to the gated dump file, enter the following:

```
xp(enable)# pim show neighbor all to-file
```

# pim show periodic-jp

## Purpose

Show pending PIM-SM join/prune message information.

## Format

**pim show periodic-jp [to-terminal| to-file]**

## Mode

Enable.

## Description

Display a list of pending joins and prunes and when the next series will be sent.

## Parameters

|                    |  |
|--------------------|--|
| <b>to-terminal</b> | Displays the information on screen. If you do not specify how to output the information, the X-Pedition router will select the to-terminal option (the default). |
| <b>to-file</b>     | Writes the information to the gated dump file.   |

## Restrictions

None.

## Example

To display the list of joins and prunes on screen, enter the following:

```
xp(enable)# pim show periodic-jp to-terminal
```

To write the list of joins and prunes to the gated dump file, enter the following:

```
xp(enable)# pim show periodic-jp to-file
```

# pim show route

## Purpose

Display multicast route information.

## Format

```
pim show route [all] [detail] [source <IP_address>] [group <IP_address>]  
[to-terminal| to-file]
```

## Mode

Enable.

## Description

Display multicast route information (with or without detail) for a route. Information includes the inbound interface, outbound interfaces, and flags for that route. Routes may specify a source-group pair (**source** <IP\_address> **group** <IP\_address>), all routes for a group (**group** <IP\_address>), all routes for a source (**source** <IP\_address>), or all active routes (**all**).

## Parameters

|                                 |  |
|---------------------------------|--|
| <b>[all]</b>                    | List all active PIM group routes and (S,G) routes.   |
| <b>[detail]</b>                 | Provide detailed information about PIM group routes and (S,G) routes.  |
| <b>[source</b><br><IP_address>] | Display information about a specific source. Requires <b>group</b> <IP address>.   |
| <b>[group</b><br><IP_address>]  | Display information about a specific group.  |
| <b>to-terminal</b>              | Displays the information on screen. If you do not specify how to output the information, the X-Pedition router will select the to-terminal option (the default). |
| <b>to-file</b>                  | Writes the information to the gated dump file.   |

## Restrictions

None.

## Example

To display basic multicast route information on screen for a specific group, enter the following:

```
xp(enable)# pim show route group 229.0.65.6 to-terminal
```

To write detailed multicast route information for all routes to the gated dump file, enter the following:

```
xp(enable)# pim show route all detail to-file
```

To display multicast route information on screen for a source-group pair, enter the following:

```
xp(enable)# pim show route source 10.136.64.7 group 229.0.65.6
```

# pim show rp-hash

## Purpose

Display a group-to-RP mapping.

## Format

**pim show rp-hash** <IP\_address / netmask> [to-terminal| to-file]

## Mode

Enable.

## Description

Display a group-to-RP mapping for a group and mask.

## Parameters

|                        |  |
|------------------------|--|
| <IP_address / netmask> | The IP address and netmask of the group whose information you will view.   |
| <b>to-terminal</b>     | Displays the information on screen. If you do not specify how to output the information, the X-Pedition router will select the to-terminal option (the default). |
| <b>to-file</b>         | Writes the information to the gated dump file.   |

## Restrictions

None.

## Example

To display all group-to-rp mappings to the terminal, enter the following:

```
xp(enable)# pim show rp-hash 224.0.0.0/4
```

To write all group-to-rp mappings for the range 229.0.65.6 to 255.255.255.0 to the gated dump file, enter the following:

```
xp(enable)# pim show rp-hash 229.0.65.6 to 255.255.255.0 to-file
```

# pim show rp-set

## Purpose

Show set of PIM-SM RP mappings.

## Format

**pim show rp-set [to-terminal| to-file]**

## Mode

Enable.

## Description

Display list of group-to-RP mappings received from the BSR.

## Parameters

|                    |  |
|--------------------|--|
| <b>to-terminal</b> | Displays the information on screen. If you do not specify how to output the information, the X-Pedition router will select the to-terminal option (the default). |
| <b>to-file</b>     | Writes the information to the gated dump file.   |

## Restrictions

None.

## Example

To display a list of received group-to-RP mappings on screen, enter the following:

```
xp(enable)# pim show rp-set to-terminal
```

To write the list of received group-to-RP mappings to the gated dump file, enter the following:

```
xp(enable)# pim show rp-set to-file
```

# pim show timers

## Purpose

Display PIM protocol timer values.

## Format

**pim show timers [to-terminal| to-file]**

## Mode

Enable.

## Description

The **pim show timers** command allows you to display values for PIM protocol timers.

## Parameters

|                    |  |
|--------------------|--|
| <b>to-terminal</b> | Displays the information on screen. If you do not specify how to output the information, the X-Pedition router will select the to-terminal option (the default). |
| <b>to-file</b>     | Writes the information to the gated dump file.   |

## Restrictions

None.

## Examples

To display timer values on screen, enter the following:

```
xp(enable)# pim show timers to-terminal
```

To write timer values to the gated dump file, enter the following:

```
xp(enable)# pim show timers to-file
```



# pim sparse add crp-group

## Purpose

Specifies a range of multicast addresses for which the router will attempt to become the RP.

## Format

**pim sparse add crp-group** <IP-addr-netmask> **to-component** <name> [**priority** <num>]

## Mode

Configure.

## Description

Specifies a range of multicast addresses for which the router will attempt to become the RP. If the router is not eligible to be a CRP, you may not use this option. If you specify crp-on but do not select a group, the router will be a CRP for 224/4.

## Parameters

|                               |  |
|-------------------------------|--|
| <IP-addr-netmask>             | The name of the group address and netmask. |
| <b>to-component</b><br><name> | The name of the PIM-SM component.          |
| [ <b>priority</b> <num>]      | The priority level assigned to the C-RP.   |

## Restrictions

You must enter the following syntax before using this command.

```
xp(config)# pim sparse set component crp-on| crp-address <IPaddr>
```

## Example

To configure the router as a crp for groups in the range 228.160.x.x - 228.160/12, use the following syntax:

```
xp(config)# pim sparse add crp-group 228.160/12 to-component nyc3
```

# pim sparse add interface

## Purpose

Associates an interface with the PIM sparse component.

## Format

**pim sparse add interface** <intf> **to-component** <name>

## Mode

Configure.

## Description

The **pim sparse add interface** command allows you to enable PIM protocol processing on a specific interface.

## Parameters

|                               |                                   |
|-------------------------------|-----------------------------------|
| <b>interface</b> <intf>       | The interface you will activate.  |
| <b>to-component</b><br><name> | The name of the PIM-SM component. |

## Restrictions

None.

## Example

To enable sparse mode on interface *foo* and add it to component *nyc3*, enter the following:

```
xp(config)# pim sparse add interface foo to-component nyc3
```

# pim sparse add static-rp

## Purpose

Adds a static RP-mapping to the component specified.

## Format

**pim sparse add static-rp** <IP-addr> **group** <IP-addr> **to-component** <name>

## Mode

Configure.

## Description

The **pim sparse add static-rp** command allows you to add a static RP-mapping to the component specified. The multicast address listed will serve a specific group.

## Parameters

|                                     |   |
|-------------------------------------|---|
| <IP_address>                        | The IP address of the port you will assign as the RP.         |
| <b>group</b> <IP_address / netmask> | The address and netmask of the group that will map to the RP. |
| <b>to-component</b> <name>          | The name of the PIM-SM component.                             |

## Restrictions

The group IP address must be a valid multicast IP address.

## Example

To set 172.16.15.3 as an RP for 226.3.3.3/32, enter the following:

```
xp(config)# pim sparse add static-RP 172.16.15.3 group 226.3.3.3/32 to-component nyc3
```

# pim sparse create component

## Purpose

Creates a PIM component.

## Format

**pim sparse create component** *<name>*

## Mode

Configure.

## Description

The **pim sparse create component** command allows you to create a PIM component—a grouping that allows you to specify certain settings for one or more interfaces. You must define a sparse component to run PIM-SM.

## Parameters

---

|                                      |                                     |
|--------------------------------------|-------------------------------------|
| <b>component</b> <i>&lt;name&gt;</i> | The name assigned to the component. |
|--------------------------------------|-------------------------------------|

---

## Restrictions

You may specify only one component on the router.

## Example

To run sparse mode and create a component, enter the following:

```
xp(config)# pim sparse create component nyc3
```

# pim sparse set component

## Purpose

Sets values for a sparse-mode component.

## Format

```
pim sparse set component [bsr-on| bsr-off] bsr-address <IP-addr>] [bsr-period <sec>]
[bsr-priority <num>] [bsr-timeout <sec>] [crp-on| crp-off] crp-address <IPaddr>]
[crp-adv-period <sec>] [crp-priority <num>] [crp-holdtime <sec>] [threshold <num>]
[threshold-dr <num>] [threshold-rp <num>] [reg-sup-timeout <sec>] [probe-period <sec>]
[mrt-spt-mult <num>]
```

## Mode

Configure.

## Description

The **pim sparse set component** command allows you to set sparse-mode-specific values to use on the router.

## Parameters

|                                 |   |
|---------------------------------|---|
| <b>bsr-on</b>                   | Allows router to be a candidate bootstrap router (BSR). You may select this option <i>only once</i> on any router.  |
| <b>bsr-off</b>                  | Prevent the router from becoming the BSR (default).   |
| <b>bsr-address</b><br><IP-addr> | The address to advertise as the BSR—the largest IP configured on the router (unless specifically stated otherwise). This option nullifies bsr-off and automatically selects bsr-on (i.e., if you set this option, you do not need to set bsr-on). |
| <b>bsr-period</b> <sec>         | The length of time (in seconds) between originating bootstrap messages. The default value for this option is 60 seconds.  |
| <b>bsr-priority</b> <num>       | BSRs with higher priorities are preferred. If two routers share the same priority, the one with the larger advertised address wins. The default priority value is 0.  |
| <b>bsr-timeout</b> <sec>        | The length of time (in seconds) that neighbors should wait for bootstrap messages before assuming this router is unreachable. The default is 130 seconds.   |
| <b>crp-on</b>                   | Allows the router to be a candidate rendezvous point (RP).  |

|                                 |  |
|---------------------------------|--|
| <b>crp-off</b>                  | Prevents the router from becoming the RP for any group.  |
| <b>crp-address</b><br><IPaddr>  | The address advertised by the BSR is the largest IP configured on the router (unless specifically stated otherwise). This option nullifies crp-off and automatically selects crp-on (i.e., if you set this option, you do not need to set crp-on.)   |
| <b>crp-adv-period</b><br><sec>  | The length of time (in seconds) between originating CRP advertisement messages. The default value for this option is 60 seconds.   |
| <b>crp-priority</b> <num>       | CRPs with lower priorities are preferred. If two routers share the same priority, the one with the larger advertised address wins. Any group that does not have a priority assigned to it will use this priority. If you do not specify any groups, this priority will be used for 224/4.  |
| <b>crp-holdtime</b> <sec>       | The length of time (in seconds) the BSR should use to time out CRP-Adv messages. The default is 150 seconds.   |
| <b>threshold</b> <num>          | The rate of traffic (in bytes/sec) to reach when either the DR (designated router) or the RP (rendezvous point) will switch to a shortest path tree. The default is 0 bytes/sec.   |
| <b>threshold-dr</b> <num>       | The rate of traffic (in bytes/sec) to reach when the DR (designated router) will switch to a shortest path tree. The default is 0 bytes/sec. When using the default value of zero, the DR will attempt to switch to the SPT when it receives the first packet.   |
| <b>threshold-rp</b> <num>       | The rate of traffic (in bytes/sec) to reach when the RP (rendezvous point) will switch to a shortest path tree. The default is 0 bytes/sec. When using the default value of zero, the RP will attempt to switch to the SPT when it receives the first packet.  |
| <b>reg-sup-timeout</b><br><sec> | <p>The mean number of seconds between receiving a register-stop message and sending registers again. A low value indicates more frequent bursts at the RP. A high value indicates a longer join latency for new receivers. The default is 60 seconds.</p> <p><b>Note:</b> You may lower the timeout value if you send null register messages <i>n</i> seconds (where <i>n</i> is specified in probe-period) before the timer expires. This prevents register bursts.</p> |
| <b>probe-period</b> <sec>       | When you use null register messages, you can specify the number of seconds before the register-suppression timer expires to send a null register message. If a router receives a register-stop message before sending the null register message, the register-suppression timer will reset and delay sending the null register message.  |
| <b>mrt-spt-mult</b><br><num>    | The number of times to examine the MRT before trying a switch. The MRT is examined every <b>mrt-period</b> seconds (set in <a href="#">pim global set defaults on page 790</a> ).  |

## Restrictions

None.

## Examples

To enable a router as a C-BSR, enter the following:

```
xp(config)# pim sparse set component nyc3 bsr-on
```

To set component nyc3 with a specific bsr-address (172.16.3.5), enter the following:

```
xp(config)# pim sparse set component nyc3 bsr-address 172.16.3.5
```

To enable a router as a C-RP, enter the following:

```
xp(config)# pim sparse set component nyc3 crp-on
```

To set the switching threshold for the router functioning as an RP to switch to a shortest path tree once traffic flow reaches 200 bytes/sec, enter the following:

```
xp(config)# pim sparse set component nyc3 threshold-rp 200
```

To set the router functioning as a DR to switch to a shortest path tree immediately, use the following:

```
xp(config)# pim sparse set component nyc3 threshold-dr 0
```

# pim sparse set interface

## Purpose

Sets interface-specific options for PIM-sparse.

## Format

```
pim sparse set interface [boundary] [hello-interval <sec>] [hello-holdtime <sec>]  
[hello-priority <sec>] [assert-holdtime <sec>] [jp-interval <sec>] [jp-holdtime <sec>]
```

## Mode

Configure.

## Description

This command sets interface-specific options for PIM-sparse. See [pim global set defaults on page 790](#) for definitions of these options.

## Parameters

|                         |  |
|-------------------------|--|
| [boundary]              | Specifies whether the router will be a multicast border router on this interface. BSR messages do not propagate through a boundary interface.  |
| [hello-interval <sec>]  | The length of time (in seconds) between hello packets that the router sends on its interfaces. By default, the interval is <b>30</b> seconds.  |
| [hello-holdtime <sec>]  | The length of time (in seconds) that neighbors should wait for hello messages before expiring this router as a neighbor. A value of 65535 specifies that this router should never timeout as a neighbor. By default, the hold time is <b>105</b> seconds.  |
| [hello-priority <sec>]  | The priority for becoming Designated Router (DR) on a multiaccess network.   |
| [assert-holdtime <sec>] | The number of seconds between the time an assert is received and the time at which the assert is timed out. The default is <b>180</b> seconds.   |
| [jp-interval <sec>]     | The number of seconds between transmissions of a Join/Prune message. The default is <b>60</b> seconds.   |
| [jp-holdtime <sec>]     | The Join/Prune hold time advertised in PIM Join/Prune messages. Receivers must wait at least this long after receiving a Join/Prune message before deleting the Join/Prune state associated with the advertiser. The recommended value is <b>3.5 * jp-interval</b> . The default is 210 seconds. |



## Restrictions

None.

## Example

To increase the duration between hello messages sent from this router to 60 seconds, enter the following:

```
xp(config)# pim sparse set hello-interval 60
```



# Chapter 49

## ping Command

This chapter describes the **ping** command.

### ping

#### Purpose

Test connections between the X-Pedition router and an IPv4 or IPv6 host.

#### Format

```
ping { <IPv4addr> | <IPv6addr [%zone-id]> | <hostname> [ipv6] }  
[<IPv4 Parameters> | <IPv6 Parameters>]
```

#### Mode

User or Enable.

## Description

The **ping** command tests connection between the X-Pedition router and an IPv4 or IPv6 host. The **ping** command sends ICMP Echo Request packets to the host you specify. If you specify an IPv4 address or hostname, ICMPv4 Echo Requests will be sent. If you specify an IPv6 address or hostname, ICMPv6 Echo Requests will be sent. The **ipv6** keyword must be specified to declare a hostname an IPv6 hostname.

- If the packets reach the host, the host sends responds with an ICMP (v4 or v6) Echo Reply to the router and the CLI displays messages stating that the host can be reached.
- If the host does not respond, the router assumes the host cannot be reached from the router and the CLI displays messages stating that the host did not reply.

Use the IPv4 parameters listed below with an IPv4 address or hostname, and the IPv6 parameters listed below with an IPv6 address or hostname.

This command can be interrupted with the terminal interrupt key sequence.

### Pinging IPv6 Link-Local Addresses

The optional *%zone-id* parameter can be entered in conjunction with a link-local IPv6 address, to uniquely identify an interface in cases where all link-local addresses on a node are the same. On X-Pedition routers, the IPv6 interface name is used as the zone-id.

Note that you can only ping a link-local address of an interface on another node if that interface is directly connected to an interface on the local router. In this case, the interface name entered with the *%zone-id* parameter is the name of the local interface on the link (*not* the interface name of the remote interface being pinged). For example, if intf1 on router A is directly connected to (that is, on the same link as) intf2 on router B, then you can ping the link-local address of intf2 on router B from router A, by specifying the link-local address of intf2 (on router B) and the zone id of intf1 (on router A).

You cannot ping the link-local address of an interface on another node if the interface is not directly connected to an interface on the local router.

You can ping the link-local address of an interface on the local router. In this case, the interface name entered with the *%zone-id* parameter is the name of the local interface being pinged.

**Note:** For more information about the use of zone-ids, see the IPv6 Scoped Address Architecture draft (<http://www.ietf.org/internet-drafts/draft-ietf-ipv6-scoping-arch-01.txt>), which describes how scoped addresses (such as link-local or site-local addresses) are represented textually using zone-ids for disambiguation.

## Parameters

|   |   |
|---|---|
| <i>IPv4addr</i>  <br><i>IPv6addr</i> [ <i>%zone-id</i> ]  <br><i>hostname</i> [ <b>ipv6</b> ] | Specifies the host to contact.<br><br>If you enter an IPv4 address or an IPv4 hostname, the router will send ICMPv4 Echo Requests.<br><br>If you enter an IPv6 address or an IPv6 hostname followed by the <b>ipv6</b> keyword, the router will send ICMPv6 Echo Requests. When you are pinging a link-local address, use the optional <i>%zone-id</i> parameter, where <i>zone-id</i> is an interface name, to uniquely identify the interface. By default, <i>hostname</i> is assumed to be IPv4. The <b>ipv6</b> keyword must be specified to declare a hostname an IPv6 hostname. |
|---|---|

## IPv4 Parameters

|   |   |
|---|---|
| <b>packets</b> < <i>num</i> >             | The number of ICMP Echo Request packets to send. The default is 1.  |
| <b>size</b> < <i>num</i> >                | The packet size. Maximum size is 5000 bytes. Default size is 36 bytes, which generates a 64 byte IPv4 packet.   |
| <b>wait</b> < <i>sec</i> >                | The number of seconds the X-Pedition router will wait for a positive response from the host before assuming that the host has not responded. The default is 1.  |
| <b>flood</b>                              | Causes the X-Pedition router to send a new ping request as soon as a ping reply is received. If you do not specify the <b>flood</b> option, the router waits to send a new request. The amount of time the router waits is specified by the <b>wait</b> option.   |
| <b>dontroute</b>                          | Restricts the ping to locally attached hosts.   |
| <b>internalpriority</b><br>< <i>num</i> > | Allows you to set the queue from which the ping packets will be sent. The value of < <i>num</i> > can be one of the following:<br><br>0 — Selects the regular traffic queue<br><br>1 — Selects the medium priority queue<br><br>2 — Selects the high priority queue<br><br>3 — Select the control message queue. This is the default. |
| <b>sip</b> < <i>IPv4addr</i> >            | Allows you to set the source IPv4 address of the ICMP packets. By default, the source address is the address of the sending interface.  |

|                  |  |
|------------------|--|
| <b>tos</b> <num> | Allows you to set the Type of Service value in the Echo Request packets. The default value is 0.             |
| <b>ttl</b> <num> | Allows you to set the maximum number of gateways (“hops”) to travel. The value can range from 1 through 255. |

## IPv6 Parameters

|                        |  |
|------------------------|--|
| <b>packets</b> <num>   | Specifies how many ICMPv6 Echo Requests to send. The default value for <num> is 5.   |
| <b>size</b> <num>      | Specifies the length of the data portion of the Echo Request packets. The value of <num> may be between 0 and 65488 bytes. The default is 16 bytes, which generates a 64 byte IPv6 packet.   |
| <b>pad</b> <pad-bytes> | Allows you to specify the bytes to use for padding to completely fill the data portion of the packets sent. Enter the pad bytes as a hex data pattern, from 0 to ffff.<br><br>The ICMPv6 header size is 48 octets including the IPv6 header. |
| <b>wait</b> <sec>      | Specifies the amount of time in seconds to wait for an Echo Reply before sending another one. The default is 1 second.   |
| <b>sip</b> <IPv6addr>  | Allows you to set the source IPv6 address of the ICMP packets. By default, the source address is the address of the sending interface.   |

## Restrictions

If you enter this command from the User mode, the only parameter you can use is <IPv4addr> / <IPv6addr [%zone-id]> / <hostname> [ipv6]. To use any of the other parameters, you must be in Enable mode.

## Examples

The following example sends the default of 5 ICMPv6 packets to an IPv6 host identified by its IPv6 address.

```
xp# ping 22::2e0:63ff:fe13:2003
PING6(64=40+8+16 bytes) 20::2e0:63ff:fe13:2043 --> 22::2e0:63ff:fe13:2003
24 bytes from 22::2e0:63ff:fe13:2003, icmp_seq=0 time=222.413 ms
24 bytes from 22::2e0:63ff:fe13:2003, icmp_seq=1 time=111.879 ms
24 bytes from 22::2e0:63ff:fe13:2003, icmp_seq=2 time=96.472 ms
24 bytes from 22::2e0:63ff:fe13:2003, icmp_seq=3 time=98.02 ms
24 bytes from 22::2e0:63ff:fe13:2003, icmp_seq=4 time=102.593 ms

--- 22::2e0:63ff:fe13:2003 ping6 statistics ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/std-dev = 96.472/126.275/222.413/48.368 ms
```

This example sends 5 ICMPv4 packets to an IPv4 host identified by its IPv4 address:

```
xp# ping 20.1.1.1 packets 5
PING 20.1.1.1 (20.1.1.1): 36 data bytes
44 bytes from 20.1.1.1: icmp_seq=0 ttl=255 time=30.000 ms
44 bytes from 20.1.1.1: icmp_seq=1 ttl=255 time=0.000 ms
44 bytes from 20.1.1.1: icmp_seq=2 ttl=255 time=0.000 ms
44 bytes from 20.1.1.1: icmp_seq=3 ttl=255 time=0.000 ms
44 bytes from 20.1.1.1: icmp_seq=4 ttl=255 time=10.000 ms

--- 20.1.1.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.000/8.000/30.000 ms
```

This example pings the IPv6 interface on a directly connected link between two X-Pedition routers. The ping is sent by router A over its IPv6 interface named intf1 to the link-local IPv6 address of the directly connected interface on router B.

```
xpa# ping fe80::2e0:63ff:fe13:2003%intf1
PING6(64=40+8+16 bytes) fe80::2e0:63ff:fe13:2043%intf1 --> fe80::2e0:63ff:fe13:2003%intf1
24 bytes from fe80::2e0:63ff:fe13:2003%intf1, icmp_seq=0 time=59.621 ms
24 bytes from fe80::2e0:63ff:fe13:2003%intf1, icmp_seq=1 time=64.453 ms
24 bytes from fe80::2e0:63ff:fe13:2003%intf1, icmp_seq=2 time=132.73 ms
24 bytes from fe80::2e0:63ff:fe13:2003%intf1, icmp_seq=3 time=1280.43 ms
24 bytes from fe80::2e0:63ff:fe13:2003%intf1, icmp_seq=4 time=133.433 ms

--- fe80::2e0:63ff:fe13:2003 ping6 statistics ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/std-dev = 59.621/334.133/1280.430/474.216 ms
```





# Chapter 50

## port Commands

The **port** commands set and display the following parameters:

- Port state (enabled or disabled)
- Bridging status (flow-based or address-based)
- Port operating mode (half duplex or full duplex)
- Port speed for the 10/100 ports (10-Mbps or 100-Mbps)
- Port mirroring (used for analyzing network traffic)
- Port shut down if broadcast threshold is reached

### Command Summary

[Table 43](#) lists the **port** commands. The sections following the table describe the command syntax.

**Table 43. port Commands**

|  |
|--|
| <b>port auto-negotiate enable</b> <port-list>  <b>disable</b> <port-list>  <b>restart</b> <port-list>  |
| <b>port bmon</b> <port-list> [ <b>redirect</b>   <b>unlimited-redirect</b> ] [ <b>rate</b> <number>] [ <b>duration</b> <number>] [ <b>expire</b> <number>] [ <b>packets-limited all</b>   <b>broadcast</b> ] |
| <b>port description</b> <port-list> <desc>   |
| <b>port disable</b> <port-list>  |
| <b>port enable 8021p port</b> <port-list>  |
| <b>port flow-bridging</b> <port-list>  <b>all-ports</b>  |
| <b>port enable forced-return-flows port</b> <port-list>   <b>all-ports</b>   |

Table 43. port Commands (Continued)

|  |
|--|
| <b>port set</b> [ <i>&lt;port-list&gt;</i> ] <b> all-ports</b> [ <b>duplex</b> full half] [ <b>speed</b> 10Mbps 100Mbps  <i>&lt;number&gt;</i> ] [ <b>auto-negotiation</b> on off] [ <b>auto-negotiation-speed</b> 10Mbps 100Mbps 10_100Mbps] [ <b>auto-negotiation-duplex</b> half full both] [ <b>auto-negotiation-flowctl</b> off asymmetric symmetric both] [ <b>hash-mode</b> m0 m1 m2 m3 m-auto] [ <b>rx-hashmode</b> m0 m1 m2 m3 m4 m5 m6 m7  m8 m9] [ <b>wan-encapsulation</b> frame-relay  ppp] [ <b>ifg</b> <i>&lt;number&gt;</i> ] [ <b>input-encapsulation</b> forced-ethernet_ii] [ <b>link-timer</b> <i>&lt;number&gt;</i> ] [ <b>clock</b> <i>&lt;clock-source&gt;</i> ] [ <b>transmit-clock-source</b> local loop] [ <b>framing</b> cbit-parity m23 esf g832 g751] [ <b>mtu</b> <i>&lt;number&gt;</i> ] [ <b>mc-vlan-encap</b> <i>&lt;number&gt;</i> ] |
| <b>port show 8021p</b> <i>&lt;port-list&gt;</i> <b> all-ports</b>  |
| <b>port show autonegotiation</b> <i>&lt;port-list&gt;</i> <b> all-ports</b>  |
| <b>port show autonegotiation-capabilities</b> <i>&lt;port-list&gt;</i> <b> all-ports</b>   |
| <b>port show bmon</b> [config][detail][ <b>port</b> <i>&lt;port list&gt;</i> ][stats]  |
| <b>port show bridging-status</b> <i>&lt;port-list&gt;</i> <b> all-ports</b>  |
| <b>port show description</b> <i>&lt;port-list&gt;</i> <b> all-ports</b>  |
| <b>port show hash-mode</b> <i>&lt;port-list&gt;</i> <b> all-ports</b>  |
| <b>port show MAU</b> <i>&lt;port-list&gt;</i> <b> all-ports</b>  |
| <b>port show MAU-statistics</b> <i>&lt;port-list&gt;</i> <b> all-ports</b>   |
| <b>port show mc-vlan-encap</b> <i>&lt;port-list&gt;</i> <b> all-ports</b>  |
| <b>port show mirroring-status</b> <i>&lt;port list&gt;</i> <b>  all-ports  all-acls</b>  |
| <b>port show port-status</b> <i>&lt;port-list&gt;</i> <b> all-ports  all-smarttrunks</b>   |
| <b>port show pvst-info</b> <i>&lt;port-list&gt;</i> <b> all-ports spanning-tree</b> <i>&lt;string&gt;</i> [rstp]   |
| <b>port show serial-link-info</b> <i>&lt;port-list&gt;</i> <b> all-ports</b>   |
| <b>port show stp-info</b> <i>&lt;port-list&gt;</i> <b> all-ports [rstp]</b>  |
| <b>port show vlan-info</b> <i>&lt;port-list&gt;</i> <b> all-ports</b>  |

# port auto-negotiate

## Purpose

Enables, disables, and/or restarts auto-negotiation on a port.

## Format

**port auto-negotiate enable** <port-list>|**disable** <port-list>|**restart** <port-list>

## Mode

Enable.

## Description

The **port auto-negotiate** command allows you to enable auto-negotiation on a port, disable auto-negotiation on a port, and/or restart auto-negotiation on a port. Auto-negotiation is a process whereby both ports on a connection resolve the best line speed, duplex mode and flow control scheme to communicate with each other.

## Parameters

|                            |  |
|----------------------------|--|
| <b>enable</b> <port-list>  | Enables auto-negotiation on the port or set of ports.  |
| <b>disable</b> <port-list> | Disables auto-negotiation on the port or set of ports. |
| <b>restart</b> <port-list> | Restarts auto-negotiation on the port or set of ports. |

## Restrictions

None.

## Example

To enable auto-negotiation on port et.2.1:

```
xp# port auto-negotiate enable et.2.1
```

# port bmon

## Purpose

Monitor broadcast traffic on a port. This command is useful in cases where excess broadcast traffic heading toward the control module may degrade performance and you need to temporarily shut down the port.

## Format

```
port bmon <port-list> [rate <number>] [duration <number>] [expire <number>]  
[packet-limited all|broadcast] [redirect <port>] [unlimited-redirect <port>]
```

## Mode

Configure.

## Description

The **port bmon** command allows you to monitor the broadcast traffic on one or more ports and shut down a port if its broadcast traffic reaches and sustains a certain rate limit for a specific length of time. The **port bmon** command can also *redirect* the traffic from a channel with a monitored port to another port instead of shutting the monitored port down. The unlearned traffic for the monitor port's channel (all ports on that line card) is redirected to the target port and learned traffic flows continue to forward as they were learned. When configuring **port bmon**, you must specify a port to which you will redirect traffic if you are using the redirection feature—otherwise, the command will shut down the port by default.

With the **port bmon** command, you can define monitoring thresholds on a port or set of ports. If those thresholds are met or exceeded, the port(s) will shut down for a user-specified period. This will reduce the risk that the control module may become overloaded by traffic and crash.

## Parameters

|                         |   |
|-------------------------|---|
| <b>port</b> <port-list> | Specifies the ports that you are monitoring for broadcasts.   |
| <b>rate</b> <number>    | The rate limit, in Kpkts per second, which will trigger a port shut down if the rate is sustained for the specified duration. Values can be from 1-1000. The default value is 10. |

|   |  |
|---|--|
| <b>duration</b> <number>                      | Number of seconds that the specified rate limit is sustained, after which the port will be shut down. Values can be from 1-3600. The default value is 1.   |
| <b>expire</b> <number>                        | Number of seconds that the port will be shut down or redirected if the rate threshold is reached. Values can be from 60-36000. The default value is 300.   |
| <b>packets-limited all</b>   <b>broadcast</b> | Specifies the type of packets to monitor for shutdown or redirect. Specify <b>all</b> to monitor all packets. Specify <b>broadcast</b> to only monitor broadcast packets. The default value is <b>all</b> .  |
| <b>redirect</b> <port>                        | Specifies the port to which you will redirect traffic. The redirect option routes all unlearned traffic through another port after the current port reaches capacity. Redirect sends traffic for the number of seconds defined as the <b>expire</b> value, but waits the number of seconds defined as the <b>duration</b> before redirecting traffic. This option cannot be used with the unlimited-redirect option. |
| <b>unlimited-redirect</b> <port>              | Specifies the port to which you will redirect traffic. The unlimited-redirect option routes all unlearned traffic through another port after the current port reaches capacity. Unlimited-redirect sends traffic <i>indefinitely</i> , but waits the number of seconds defined as the <b>duration</b> before redirecting traffic. This option cannot be used with the redirect or expire options.                    |

## Restrictions

None.

## Examples

To monitor traffic on port et.1.3 and shut it down for 5 minutes if the rate of 10,000 packets per second is sustained for 1 second:

```
xp(config)# port bmon et.1.3 packets-limited all
```

To monitor traffic on port et.1.3 and shut it down for 3 minutes if the rate of 25,000 packets per second is sustained for 5 seconds:

```
xp(config)# port bmon et.1.3 rate 25 duration 5 expire 180 packets-limited all
```

To configure a 360-second expiration on port et.1.3 whenever a rate of 100,000 broadcast packets per second is sustained for 1 second:

```
xp(config)# port bmon et.1.3 rate 100 expire 360 packets-limited broadcast
```

### How to use redirection:

This will redirect all unlearned traffic on port et.3.2's channel to port et.4.3 for 60 seconds, one second after the 1kPkts/sec traffic limit is reached:

```
xp(config)# port bmon et.3.2 redirect et.4.3 rate 1 expire 60 packets-limited all
```

This will redirect all unlearned traffic on port et.2.2's channel to port et.3.1 indefinitely, one second after the 5kPkt/sec broadcast traffic limit is reached:

```
xp(config)# port bmon et2.2 unlimited-redirect et.3.1 rate 5
```

This will redirect all unlearned traffic on port et.1.3's channel to port et.2.3 for 100 seconds, five seconds after the 2kPkt/sec limit has been reached:

```
xp(config)# port bmon et.1.3 redirect et.2.3 expire 100 rate 2 duration 5
```

# port description

## Purpose

Defines a user description for a port.

## Format

**port description** <port-list> <desc>

## Mode

Configure.

## Description

The **port description** command allows you to define a character string description for a port. This is useful for management purposes.

## Parameters

|                                   |   |
|-----------------------------------|---|
| <b>description</b><br><port-list> | Specifies the port(s). Valid for Ethernet and WAN ports only.   |
| <b>description</b> <desc>         | Specifies the character string used for the description of the port. This must be 125 characters or less. |

## Restrictions

This command is valid for Ethernet and WAN only.

## Example

To set port et.2.1 with the description 'vlan1-2':

```
xp(config)# port description et.2.1 vlan1-2
```

# port disable

## Purpose

Disable a port.

## Format

**port disable** *<port-list>*

## Mode

Configure.

## Description

The **port disable** command disables the specified ports. Disabled ports do not send or receive any traffic. You might want to disable unused ports to prevent network users from inadvertently or unscrupulously connecting to unoccupied but enabled ports on the X-Pedition router.

## Parameters

|                          |  |
|--------------------------|--|
| <i>&lt;port-list&gt;</i> | Specifies the ports you are disabling. |
|--------------------------|--|

## Restrictions

None.

## Examples

To disable port et.1.3 on the X-Pedition router:

```
xp(config)# port disable et.1.3
```

To disable ports 1 through 5 on the Ethernet line card in slot 3 of the X-Pedition chassis:

```
xp(config)# port disable et.3.1-5
```



# port enable 8021p

## Purpose

Enables 802.1p encapsulation.

## Format

**port enable 8021p port** <port-list> | **all-ports**

## Mode

Configure.

## Description

The **port enable 8021p** command enables 802.1p encapsulation on the specified ports. The 802.1p standard provides the ability to classify traffic into eight priority categories or class of services. This classification scheme is based upon MAC frame information and is used for QoS (Quality of Service) for VLANs.

## Parameters

|                  |  |
|------------------|--|
| <port-list>      | Specifies the port(s) you are enabling.            |
| <b>all-ports</b> | Enables 802.1p encapsulation on all relevant ports |

## Restrictions

None.

## Example

To enable 802.1p encapsulation on port et.1.3:

```
xp(config)# port enable 8021p port et.1.3
```

## port flow-bridging

### Purpose

Set ports to use flow-based bridging.

### Format

**port flow-bridging** <port-list> | **all-ports**

### Mode

Configure.

### Description

The **port flow-bridging** command changes the specified ports from using address-based bridging to using flow-based bridging. A port can use only one type of bridging at a time.

Each port has an L2 lookup table where MAC address or flows are stored.

- If the port is configured for address-based bridging (default), each L2 table entry consists of a MAC address and a VLAN ID.
- If the port is configured for flow-based bridging, each L2 table entry consists of a source MAC address, a destination MAC address, and a VLAN ID.

Suppose that a port on the X-Pedition router is connected to a hub that is connected to three workstations, A, B, and C. If each workstation is talking to one another and sending broadcast traffic, the L2 table on the X-Pedition port would contain the following entries for the workstations. Assume that the VLAN ID is “1” for all entries.

If the ports are configured for address-based bridging:

- MAC address A
- MAC address B
- MAC address C
- MAC broadcast address

If the ports are configured for flow-based bridging:

- MAC addresses A->B
- MAC addresses B->A
- MAC addresses B->C
- MAC addresses A->C
- MAC addresses C->A
- MAC addresses C->B
- MAC addresses A->broadcast
- MAC addresses B->broadcast
- MAC addresses C->broadcast

## Parameters

|                          |  |
|--------------------------|--|
| <i>&lt;port-list&gt;</i> | Specifies the ports you are changing to flow-based bridging.           |
| <b>all-ports</b>         | Changes all the ports on the X-Pedition router to flow-based bridging. |

## Restrictions

None.

## Example

To configure Ethernet port et.3.7 for flow-based bridging:

```
xp(config)# port flow-bridging et.3.7
```

## port enabled forced-return-flows

### Purpose

Enable the forced-return-flows to function on a port or list of ports.

### Format

**port enable forced-return-flows port** <port-list>|**all-ports**

### Mode

Configure.

### Description

The **port enable forced-return-flows** command allows you to perform routing without the use of a layer 3 protocol such as RIP or OSPF—these setups may involve VRRP and static gateways. In the case of VRRPs and static gateways, when a remote gateway goes down it does not notify routers more than one hop away. This can cause existing flows to restrict the flow of traffic. With forced-return-flows enabled, each new flow checks the exit port for a “reverse flow” (the source/destination IP addresses are the reverse of this new flow). If the “reverse flow” has an exit port that differs from the new flow’s entry port, the exit port of the “reverse flow” changes to the new flow’s entry port.

### Parameters

|                  |   |
|------------------|---|
| <port-list>      | Enable forced return flows to a specific port on the port list. |
| <b>all-ports</b> | Specifies all ports.  |

### Restrictions

None.

### Example

```
xp(config)# port enable forced-return-flows port et.4.6
```

# port set

## Format

```
port set [<port-list>|all-ports] [duplex full|half] [speed 10Mbps|100Mbps|<number>]
[auto-negotiation on|off] [auto-negotiation-speed 10Mbps|100Mbps|10_100Mbps]
[auto-negotiation-duplex half|full|both] [auto-negotiation-flowctl off|asymmetric|symmetric|
both] [hash-mode m0|m1|m2|m3|m-auto] [rx-hashmode m0|m1|m2|m3|m4|m5|m6|m7|m8|m9]
[wan-encapsulation frame-relay|ppp] [ifg <number>]
[input-encapsulation forced-ethernet_ii] [link-timer <number>] [clock <clock-source>]
[transmit-clock-source local|loop] [framing cbit-parity|m23|esf|g832|g751] [mtu <number>]
[mc-vlan-encap <number>]
```

## Mode

Configure.

## Description

The **port set** command allows users to set the port operating mode and speed. Depending on the port's media type, users may set any of the following parameters:

- Note:** By default, all ports use autosensing to detect the operating mode and speed of the network segment to which they are connected. If you use this command to set a port parameter, the setting disables autosensing for that parameter on the port. For example, if you set the speed of a segment to 10-Mbps, that segment no longer uses autosensing for the port speed and will always attempt to operate at 10-Mbps.
- Ethernet ports (e.g., et.2.1)
    - Auto-negotiation (on or off, speed, and duplex)
    - Duplex (half or full)
    - Port speed
    - Hash-mode
    - Input-encapsulation
    - Inter-frame Gap (IFG)
    - Packet VLAN encapsulation
  - Gigabit ports (e.g., gi.4.1)
    - Auto-negotiation (on or off and flow control)
    - Hash-mode
    - Link-timer
    - Inter-frame Gap (IFG)
    - Packet VLAN encapsulation
    - Maximum Transmit Unit (MTU)

- Ten Gig ports (e.g., xg.3.1)
  - Auto-negotiation flow control
  - hash-mode
  - Packet VLAN encapsulation
  - RX-hashmode
  - Maximum Transmit Unit (MTU)
- HSSI ports (e.g., hs.3.1)
  - Clock source
  - wan-encapsulation
  - shared-flags
  - speed
  - clock
- Serial ports (e.g., se.3.1)
  - wan-encapsulation
  - shared-flags
  - speed
- ATM ports (e.g., at.3.1)
  - Hash-mode
  - Transmit-clock-source
  - Framing (ATM ports only, no VP or VC)
- POS (Sonet) ports (e.g., so.3.1)
  - Hash-mode
  - Packet VLAN encapsulation
- FDDI ports (e.g., fi.3.1)
  - Input-encapsulation
  - Hash-mode
  - Packet VLAN encapsulation
  - Inter-frame Gap (IFG)

## Parameters

|  |  |
|--|--|
| <code>&lt;port-list&gt; all-ports</code> | Specifies the port to which you will apply the setting (supported ports include Ethernet, Gigabit, Ten Gig, ATM, POS, HSSI, Serial, Sonet, FDDI, FE, and WAN ports). The <b>all-ports</b> keyword applies the settings you select to all the X-Pedition ports. |
| <b>duplex full half</b>                  | Sets the operating mode to half duplex or full duplex. This option is valid for 10/100 Mbps Ethernet only.   |
| <b>speed<br/>10Mbps 100Mbps</b>          | On Fast Ethernet ports with auto-negotiation disabled, set the port speed to 10Mbps or 100Mbps using appropriate keywords, or set the speed to a number in bits/sec on WAN ports.  |

|   |  |  |
|---|--|--|
| <b>auto-negotiation on off</b>                                | Turns on or off auto-negotiation for Gigabit Ethernet ports. Auto-negotiation is a process whereby both ports on a connection resolve the best line speed, duplex mode and flow control scheme to communicate with each other. |  |
| <b>auto-negotiation-speed 10Mbps 100Mbps 10_100Mbps</b>       | Sets the auto-negotiation speed on a Fast Ethernet port.   |  |
|   | <b>10Mbps</b>  | Sets the auto-negotiation line speed capability advertised to 10Mbps/sec                 |
|   | <b>100Mbps</b>   | Sets the auto-negotiation line speed capability advertised to 100Mbps/sec                |
|   | <b>10_100Mbps</b>  | Sets the auto-negotiation line speed capability advertised to 10Mbps/sec and 100Mbps/sec |
| <b>auto-negotiation-duplex half full both</b>                 | Sets the auto-negotiation duplex mode on a Fast Ethernet port.   |  |
|   | <b>half</b>  | Sets the auto-negotiation duplex mode advertised to half-duplex.                         |
|   | <b>full</b>  | Sets the auto-negotiation duplex mode advertised to full-duplex.                         |
|   | <b>both</b>  | Sets the auto-negotiation duplex mode advertised to half-duplex and full-duplex.         |
| <b>auto-negotiation-flowctl off asymmetric symmetric both</b> | Sets the flow-control on a full-duplex Gigabit Ethernet port.  |  |
|   | <b>off</b>   | Clears the flow-control capability advertised by the port.                               |
|   | <b>asymmetric</b>  | Sets the flow-control capability advertised to asymmetric pause.                         |
|   | <b>symmetric</b>   | Sets the flow-control capability advertised to symmetric pause.                          |
|   | <b>both</b>  | Sets the flow-control capability advertised to asymmetric pause and symmetric pause.     |

|  |  |
|--|--|
| <b>hash-mode</b><br><b>m0 m1 m2 m3 </b><br><b>m-auto</b> | <p>Sets the Layer-2 hash mode for this port, which disables automatic hashing. This hash mode defines the algorithm scheme that will be used to calculate the hash value used for the Layer-2 and Layer-3 lookup table.</p> <p>The 48-bit MAC address is hashed into 8-bit groupings, represented by either B5, B4, B3, B2, B1, or B0. Assuming a MAC address of the value B5B4:B3B2:B1B0, the following describes the various hash mode and the resulting MAC address format:</p> <p><b>m0</b>     B5B4:B3B2:B1B0</p> <p><b>m1</b>     B5B4:B3B2:B0B1</p> <p><b>m2</b>     B5B4:B2B3:B1B0 (default hash mode)</p> <p><b>m3</b>     B4B5:B3B2:B1B0</p> <p><b>m-auto</b> Auto-hashing periodically queries the L2 or L3 tables for hash bucket overflow on a port. If the number of overflows exceed a certain threshold level, auto-hashing will automatically change the hash mode for that port. Eventually a 'best' hash mode for the particular traffic will be found, which will provide optimal distribution across the L2 or L3 lookup table.</p> <p>The 16 bit hash index is calculated by the performing the following calculation:</p> <p>(B5B4) XOR (B3B2) XOR (B1B0)</p> <p><b>Note:</b> The hash-mode command is subject to merging. If you enter one command for a module setting the variant to 8 (enabling autohashing) and then enter another command for the same module setting it to another variant, the commands will merge. The second command will become activated and overwrite the first one, in this case disabling autohashing on the module.</p> <p><b>Note:</b> Setting a variant on an ER-16 module will set it on both channels on that module.</p> |
|--|--|



|   |  |
|---|--|
| <b>rx-hashmode m0  m1  m2  m3  m4  m5  m6  m7  m8  m9</b> | <p>The 10-Gbps port can distribute packets by Destination IP, Destination MAC, Source IP, Source MAC, Destination/Source MAC, or Destination/Source IP. The distribution parameters are configurable by the end user in rx-hashmode. Users may select one of the following:</p> <p><b>m0</b> Hash on Source IP/MAC, Destination IP/MAC, Ether type/L3 protocol, and vlan ID. This is the default hash mode.</p> <p><b>m1</b> Hash on Source MAC, Destination MAC.</p> <p><b>m2</b> Hash on Destination MAC.</p> <p><b>m3</b> Hash on Source MAC.</p> <p><b>m4</b> Hash on Source IP/MAC and Destination IP/MAC.</p> <p><b>m5</b> Hash on Destination IP/MAC.</p> <p><b>m6</b> Hash on Source IP/MAC.</p> <p><b>m7</b> Hash on Source IP and Destination IP.</p> <p><b>m8</b> Hash on Destination IP.</p> <p><b>m9</b> Hash on Source IP.</p> |
| <b>wan-encapsulation frame-relay ppp</b>                  | Sets the encapsulation for the WAN port to either frame-relay or PPP.  |
| <b>ifg &lt;number&gt;</b>                                 | <p>Changes the <i>Inter-frame Gap</i> (IFG) for the port by multiplying it by the &lt;number&gt; specified. The IFG values are 600-nanosecond units for 10mb connections, 40-nanosecond units for 100mb connections, and 16-nanosecond units for 1000mb connections. Possible values for this parameter are -3 through 24.</p> <p><b>Note:</b> When SmartTRUNKing to an Ethernet GIGASwitch product, set the IFG to 4 or greater to allow the GIGASwitch enough time to properly process incoming frames.</p>  |
| <b>input-encapsulation forced-ethernet_ii</b>             | Changes the interpretation of the input MAC encapsulation to Ethernet II.  |
| <b>link-timer &lt;number&gt;</b>                          | Sets the auto-negotiation link timer to the number of milliseconds specified by <number>. The <number> is a value between 0 and 20. This option is valid for Gigabit ports only.   |
| <b>clock &lt;clock-source&gt;</b>                         | <p>Sets the clock source. This parameter is applicable only when the <b>wan-encapsulation</b> parameter is specified for a HSSI port that will be connected back-to-back with a HSSI port on another router. The &lt;clock-source&gt; is one of the following values:</p> <p><b>external-clock</b> External transmit clock (DCE provided)</p> <p><b>internal-clock-51mh</b> Internal transmit clock at 51.84 Mhz</p> <p><b>internal-clock-25mh</b> Internal transmit clock at 25.92 Mhz</p> <p><b>external-rx-clock</b> External receive clock for transmit clocking</p> <p><b>Note:</b> For WAN cards without an internal clock, an external CSU/DSU is required.</p>   |

|   |   |
|---|---|
| <b>transmit-clock-source local loop</b>                 | <p>Sets the ATM port transmit clock source. The expected value is one of the following timing sources:</p> <p><b>local</b> Selects the on board crystal oscillator as the clock source<br/><b>local</b> is the default value</p> <p><b>loop</b> Selects the receiver inputs as the clock source</p> <p><b>Note:</b> Do not set both ports in the same connection with a loop clock source. At least one port must be set to local clock source.</p> |
| <b>framing cbit-parity</b><br><b> m23 esf g832 g751</b> | <p>Specifies the type of framing used by the ATM port. The expected value is one of the following framing types:</p> <p><b>cbit-parity</b> Valid for T3 only</p> <p><b>m23</b> Valid for T3 only</p> <p><b>esf</b> Valid for T1 only</p> <p><b>g832</b> Valid for E3 only</p> <p><b>g751</b> Valid for E3 only</p>  |
| <b>mtu &lt;number&gt;</b>                               | Sets the Maximum Transmit Unit (MTU) for the port by the amount specified (64–65442). The default value depends on the port type. This parameter is not valid for ethernet ports.   |
| <b>mc-vlan-encap</b><br><b>&lt;number&gt;</b>           | The X-Pedition router can forward multicast packets to only one VLAN on an 802.1Q trunk. To resolve this problem, all outgoing multicast traffic on a Q trunk port is redirected to <b>vlan &lt;number&gt;</b> . On the other end of the Q trunk link, a SmartSwitch 2000/6000 is used and configured with VLAN classification. This allows multicast traffic to forward successfully.  |

## Restrictions

For 10/100 Mbps Ethernet, you must set both the operating mode and the speed. You cannot set one without setting the other. For Gigabit Ethernet, you can only turn on or off auto-negotiation. You cannot set the speed or duplex for Gigabit modules.

## Examples

To configure port et.1.5 to be 10 Mbps and half duplex:

```
xp(config)# port set et.1.5 speed 10mbps duplex half
```

To turn off auto-negotiation for the Gigabit port gi.4.2:

```
xp(config)# port set gi.4.2 auto-negotiation off
```

To set the Layer 2 hash mode for all ports to the m0 hash algorithm:

```
xp(config)# port set all-ports hash-mode m0
```

To set the speed for a HSSI ppp WAN port located on port 1 of slot 3:

```
xp(config)# port set hs.3.1 wan-encapsulation ppp speed 45000000
```

To set an internal clock source (25.92 Mhz) for a HSSI ppp WAN port located on port 1 of slot 3:

```
xp(config)# port set hs.3.1 wan-encapsulation ppp speed 45000000 clock internal-clock-25mh
```

To set the speed for a serial frame relay WAN port located at port 4 of slot 2, VC 100:

```
xp(config)# port set se.2.4.100 wan-encapsulation frame-relay speed 1500000
```

To increase the inter-frame gap for port et.1.1 by 400 nanoseconds (10 \* 40ns):

```
xp(config)# port set ifg et.1.1 ifg 10
```

To view the RX hashmode options available for all ports, enter the following:

```
xp(config)# port set all-ports rx-hashmode ?
[rx-hashmode] requires a value of this type:
[keyword]    - One of the following keywords:
  m0          - Hash on Source IP/MAC, Destination IP/MAC, Ether type/L3 protocol, and vlan ID.
               This is the default hash mode.
  m1          - Hash on Source MAC, Destination MAC.
  m2          - Hash on Destination MAC.
  m3          - Hash on Source MAC.
  m4          - Hash on Source IP/MAC and Destination IP/MAC.
  m5          - Hash on Destination IP/MAC.
  m6          - Hash on Source IP/MAC.
  m7          - Hash on Source IP and Destination IP.
  m8          - Hash on Destination IP.
  m9          - Hash on Source IP.
```

To hash incoming 10-Gigabit traffic on port **xg.3.1** by Source MAC address for distribution over the module's backplane connections, enter the following:

```
xp(config)# port set xg.3.1 rx-hashmode m3
```

## port show 8021p

### Purpose

Displays 802.1p encapsulation status.

### Format

**port show 8021p** <port-list>|**all-ports**

### Mode

Enable.

### Description

The **port show 8021p** command displays whether 802.1p encapsulation is enabled or disabled on a port or list of ports. The 802.1p standard provides the ability to classify traffic into eight priority categories or class of services. This classification scheme is based upon MAC frame information and is used for QoS (Quality of Service) for VLANs.

### Parameters

|                  |  |
|------------------|--|
| <port-list>      | Specifies the ports for which you want to display the description. |
| <b>all-ports</b> | Displays the description for all the X-Pedition ports.             |

### Restrictions

None.

### Example

To display 802.1p encapsulation status for port et.2.1:

```
xp# port show 8021p et.2.1

Port      802.1p Status
----      -
et.2.1    Disabled
```

# port show autonegotiation

## Purpose

Displays auto-negotiation information.

## Format

**port show autonegotiation** <port-list>|**all-ports**

## Mode

Enable.

## Description

The **port show autonegotiation** command displays auto-negotiation information. This command displays port number, administration status, current status, remote signaling, fault advertised, and fault received. Auto-negotiation is a process whereby both ports on a connection resolve the best line speed, duplex mode and flow control scheme to communicate with each other.

## Parameters

|                  |  |
|------------------|--|
| <port-list>      | Specifies the ports for which you want to display the description. |
| <b>all-ports</b> | Displays the description for all the X-Pedition ports.             |

## Restrictions

None.

## Example

To display auto-negotiation information for port et.2.1:

|   |                 |                   |                      |                     |                   |
|---|-----------------|-------------------|----------------------|---------------------|-------------------|
| xp# <b>port show autonegotiation et.2.1</b> |                 |                   |                      |                     |                   |
| Port  | Admin<br>Status | Current<br>Status | Remote<br>Signalling | Fault<br>Advertised | Fault<br>Received |
| -----                                       | -----           | -----             | -----                | -----               | -----             |
| et.2.1                                      | disabled        | other             | not detected         | n/a                 | n/a               |

## port show autonegotiation-capabilities

### Purpose

Displays auto-negotiation capabilities.

### Format

**port show autonegotiation-capabilities** *<port-list>*|**all-ports**

### Mode

Enable.

### Description

The **port show autonegotiation-capabilities** command displays auto-negotiation capabilities. This command displays a list of port capabilities, advertised capabilities, and any received capabilities from another port. Auto-negotiation is a process whereby both ports on a connection resolve the best line speed, duplex mode and flow control scheme to communicate with each other.

### Parameters

|                          |  |
|--------------------------|--|
| <i>&lt;port-list&gt;</i> | Specifies the ports for which you want to display the description. |
| <b>all-ports</b>         | Displays the description for all the X-Pedition ports.             |

### Restrictions

None.

Example

To display auto-negotiation capabilities for port et.2.1:

| xp# port show autonegotiation-capabilities et.2.1 |                  |                  |          |
|---|------------------|------------------|----------|
| Port  | Capability       | Advertised       | Received |
| -----   | -----            | -----            | -----    |
| et.2.1  | other            | other            |          |
|   | 10 baseT         | 10 baseT         |          |
|   | 10 baseT FD      | 10 baseT         | FD       |
|   | 100 baseT4       | 100 baseT4       |          |
|   | 100 baseTX       | 100 baseTX       |          |
|   | 100 baseTX FD    | 100 baseTX       | FD       |
|   | 100 baseT2       | 100 baseT2       |          |
|   | 100 baseT2 FD    | 100 baseT2       | FD       |
|   | Pause            | Pause            |          |
|   | Asymmetric Pause | Asymmetric Pause |          |
|   | Symmetric Pause  | Symmetric Pause  |          |
|   | Asym-Sym Pause   | Asym-Sym Pause   |          |
|   | 1000 baseX       | 1000 baseX       |          |
|   | 1000 baseX FD    | 1000 baseX       | FD       |
|   | 1000 baseT       | 1000 baseT       |          |
|   | 1000 baseT FD    | 1000 baseT       | FD       |

## port show bmon

### Purpose

Display broadcast monitoring information for X-Pedition ports.

### Format

**port show bmon** [**config**] [**detail**] [**port** <port list>] [**stats**]

### Mode

Enable.

### Description

The **port show bmon** command displays broadcast monitoring information for X-Pedition ports.

### Parameters

If no parameters are specified, the current states of all ports are displayed.

|                         |  |
|-------------------------|--|
| <b>config</b>           | Displays configuration information for broadcast monitoring.   |
| <b>detail</b>           | Displays all information for broadcast monitoring.             |
| <b>port</b> <port-list> | Specifies the ports for which you want to display information. |
| <b>stats</b>            | Displays statistics information for broadcast monitoring.      |

### Restrictions

None.



## Example

To display the state of ports with broadcast monitoring:

```
xp# port show bmon
Port: et.1.1 State: On

Port: et.6.8 State: ShutDn Shutdown: 39 (sec)

Port: et.7.8 State: On
```

The above example shows three ports, with the port et.6.8 shut down for 39 seconds.

To display broadcast monitoring configuration values set for the ports:

```
xp# port show bmon config
Port: et.1.1 Rate (Kpps): 10 Burst (sec): 1 Shutdown (sec):300

Port: et.6.8 Rate (Kpps): 10 Burst (sec): 5 Shutdown (sec):60

Port: et.7.8 Rate (Kpps): 2 Burst (sec): 2 Shutdown (sec):60
```

In the above example, port et.1.1 has been configured with default values.

To display broadcast monitoring statistics for the ports:

```
xp# port show bmon stats
Port: et.1.1 Current Broadcast Rate (Kpps): 0.000

Port: et.6.8 Burst at port shutdown (Kpps): 10.032
ShutDn Count: 2

Port: et.7.8 Current Broadcast Rate (Kpps): 0.000
```

In the above example, the current broadcast traffic on et.1.1 and et.7.8 is zero. The port et.6.8 is currently shut down and it shows a burst of 10.032K packets per second at its shut down. This port has been shut down twice because of excessive broadcast traffic.

To show broadcast monitoring details for the ports:

```
xp# port show bmon detail
Port: et.1.1 Rate (Kpps): 10 Burst (sec): 1 Shutdown (sec):300
State: On
Current Broadcast Rate (Kpps): 0.000

Port: et.6.8 Rate (Kpps): 10 Burst (sec): 5 Shutdown (sec):60
State: ShutDn Expire: 39 (sec)
Burst at port shutdown (Kpps): 10.032
ShutDn Count: 2

Port: et.7.8 Rate (Kpps): 2 Burst (sec): 2 Shutdown (sec):60
State: On
Current Broadcast Rate (Kpps): 0.000
```

The above example shows configuration, state, and statistics information.

# port show bridging-status

## Purpose

Display the bridging status of X-Pedition ports.

## Format

**port show bridging-status** <port-list>|all-ports

## Mode

Enable.

## Description

The **port show bridging-status** command displays bridging-status information for X-Pedition ports.

## Parameters

|                  |   |
|------------------|---|
| <port-list>      | Specifies the ports for which you want to display information.  |
| <b>all-ports</b> | Displays the selected information for all the X-Pedition ports. |

## Restrictions

None.

## Example

To display the bridging status for all available ports:

| xp# port show bridging-status all-ports |             |            |            |               |
|---|-------------|------------|------------|---------------|
| Port                                    | Mgmt Status | phy-state  | link-state | Bridging Mode |
| et.4.1                                  | No Action   | Disabled   | Link Down  | Address       |
| et.4.2                                  | No Action   | Disabled   | Link Down  | Address       |
| et.4.3                                  | No Action   | Forwarding | Link Up    | Address       |
| et.4.4                                  | No Action   | Disabled   | Link Down  | Address       |
| et.4.5                                  | No Action   | Disabled   | Link Down  | Address       |
| et.4.6                                  | No Action   | Forwarding | Link Up    | Address       |
| et.4.7                                  | No Action   | Disabled   | Link Down  | Address       |
| et.4.8                                  | No Action   | Disabled   | Link Down  | Address       |

## port show description

### Purpose

Display the user defined descriptions of X-Pedition ports.

### Format

**port show description** <port-list>|all-ports

### Mode

Enable.

### Description

The **port show description** command lets you display the user defined description for X-Pedition ports. The description is defined using the **port description** command.

### Parameters

|             |  |
|-------------|--|
| <port-list> | Specifies the ports for which you want to display the description. |
| all-ports   | Displays the description for all the X-Pedition ports.             |

### Restrictions

This command is valid for Ethernet and WAN only.

### Example

To display the bridging status for all available ports:

```
xp# port show description et.2.1
```

| Port Name | Description |
|-----------|-------------|
| et.2.1    | vlan1-2     |

# port show hash-mode

## Purpose

Displays the Layer 2 hash mode for a particular port(s).

## Format

**port show hash-mode** *<port-list>*|**all-ports**

## Mode

Enable.

## Description

The **port show hash-mode** command displays the Layer 2 hash mode used by a particular port(s). An example is displayed to show the resulting MAC address format by using this hash mode. See [port set on page 837](#) for a description of all hash modes.

## Parameters

|                          |   |
|--------------------------|---|
| <i>&lt;port-list&gt;</i> | Specifies the ports for which you will display the description. |
| <b>all-ports</b>         | Displays all X-Pedition ports.                                  |

## Restrictions

None.

## Example

To display the hash mode for port et.2.1:

```
xp# port show hash-mode et.2.1

L2 Port Hash Mode (assume a MAC address = 0011:2233:4455
-----
Port et.2.1      Mode-2      0011_3322_4455
```

## port show MAU

### Purpose

Displays Media Access Control information.

### Format

**port show MAU** *<port-list>* | **all-ports**

### Mode

Enable.

### Description

The **port show MAU** command displays Media Access Control (MAC) information. This command displays port number, media type, default media type, jack type, operational status, and support level.

### Parameters

|                          |  |
|--------------------------|--|
| <i>&lt;port-list&gt;</i> | Specifies the ports for which you want to display the description. |
| <b>all-ports</b>         | Displays the description for all the X-Pedition ports.             |

### Restrictions

None.

### Example

To display MAC information for port et.2.1:

|                                 |               |               |           |             |           |
|---------------------------------|---------------|---------------|-----------|-------------|-----------|
| xp# <b>port show MAU et.2.1</b> |               |               |           |             |           |
| Port                            | MUA Type      | Default Type  | Jack Type | Status      | Supported |
| -----                           | -----         | -----         | -----     | -----       | -----     |
| et.2.1                          | 100 BaseFX HD | 100 BaseFX HD | fiber SC  | operational | no        |

# port show MAU-statistics

## Purpose

Displays Media Access Control statistics.

## Format

**port show MAU-statistics** <port-list>|all-ports

## Mode

Enable.

## Description

The **port show MAU-statistics** command displays Media Access Control (MAC) statistics. This command displays port number, media availability, media availability state exits totals, jabber (excessively long frames) state, jabbering state enters totals, and false carriers totals.

## Parameters

|                  |  |
|------------------|--|
| <port-list>      | Specifies the ports for which you want to display the description. |
| <b>all-ports</b> | Displays the description for all the X-Pedition ports.             |

## Restrictions

None.

## Example

To display MAC statistics for port et.2.1:

| xp# <b>port show MAU-statistics et.2.1</b> |               |             |                    |                     |                    |       |
|--|---------------|-------------|--------------------|---------------------|--------------------|-------|
| Port                                       | Media Avail.  | State Exits | Media Avail. State | Jabber State Enters | Jabbering Carriers | False |
| et.2.1                                     | not available | 0           | other              | 0                   | 0                  |       |

## port show mc-vlan-encap

### Purpose

Displays the vlan ID where an outbound multicast packet on an 802.1q trunk port will be redirected.

### Format

**port show mc-vlan-encap** <port-list>|**all-ports**

### Mode

Enable.

### Description

The **port show mc-vlan-encap** command displays which vlan(s) to redirect the outbound multicast traffic to on a port or a list of ports. The X-Pedition router can forward multicast packets to only one vlan on an 802.1Q trunk. To resolve this problem, all outgoing multicast traffic on a Q trunk port is redirected to **vlan** <number>. On the other end of the Q trunk link, a SmartSwitch 2000/6000 is used and configured with VLAN classification. This allows multicast traffic to forward successfully.

### Parameters

|                  |   |
|------------------|---|
| <port-list>      | Specifies the ports for which you will display the description. |
| <b>all-ports</b> | Displays all X-Pedition ports.                                  |

### Restrictions

This command applies only to Q-trunk ports.

### Examples

To display the hash mode for port et.2.1:

```
xp# port show mc-vlan-encap et.4.6
Port et.4.6      MC Encapsulation Vlan: 10
```



# port show mirroring-status

## Purpose

Show the port mirroring status for ports in the X-Pedition chassis.

## Format

**port show mirroring-status** *<port list>* | **all-ports** | **all-acls**

## Mode

Enable.

## Description

The **port show mirroring-status** command shows the following port mirroring status information for the specified chassis ports:

- Whether port mirroring is enabled
- The ports or acls that are being mirrored
- The mirroring mode (input port, output port, or both)

## Parameters

|                          |   |
|--------------------------|---|
| <i>&lt;port list&gt;</i> | List of Ethernet ports or WAN modules. For example: et.1.3,hs.3,et.2.(1-3),se.4 |
| <b>all-ports</b>         | Display information for all ports.  |
| <b>all-acls</b>          | Display information for all flow mirroring rules.                               |

## Restrictions

None.

## Example

To display the port mirroring status for port 5:

```
xp(config)# port show mirroring-status 5
```

## port show port-status

### Purpose

Display various information about specified ports.

### Format

**port show port-status** *<port-list/SmartTRUNK-list>* | **all-ports** | **all-smarttrunks**

### Mode

Enable.

### Description

The **port show port-status command** lets you display port-status information for X-Pedition ports or SmartTRUNKs.

### Parameters

|  |  |
|--|--|
| <i>&lt;port-list /<br/>SmartTRUNK-list&gt;</i> | Specifies the LAN/WAN ports or SmartTRUNKs for which you want to display status information. |
| <b>all-ports</b>                               | Displays information for all the X-Pedition ports.   |
| <b>all-smarttrunks</b>                         | Displays information for all SmartTRUNKs.  |

### Restrictions

This command does not show Virtual Circuit (VC) information. To see the state of sub-interfaces, you need to use the appropriate facility command, such as the **frame-relay show stats** command.

## Example

To display the port status for all ports on Ethernet module 1 (et.1):

```
xp# port show port-status et.1.*
```

Flags: M - Mirroring enabled S - SmartTRUNK port

| Port   | Port Type            | Link Admin |          | State  | State       |       | Flags |
|--------|----------------------|------------|----------|--------|-------------|-------|-------|
|        |                      | Duplex     | Speed    |        | Negotiation | Flags |       |
| et.1.1 | 10/100-Mbit Ethernet | Half       | 10 Mbits | Manual | Up          | Up    |       |
| et.1.2 | 10/100-Mbit Ethernet | Half       | 10 Mbits | Manual | Up          | Up    |       |
| et.1.3 | 10/100-Mbit Ethernet | Half       | 10 Mbits | Manual | Up          | Up    |       |
| et.1.4 | 10/100-Mbit Ethernet | Half       | 10 Mbits | Manual | Up          | Up    |       |
| et.1.5 | 10/100-Mbit Ethernet | Half       | 10 Mbits | Manual | Up          | Up    |       |
| et.1.6 | 10/100-Mbit Ethernet | Half       | 10 Mbits | Manual | Up          | Up    |       |
| et.1.7 | 10/100-Mbit Ethernet | Half       | 10 Mbits | Manual | Up          | Up    |       |
| et.1.8 | 10/100-Mbit Ethernet | Half       | 10 Mbits | Manual | Up          | Up    |       |

# port show pvst-info

## Purpose

Display Spanning Tree (STP) information for a particular spanning tree.

## Format

**port show pvst-info** <port-list>|**all-ports** **spanning-tree** <string> [**rstp**]

## Mode

Enable.

## Description

The **port show pvst-info** command displays Spanning-Tree information for a particular spanning tree.

## Parameters

|                                  |   |
|----------------------------------|---|
| <port-list>  <b>all-ports</b>    | Specifies the ports for which you want to display information. The <b>all-ports</b> keyword displays the selected information for all the X-Pedition ports. |
| <b>spanning-tree</b><br><string> | Specifies the name of the spanning tree for which you want to display information.  |
| <b>rstp</b>                      | Display RSTP-related information.   |

## Restrictions

None.

## Example

To display the spanning tree information for spanning tree on all ports:

xp# port show pvst-info all-ports spanning-tree red

| Port   | Priority | Cost  | STP     | State      | Designated-Bridge | Designated Port |
|--------|----------|-------|---------|------------|-------------------|-----------------|
| ----   | -----    | ----- | -----   | -----      | -----             | -----           |
| et.7.1 | 008      | 00010 | Enabled | Forwarding | 8000:00001d17ed21 | 8 071           |
| et.7.2 | 000      | 00000 | Enabled | Disabled   | 0000:000000000000 | 0 000           |
| et.7.3 | 008      | 00010 | Enabled | Blocking   | 8000:00e0630457c0 | 8 005           |
| et.7.4 | 008      | 00010 | Enabled | Blocking   | 8000:00e0630457c0 | 8 006           |

xp# port show pvst-info all ports spanning-tree red rstp

| Port   | Port Role | Point To Point Status<br>(Admin/Oper) | Edge Port Status<br>(Admin/Oper) | Sends RSTP? |
|--------|-----------|---------------------------------------|----------------------------------|-------------|
| ----   | -----     | -----                                 | -----                            | -----       |
| et.7.1 | Root      | Auto/True                             | False/False                      | Yes         |
| et.7.2 | Disabled  | Auto/False                            | False/False                      | Yes         |
| et.7.3 | Alternate | Auto/True                             | False/False                      | Yes         |
| et.7.4 | Alternate | Auto/True                             | False/False                      | Yes         |

## port show serial-link-info

### Purpose

Displays the serial link information for X-Pedition ports.

### Format

**port show serial-link-info** <port-list>|**all-ports**

### Mode

Enable.

### Description

The **port show serial-link-info** command displays the status of the DTE-DCE control signals for particular ports.

### Parameters

|                  |   |
|------------------|---|
| <port-list>      | Specifies the port(s) to display all serial-port information. |
| <b>all-ports</b> | Displays all X-Pedition ports.                                |

### Restrictions

This command applies only to WAN ports.

### Examples

| xp# port show serial-link-info all-ports |            |     |     |         |      |     |       |
|--|------------|-----|-----|---------|------|-----|-------|
| Port                                     | Port Type  | CD  | CTS | RTS/DTR | DSR  | LL  | LINK  |
| ----                                     | -----      | - - | - - | -----   | ---- | --- | ----- |
| se.5.1                                   | V.35       | on  | on  | on      | on   | off | on    |
| se.5.2                                   | V.35       | on  | on  | on      | on   | off | on    |
| se.5.3                                   | WAN Serial | off | off | off     | off  | off | off   |
| se.5.4                                   | WAN Serial | off | off | off     | off  | off | off   |

**CD** Carrier Detected

**CTS** Clear To Send

**RTS/DTR** Request To Send/Data Terminal Ready

**DSR** Data Set Ready

**LL** Local Loopback

# port show stp-info

## Purpose

Display Spanning Tree (STP) information for X-Pedition ports.

## Format

**port show stp-info** *<port-list>***|all-ports** [**rstp**]

## Mode

Enable.

## Description

The **port show stp-info** command lets you display Spanning-Tree information for X-Pedition ports.

## Parameters

|                          |   |
|--------------------------|---|
| <i>&lt;port-list&gt;</i> | Specifies the ports for which you want to display information.  |
| <b>all-ports</b>         | Displays the selected information for all the X-Pedition ports. |
| <b>rstp</b>              | Displays RSTP-related information.                              |

## Restrictions

None.

## Example

To display the spanning tree information for all available ports:

| xp# port show stp-info all-ports |          |       |          |            |                   |       |
|----------------------------------|----------|-------|----------|------------|-------------------|-------|
| Port                             | Priority | Cost  | STP      | State      | Designated        |       |
|                                  |          |       |          |            | Designated-Bridge | Port  |
| ----                             | -----    | ----  | ---      | ----       | -----             | ----- |
| et.2.1                           | 008      | 00001 | Enabled  | Forwarding | 0064:00e06336b60e | 8 011 |
| et.2.2                           | 000      | 00000 | Disabled | Disabled   | 0000:000000000000 | 0 000 |
| et.2.3                           | 000      | 00000 | Disabled | Disabled   | 0000:000000000000 | 0 000 |
| et.2.4                           | 000      | 00000 | Disabled | Disabled   | 0000:000000000000 | 0 000 |
| et.2.5                           | 000      | 00000 | Disabled | Disabled   | 0000:000000000000 | 0 000 |
| et.2.6                           | 008      | 00010 | Enabled  | Forwarding | 07d0:00e0633680ce | 8 026 |
| et.2.7                           | 008      | 00010 | Enabled  | Forwarding | 07d0:00e0633680ce | 8 027 |
| et.2.8                           | 008      | 00010 | Enabled  | Forwarding | 07d0:00e0633680ce | 8 028 |
| gi.3.1                           | 008      | 00001 | Enabled  | Blocking   | 03e8:00e06334eb4e | 8 035 |
| gi.3.2                           | 008      | 00001 | Enabled  | Blocking   | 03e8:00e06334eb4e | 8 035 |

| xp# port show stp-info all-ports rstp |            |                       |                  |             |
|---------------------------------------|------------|-----------------------|------------------|-------------|
| Port                                  | Port Role  | Point To Point Status | Edge Port Status | Sends RSTP? |
|                                       |            | (Admin/Oper)          | (Admin/Oper)     |             |
| ----                                  | -----      | -----                 | -----            | -----       |
| et.2.1                                | Root       | Auto/True             | False/False      | Yes         |
| et.2.2                                | Disabled   | Auto/False            | False/False      | Yes         |
| et.2.3                                | Disabled   | Auto/False            | False/False      | Yes         |
| et.2.4                                | Disabled   | Auto/False            | False/False      | Yes         |
| et.2.5                                | Disabled   | Auto/False            | False/False      | Yes         |
| et.2.6                                | Designated | Auto/True             | True/True        | Yes         |
| et.2.7                                | Designated | Auto/True             | True/True        | Yes         |
| et.2.8                                | Designated | Auto/True             | True/True        | Yes         |
| gi.3.1                                | Alternate  | Auto/True             | False/False      | Yes         |
| gi.3.2                                | Alternate  | Auto/True             | False/False      | Yes         |



# port show vlan-info

## Purpose

Display VLAN information for X-Pedition ports.

## Format

**port show vlan-info** <port-list>|**all-ports**

## Mode

Enable.

## Description

The **port show vlan-info** command lets you display VLAN information about X-Pedition ports.

## Parameters

|                  |   |
|------------------|---|
| <port-list>      | Specifies the ports for which you want to display information.  |
| <b>all-ports</b> | Displays the selected information for all the X-Pedition ports. |

## Restrictions

None

## Example

To display the VLAN information for all available ports:

| xp# port show vlan-info all-ports |             |          |           |                |
|-----------------------------------|-------------|----------|-----------|----------------|
| Port                              | Access Type | IP VLANs | IPX VLANs | Bridging VLANs |
| -----                             | -----       | -----    | -----     | -----          |
| et.4.1                            | access      | DEFAULT  | DEFAULT   | DEFAULT        |
| et.4.2                            | access      | DEFAULT  | DEFAULT   | DEFAULT        |
| et.4.3                            | access      | DEFAULT  | DEFAULT   | DEFAULT        |
| et.4.4                            | access      | DEFAULT  | DEFAULT   | DEFAULT        |
| et.4.5                            | access      | DEFAULT  | DEFAULT   | DEFAULT        |
| et.4.6                            | access      | DEFAULT  | DEFAULT   | DEFAULT        |
| et.4.7                            | access      | DEFAULT  | DEFAULT   | DEFAULT        |
| et.4.8                            | access      | DEFAULT  | DEFAULT   | DEFAULT        |



# Chapter 51

## port-list Commands

The **port-list** commands provide a shorthand mechanism for specifying affected ports. Port-lists can consist of:

- List of one or more ports which may be non-consecutive
- Range of ports within a module
- Wildcard character to specify all the ports within a module

The **port-list** commands allow the port list to be compressed to create a single command with a port list from multiple commands, or expanded to create separate CLI commands for each port. After expanding a CLI command with a port list, each port can be managed separately without disturbing the operation of other ports in the port list. When the configuration changes are complete, CLI commands which have port lists may be compressed to reduce the size and simplify the configuration.

### Command Summary

[Table 44](#) lists the **port-list** commands. The sections following the table describe the command syntax.

**Table 44. port-list Commands**

|                           |
|---------------------------|
| <b>port-list compress</b> |
| <b>port-list expand</b>   |

# port-list compress

## Purpose

Compress a group of commands that contain individual port lists to one command with a combined port list.

## Format

**port-list compress**

## Mode

Configure.

## Description

The **port-list compress** command compresses a selected group of like commands that contain individual port lists into one command with a combined port list. When executed, a list of commands and their command numbers will be displayed. This is the list of possible commands currently in the active configuration that can be compressed. The user will then be prompted to give a list of command numbers to compress, or select "none" or "all" of the command numbers. If "none" is selected the command will exit without compressing any commands. If "all" is selected the command will compress all the listed commands. The compressing will be done on like commands that are grouped together. When a command is detected to be different from the previous commands, it becomes a part of the next group, and the previous group of commands will be compressed.

## Parameters

None.

## Restrictions

The following commands will not be compressed:

- Partial or errored commands.
- Commands which contain more than one port-list.
- Commands that contain the keyword "all-ports"
- Command with WAN port-lists which specify VCs (example at.1.1.0.100).

## Example

The following command compresses commands 12, 13, and 14.

```
xp(config)# port-list compress  
Port-list Commands:  
12: port set se.1.1 wan-encapsulation ppp speed 1536000  
13: port set se.1.3 wan-encapsulation ppp speed 1536000  
14: port set se.1.4 wan-encapsulation ppp speed 1536000  
24: ppp add-to-mlp mp.1 port se.1.3  
25: ppp add-to-mlp mp.1 port se.1.4  
Enter command line number(s) (ex. 1,2-5,10)  
to compress or 'all' or 'none': [none]? 12-14
```

If you look at the active configuration it will show commands 12-14 replaced with:

```
port set se.1.(1,3-4) wan-encapsulation ppp speed 1536000
```

# port-list expand

## Purpose

Expand a command that contains a port-list into commands with an individual port.

## Format

**port-list expand**

## Mode

Configure.

## Description

The **port-list expand** command expands a command that contain a port list into multiple commands that contain an each individual port from the port list. When executed, a list of commands and their command numbers will be displayed. This is the list of possible commands currently in the active configuration that can be expanded. The user will then be prompted to give a list of command numbers to expand, or select "none" or "all" of the command numbers. If "none" is selected the command will exit without expanding any commands. If "all" is selected the command will expand all the listed commands.

## Parameters

None.

## Restrictions

The following commands will not be expanded:

- Partial or errored commands.
- Commands which contain more that one port-list.
- Commands that contain the keyword "all-ports"
- Command with WAN port-lists which specify VCs (example at.1.1.0.100).

## Example

The following command expands the port list.

```
xp(config)# port-list expand  
Port-list Commands:  
 12: port set se.1.(1,3-4) wan-encapsulation ppp speed 1536000  
 24: ppp add-to-mlp mp.1 port se.1.(3-4)  
Enter command line number(s) (ex. 1,2-5,10)  
to expand or 'all' or 'none': [none]?12,24
```

If you look at the active configuration it will show command number 12 replaced with:

```
port set se.1.1 wan-encapsulation ppp speed 1536000  
port set se.1.3 wan-encapsulation ppp speed 1536000  
port set se.1.4 wan-encapsulation ppp speed 1536000
```

Command number 24 will be replaced with:

```
ppp add-to-mlp mp.1 port se.1.3  
ppp add-to-mlp mp.1 port se.1.4
```





# Chapter 52

## port mirroring Command

### port mirroring

#### Purpose

Apply port mirroring to a target port on an X-Pedition router or to traffic specified by an ACL profile.

#### Format

```
port mirroring dst-ports <port_list> [src-ports <port_list> | src-acl <acl name>]
```

#### Mode

Configure.

#### Description

The **port mirroring** command can be used to duplicate traffic from a single port to another single port, a single port to multiple ports, multiple ports to a single port, or multiple ports to multiple ports. You may also use the Port Mirroring facility in conjunction with an ACL. When you set up a mirror for traffic coming into the X-Pedition router that matches a specific ACL, the X-Pedition router mirrors the traffic out to one or more ports.

## Parameters

|                              |  |
|------------------------------|--|
| <b>dst-ports</b> <port_list> | The port(s) you will use to monitor activity. This is the port or port list to which you will want to connect the traffic sniffer.<br><br><b>Note:</b> This parameter replaces the monitor-port parameter from previous releases.  |
| <b>src-ports</b> <port_list> | The port(s) for which you want to monitor activity. You can specify any ports. Traffic will be mirrored from these ports to the monitor port.  |
| <b>src-acl</b> <acl name>    | The name of the ACL that specifies the profile of the traffic that you want to monitor. The ACL must be a previously created IP ACL. The ACL may contain either <b>permit</b> or <b>deny</b> keywords. The <b>port mirroring</b> command only looks at the following ACL rule parameter values: protocol, source IP address, destination IP address, source port, destination port, and TOS. |

## Restrictions

- Enterasys recommends that you monitor Gigabit ports through other Gigabit ports—you will almost certainly experience speed-inconsistency-related problems monitoring a Gigabit port through a 10Base-T or 100Base-TX port.
- When you enable L4-bridging on a mirrored ACL, the X-Pedition router will mirror only established unicast flows and ACL denied or dropped flows that match the given ACL.
- The X-Pedition router cannot mirror traffic from an ATM interface.
- ACLs and ports cannot be mirrored simultaneously.
- You may define up to 10 port mirrors via a maximum of 10 port mirroring commands and 128 ACL mirrors, but the actual limit will depend on the resources available.
- Packets that are lost due to CRC and BUFFER\_OVERFLOW errors are not mirrored to the destination port. If ACL mirroring is configured, packets dropped due to unresolved ARPs, rejected routes, and ICMP packets generated by the X-Pedition router in response to these will not be mirrored.
- Packets on mirrored Q-Trunk ports will not carry the IEEE 802.1Q tag header.
- Because the X-Pedition router mirrors packets after they are routed, the mirrored outputs for routed packets will appear to have the same destination MAC addresses as the egress flows, even when mirroring the ingress ports. Additionally, due to hardware limitation, these mirrored outputs will list the X-Pedition system MAC address as their source rather than the MAC address associated with the ingress or egress interface.

**Note:** This restriction does not apply to packets switched within the same VLAN.

For example, routed packets from source A to destination B on link 2 in the diagram below are seen leaving the X-Pedition router even when port 1.2 is being monitored. The mirrored output will list the X-Pedition system MAC address as its source, even if you create the link 1 and link 2 interfaces with different MAC addresses.



## Examples

To mirror traffic on ethernet ports et.2.2 to port et1.2:

```
xp(config)# port mirroring dst-ports et.1.2 src-ports et.2.2
```

After configuring et.1.2 as a monitor-port, et.1.2 is unusable for any other function in the system. This is indicated by a A LINK\_DOWN message. However, et.1.2 is capable of transmitting packets and its LED will be lit while in operation.

To mirror traffic that is specified by the profile in the ACL “101” to port et1.2:

```
xp(config)# port mirroring dst-ports et.1.2 src-acl 101
```



# Chapter 53

## ppp Commands

The **ppp** commands allow you to define Point-to-Point Protocol (PPP) service profiles, and specify and monitor PPP High-Speed Serial Interface (HSSI) and standard serial ports.

### Command Summary

[Table 45](#) lists the **ppp** commands. The sections following the table describe the command syntax.

**Table 45. ppp Commands**

|   |
|---|
| <b>ppp add-to-mlp</b> <mlp> <b>ports</b> <port list>  |
| <b>ppp apply service</b> <service name> <b>ports</b> <port list>  |
| <b>ppp clear stats-counter</b> [frame-drop-qdepth-counter] [max-frame-enqueued-counter]<br>[frame-drop-red-counter] [rmon] <b>ports</b> <port list>   |
| <b>ppp create-mlp</b> <mlp list> <b>slot</b> <number>   |
| <b>ppp define service</b> <service name> [bridging enable disable]<br>[high-priority-queue-depth <num>] [ip enable disable] [ipx enable disable]<br>[lcp-echo on off] [lcp-magic on off] [low-priority-queue-depth <num>]<br>[max-configure <num>] [max-failure <num>] [max-terminate <num>]<br>[med-priority-queue-depth <num>] [red on off] [red-maxTh-high-prio-traffic <num>]<br>[red-maxTh-low-prio-traffic <num>] [red-maxTh-med-prio-traffic <num>]<br>[red-minTh-high-prio-traffic <num>] [red-minTh-low-prio-traffic <num>]<br>[red-minTh-med-prio-traffic <num>] [retry-interval <num>] |
| <b>ppp restart lcp-ncp</b> <b>ports</b> <port list>   |
| <b>ppp set mlp-encaps-format</b> <b>ports</b> <port list> [format short-format]   |
| <b>ppp set mlp-frag-size</b> <b>ports</b> <port list> [size <size>]   |
| <b>ppp set mlp-fragq-depth</b> <b>ports</b> <port list> <b>qdepth</b> <number-of-packets>   |

**Table 45. ppp Commands (Continued)**

|  |
|--|
| <b>ppp set mlp-orderq-depth</b> <b>ports</b> <i>&lt;port list &gt;</i> <b>qdepth</b> <i>&lt;number-of-packets&gt;</i>  |
| <b>ppp set payload-compress</b> [ <b>max-histories</b> 0 1] [ <b>type</b> stac] <b>ports</b> <i>&lt;port list&gt;</i>  |
| <b>ppp set payload-encrypt</b> [ <b>type</b> des-bis] <b>ports</b> <i>&lt;port list&gt;</i>  |
| <b>ppp set peer-addr</b> [ <b>ip-address</b> <i>&lt;ipAddr&gt;</i> ] [ <b>ipx-address</b> <i>&lt;IPX address&gt;</i> ] [ <b>ports</b> <i>&lt;port list&gt;</i> ] |
| <b>ppp set ppp-encaps-bgd</b> <b>ports</b> <i>&lt;port list&gt;</i>  |
| <b>ppp show mlp</b> <i>&lt;mlp list&gt;</i>   <b>all-ports</b>   |
| <b>ppp show service</b> <i>&lt;service name&gt;</i>   <b>all</b>   |
| <b>ppp show stats</b> <b>ports</b> <i>&lt;port&gt;</i> [ <b>bridge-ncp</b> ] [ <b>ip-ncp</b> ] [ <b>link-status</b> ] [ <b>summary</b> ]                         |

# ppp add-to-mlp

## Purpose

Add PPP ports to an MLP bundle.

## Format

**ppp add-to-mlp** <mlp> **port** <port list>

## Mode

Configure.

## Description

The **ppp add-to-mlp** command allows you to add one or more PPP ports to a previously defined MLP bundle.

## Parameters

|             |  |
|-------------|--|
| <mlp>       | The name of the previously defined MLP bundle.     |
| <port list> | The WAN port(s) you want to add to the MLP bundle. |

## Restrictions

Usage is restricted to PPP WAN ports only.

## Example

To add the port “hs.3.1” to the MLP bundle “mp.1”:

```
xp(config)# ppp add-to-mlp mp.1 port hs.3.1
```

# ppp apply service

## Purpose

Apply a pre-defined service profile to an interface.

## Format

**ppp apply service** <service name> **ports** <port list>

## Mode

Configure.

## Description

Issuing the **ppp apply service ports** command allows you to apply a previously defined service profile to a given PPP WAN port.

## Parameters

|                |   |
|----------------|---|
| <service name> | The name of the previously defined service you wish to apply to the given port(s) or interfaces.  |
| <port list>    | The port(s) to which you wish to apply the pre-defined service profile. You can specify a single port or a comma-separated list of ports. |

## Restrictions

Usage is restricted to PPP WAN ports only.

## Example

To apply the service “s1” to slot 2, serial ports 1 and 2:

```
xp(config)# ppp apply service s1 ports se.2.1,se.2.2
```



# ppp clear stats-counter

## Purpose

Clears the specified statistics counter.

## Format

**ppp clear stats-counter** [**frame-drop-qdepth-counter**] [**max-frame-enqueued-counter**] [**frame-drop-red-counter**] [**rmon**] **ports** <port list>

## Mode

Enable.

## Description

The **ppp clear stats-counter** command allows you to specify a particular statistic counter and have the statistics reset to zero. There are statistic counters on each PPP WAN port, and you can use the **ppp clear stats-counter** to clear the counter for an individual WAN port or for a group of ports.

## Parameters

|                                   |   |
|-----------------------------------|---|
| <b>frame-drop-qdepth-counter</b>  | Specify this optional parameter to reset the frame drop counter to zero.          |
| <b>max-frame-enqueued-counter</b> | Specify this optional parameter to reset the max enqueued frames counter to zero. |
| <b>frame-drop-red-counter</b>     | Specify this optional parameter to reset the packet drop counter to zero.         |
| <b>rmon</b>                       | Specify this optional parameter to reset the rmon counter to zero.                |
| <port list>                       | The WAN port(s) that you wish to clear the counter.                               |

## Restrictions

Usage is restricted to PPP WAN ports only.

## Example

To clear the frame drop counter to zero on WAN port hs.3.1:

```
xp# ppp clear stats-counter frame-drop-qdepth-counter ports hs.3.1
```

## ppp create-mlp

### Purpose

Create MLP bundles.

### Format

**ppp create-mlp** <mlp list> **slot** <number>

### Mode

Configure.

### Description

The **ppp create-mlp** command allows you to create one or more MLP bundles.

### Parameters

|            |  |
|------------|--|
| <mlp list> | The name(s) of the MLP bundles you want to create. You can specify a single bundle or a comma-separated list of MLP bundles. |
| <slot>     | The slot number for the MLP bundle(s).   |

### Restrictions

Usage is restricted to PPP WAN ports only.

### Example

To create the MLP bundle “mp.1” for slot 1:

```
xp(config)# ppp create-mlp mp.1 slot 1
```

# ppp define service

## Purpose

Define a service profile for WAN ports.

## Format

```
ppp define service <service name> [bridging enable|disable]
[high-priority-queue-depth <num>] [ip enable|disable] [ipx enable|disable] [lcp-echo on|off]
[lcp-magic on|off] [low-priority-queue-depth <num>] [max-configure <num>]
[max-failure <num>] [max-terminate <num>] [med-priority-queue-depth <num>] [red on|off]
[red-maxTh-high-prio-traffic <num>] [red-maxTh-low-prio-traffic <num>]
[red-maxTh-med-prio-traffic <num>] [red-minTh-high-prio-traffic <num>]
[red-minTh-low-prio-traffic <num>] [red-minTh-med-prio-traffic <num>]
[retry-interval <num>]
```

## Mode

Configure.

## Description

The **ppp define service** command allows you to specify the following attributes for a newly created service profile:

- Activate and deactivate bridging, IP, and/or IPX for PPP WAN ports. If you do not specify any bridging, IP, or IPX protocols for PPP WAN ports, they are all activated by default. If you specify a bridging, IP, or IPX protocol, you *must* also explicitly define the behavior of the other two (i.e., **enabled** or **disabled**).
- The allowable PPP queue depth for high-, low-, and medium-priority items.
- Enable and disable the sending of LCP Echo Request messages. LCP Echo Requests and their corresponding LCP Echo Responses determine if a link to a peer is down.
- Enable and disable the use of LCP magic numbers. Magic numbers are used to help detect loopback conditions.
- The maximum allowable number of unanswered/improperly answered configuration requests before determining that the connection to the peer is lost.
- The maximum allowable number of negative-acknowledgment responses for a given interface before declaring an inability to converge.
- The maximum allowable unacknowledged terminate requests before determining that the peer is unable to respond.
- Activate or deactivate Random Early Discard (RED) for PPP ports.

- The maximum and minimum threshold values for RED high-, low-, and medium-priority traffic.

In general, Enterasys recommends that the maximum threshold values be less than or equal to the respective high-, low-, or medium-priority queue depth. The minimum threshold values should be one-third of the respective maximum threshold.

- The number of seconds that will pass before a subsequent “resending” of the configuration request will be transmitted.

## Parameters

|   |   |
|---|---|
| <i>&lt;service name&gt;</i>                         | The name you wish to assign to the newly created service profile.   |
| <b>bridging enable disable</b>                      | Specifying the <b>enable</b> keyword activates bridging for PPP WAN ports. Specifying the <b>disable</b> keyword deactivates bridging for PPP WAN ports.  |
| <b>high-priority-queue-depth</b> <i>&lt;num&gt;</i> | The number of items allowed in the PPP queue. You can specify a number between 1 and 65,535. Enterasys recommends a value within the 5 - 100 item range. The default value is 20.   |
| <b>ip enable disable</b>                            | Specifying the <b>enable</b> keyword activates IP for PPP WAN ports. Specifying the <b>disable</b> keyword deactivates IP for PPP WAN ports.  |
| <b>ipx enable disable</b>                           | Specifying the <b>enable</b> keyword activates IPX for PPP WAN ports. Specifying the <b>disable</b> keyword deactivates IPX for PPP WAN ports.  |
| <b>lcp-echo on off</b>                              | Specifying the <b>on</b> keyword enables the sending of LCP Echo Request messages. Specifying the <b>off</b> keyword disables the sending of LCP Echo Request messages. The sending of LCP Echo Requests is enabled by default. |
| <b>lcp-magic on off</b>                             | Specifying the <b>on</b> keyword enables the use of LCP magic numbers. Specifying the <b>off</b> keyword disables the use of LCP magic numbers. The use of LCP magic numbers is enabled by default.                             |
| <b>low-priority-queue-depth</b> <i>&lt;num&gt;</i>  | The number of items allowed in the PPP queue. You can specify a number between 1 and 65,535. Enterasys recommends a value within the 5 - 100 item range. The default value is 20.   |
| <b>max-configure</b> <i>&lt;num&gt;</i>             | The maximum allowable number of unanswered requests. You can specify any number greater than or equal to 1. The default value is 10.  |
| <b>max-failure</b> <i>&lt;num&gt;</i>               | The maximum allowable number of negative-acknowledgment transmissions. You can specify any number greater than or equal to 1. The default value is 5.   |
| <b>max-terminate</b> <i>&lt;num&gt;</i>             | The maximum allowable number of unanswered/improperly answered connection-termination requests before declaring the link to a peer lost. You can specify any number greater than or equal to 1. The default value is 2.         |

|  |   |
|--|---|
| <b>med-priority-queue-depth</b> <num>    | The number of items allowed in the PPP queue. You can specify a number between 1 and 65,535. Enterasys recommends a value within the 5 - 100 item range. The default value is 20. |
| <b>red on off</b>                        | Specifying the <b>on</b> keyword enables RED for PPP WAN ports. Specifying the <b>off</b> keyword disables RED for PPP WAN ports.   |
| <b>red-maxTh-high-prio-traffic</b> <num> | The maximum allowable threshold for high-priority RED traffic. You can specify a number between 1 and 65,535. The default value is 12.  |
| <b>red-maxTh-low-prio-traffic</b> <num>  | The maximum allowable threshold for low-priority RED traffic. You can specify a number between 1 and 65,535. The default value is 12.   |
| <b>red-maxTh-med-prio-traffic</b> <num>  | The maximum allowable threshold for medium-priority RED traffic. You can specify a number between 1 and 65,535. The default value is 12.  |
| <b>red-minTh-high-prio-traffic</b> <num> | The minimum allowable threshold for high-priority RED traffic. You can specify a number between 1 and 65,535. The default value is 4.   |
| <b>red-minTh-low-prio-traffic</b> <num>  | The minimum allowable threshold for low-priority RED traffic. You can specify a number between 1 and 65,535. The default value is 4.  |
| <b>red-minTh-med-prio-traffic</b> <num>  | The minimum allowable threshold for medium-priority RED traffic. You can specify a number between 1 and 65,535. The default value is 4.   |
| <b>retry-interval</b> <num>              | The number of seconds between subsequent configuration request transmissions (the interval). You can specify any number greater than or equal to 1. The default value is 30.      |

## Restrictions

Usage is restricted to PPP WAN ports only.

## Example

To create a service profile named “pppserv4” with the following attributes:

- Bridging enabled
- IP and IPX enabled
- LCP Echo Requests disabled
- LCP magic numbers disabled
- RED disabled
- A retry interval of 20 seconds

Enter the following command line in Configure mode:

```
xp(config)# ppp define service pppserv4 bridging enable ip enable ipx enable lcp-echo off lcp-magic off red off retry-interval 20
```

## ppp restart lcp-ncp

### Purpose

Restart PPP LCP/NCP negotiation.

### Format

**ppp restart lcp-ncp ports** *<port list>*

### Mode

Enable.

### Description

The **ppp restart lcp-ncp** command allows you to reset and restart the LCP/NCP negotiation process for PPP WAN ports.

### Parameters

---

|                          |   |
|--------------------------|---|
| <i>&lt;port list&gt;</i> | The ports for which you would like to re-establish LCP/NCP negotiation. |
|--------------------------|---|

---

### Restrictions

This command line is available only for PPP WAN ports.

### Example

To restart LCP/NCP negotiation on serial ports 1 and 2 of slot 4:

|  |
|--|
| xp# <b>ppp restart lcp-ncp ports se.4.1,se.4.2</b> |
|--|

# ppp set mlp-encaps-format

## Purpose

Set MLP encapsulation format.

## Format

**ppp set mlp-encaps-format ports** *<port list>* [**format short-format**]

## Mode

Configure.

## Description

The **ppp set mlp-encaps-format** command allows you to specify the encapsulation format for MLP bundles. If this command is not configured, long format encapsulation is used for MLP bundles.

## Parameters

|                            |   |
|----------------------------|---|
| <i>&lt;port list&gt;</i>   | The MLP port(s) to which you want to apply the encapsulation format |
| <b>format short-format</b> | Specifies the use of short format for MLP encapsulation.            |

## Restrictions

Usage is restricted to PPP WAN ports only.

## Example

To specify short format encapsulation for the MLP bundles “mp.1” and “mp.4-7”:

```
xp(config)# ppp set mlp-encaps-format ports mp.1,mp.4-7 format short-format
```

## ppp set mlp-frag-size

### Purpose

Set the frame size under which no MLP fragmentation is needed.

### Format

**ppp set mlp-frag-size ports** *<port list>* [**size** *<size>*]

### Mode

Configure.

### Description

The **ppp set mlp-frag-size** command allows you to set the frame size under which no fragmentation is needed for transmission on the MLP bundle. The default size is 1500 bytes. Any frames that are less than the value set by the **ppp set mlp-frag-size** command are not fragmented. Any frames that are over the value are fragmented for transmission on the MLP bundle.

### Parameters

|                          |  |
|--------------------------|--|
| <i>&lt;port list&gt;</i> | The MLP port(s) to which the frame size applies.   |
| <i>&lt;size&gt;</i>      | The size of the frame, in bytes, that are fragmented by MLP. The value can be between 64 and 1500, inclusive. The default value is 1500. |

### Restrictions

Usage is restricted to PPP WAN ports only.

### Example

To specify that frames of 200 bytes or more are fragmented on the MLP bundles “mp.1” and “mp.4-7”:

```
xp(config)# ppp set mlp-frag-size ports mp.1,mp.4-7 size 200
```



# ppp set mlp-fragq-depth

## Purpose

Set the depth of the MLP fragment queue.

## Format

**ppp set mlp-fragq-depth ports** *<port list>* **qdepth** *<number-of-packets>*

## Mode

Configure.

## Description

The **ppp set mlp-fragq-depth** command allows you to set the depth of the queue used by MLP to hold packet fragments for reassembly.

## Parameters

|                                  |  |
|----------------------------------|--|
| <i>&lt;port list&gt;</i>         | The MLP port(s) to which the queue depth applies.  |
| <i>&lt;number-of-packets&gt;</i> | The depth of the queue, in packets, to hold unassembled packet fragments. The value can be between 100 and 4000, inclusive. The default value is 1000. |

## Restrictions

Usage is restricted to MLP WAN ports only.

## Example

To specify a queue depth of 2500 packets to hold fragments for reassembly on the MLP bundles “mp.1”:

```
xp(config)# ppp set mlp-fragq-depth ports mp.1 size 2500
```

# ppp set mlp-orderq-depth

## Purpose

Set the depth of the MLP packet order queue.

## Format

**ppp set mlp-orderq-depth ports** *<port list>* **qdepth** *<number-of-packets>*

## Mode

Configure.

## Description

The **ppp set mlp-orderq-depth** command allows you to set the depth of the queue used by MLP to hold MLP packets for preserving the packet order.

## Parameters

|                                  |   |
|----------------------------------|---|
| <i>&lt;port list&gt;</i>         | The MLP port(s) to which the queue depth applies.   |
| <i>&lt;number-of-packets&gt;</i> | The depth of the queue, in packets, to hold MLP packets. The value can be between 100 and 4000, inclusive. The default value is 1000. |

## Restrictions

Usage is restricted to MLP WAN ports only.

## Example

To specify a queue depth of 2500 packets to hold packets for reordering on the MLP bundles “mp.1”:

```
xp(config)# ppp set mlp-orderq-depth ports mp.1 size 2500
```

# ppp set payload-compress

## Purpose

Enables packet compression for PPP ports.

## Format

**ppp set payload-compress** [**max-histories** <number>] [**type stac**] **ports** <port list>

## Mode

Configure.

## Description

The **ppp set payload-compress** command allows you to enable the Stacker payload compression. You can enable compression on a single port, an entire multilink PPP (MLP) bundle, or on individual ports that are members of a multilink PPP bundle. If this command is not configured, payload compression is not enabled.

## Parameters

|                  |  |
|------------------|--|
| <number>         | Specifies the maximum number of compression history buffers to be kept. You can specify either 0 or 1. Specifying 0 disables the keeping of any histories and each packet is individually compressed. Specifying 1 allows a history buffer to be kept, which may result in better compression. The default value is 1. |
| <b>type stac</b> | Specifies the Stacker (STAC LZS) compression algorithm. This is the default.   |
| <port list>      | The port(s) on which you want to enable payload compression. You can specify a single port or a comma-separated list of ports.   |

## Restrictions

Usage is restricted to PPP WAN ports only.

## Example

To enable LZS Stac payload compression on slot 4, on serial port 2:

```
xp(config)# ppp set payload-compress ports se.4.2
```

# ppp set payload-encrypt

## Purpose

Enables packet encryption for PPP ports.

## Format

**ppp set payload-encrypt** [**type des-bis**] **ports** <port list>

## Mode

Configure.

## Description

The **ppp set payload-encrypt** command allows you to enable the encryption of packets using the DES-bis algorithm. You can enable encryption on a single port, an entire multilink PPP (MLP) bundle, or on individual ports that are members of an MLP bundle. If this command is not configured, payload encryption is not enabled.

## Parameters

|                     |   |
|---------------------|---|
| <b>type des-bis</b> | Specifies the DES-bis encryption algorithm. This is the default.  |
| <port list>         | The port(s) on which you want to enable payload encryption. You can specify a single port or a comma-separated list of ports. |

## Restrictions

Usage is restricted to PPP WAN ports only.

## Example

To enable DES-bis payload encryption on slot 4, on serial port 2:

```
xp(config)# ppp set payload-encrypt ports se.4.2
```

**Note:** After the router executes this command, the CLI will prompt the user for transmit-key and receive-key information.

# ppp set peer-addr

## Purpose

Set the peer address in case that IPCP/IPXCP can't resolve the address.

## Format

**ppp set peer-addr** [**ip-address** <IP address>] [**ipx-address** <IPX address>] [**ports** <port list>]

## Mode

Configure.

## Description

Issuing the **ppp set peer-addr** command allows you to set the peer address if it can't be resolved by IPCP or IPXCP.

## Parameters

|           |   |
|-----------|---|
| <address> | The IP or IPX address you wish to use.            |
| <port>    | The port to which you wish to assign the address. |

## Restrictions

Usage is restricted to PPP port only.

## Example

To assign an IP address 10.1.1.1/16 to slot 2, serial port 1:

```
xp(config)# ppp set peer-addr ip-address 10.1.1.1/16 ports se.2.1
```

## ppp set ppp-encaps-bgd

### Purpose

Force the ingress packets to be encapsulated in bridged format.

### Format

**ppp set ppp-encaps-bgd ports** *<port list>*

### Mode

Configure.

### Description

Issuing the **ppp set ppp-encaps-bgd** command allows you to use bridged format encapsulation on a given ppp port.

### Parameters

|                          |   |
|--------------------------|---|
| <i>&lt;port list&gt;</i> | The port(s) to which you wish to use bridged encapsulation. You can specify a single port or a comma-separated list of ports. |
|--------------------------|---|

### Restrictions

Usage is restricted to ppp port only.

### Example

To force the bridged encapsulation to slot 2, serial ports 1 and 2:

```
xp(config)# ppp set ppp-encaps-bgd ports se.2.1,se.2.2
```

# ppp show mlp

## Purpose

Displays the PPP ports that have been added into an MLP bundle.

## Format

**ppp show mlp** *<mlp list>***|all-ports**

## Mode

Enable.

## Description

The **ppp show mlp** command allows you to display information about one or more MLP bundles.

## Parameters

|                         |   |
|-------------------------|---|
| <i>&lt;mlp list&gt;</i> | The name(s) of the MLP bundles on which you want information. You can specify a single bundle or a comma-separated list of MLP bundles. |
| <b>all-ports</b>        | Displays information on all MLP ports.  |

## Restrictions

None.

## Example

To display the PPP ports for mp.1:

```
xp# ppp show mlp mp.1
mp.1:
Slot: 4
PPP ports: se.4.1,se.4.3
```

# ppp show service

## Purpose

Displays PPP service profiles.

## Format

**ppp show service** *<service name>*|**all**

## Mode

Enable.

## Description

The **ppp show service** command allows you to display one or all of the available PPP service profiles.

## Parameters

|                             |   |
|-----------------------------|---|
| <i>&lt;service name&gt;</i> | The service profile you wish to display.            |
| <b>all</b>                  | Displays all of the available PPP service profiles. |

## Restrictions

None.

## Example

To display the available PPP service profiles named profile\_4:

```
xp# ppp show service profile_4
```



# ppp show stats

## Purpose

Displays bridge NCP, IP NCP, and link-status parameters.

## Format

**ppp show stats ports** <port> [**bridge-ncp**] [**ip-ncp**] [**link-status**] [**summary**]

## Mode

Enable.

## Description

The **ppp show stats** command allows you to display parameters for bridge NCP, IP NCP, and link-status on PPP WAN ports. You can specify one, two, or three of the available parameter types.

## Parameters

|                    |  |
|--------------------|--|
| <port>             | The PPP WAN port for which you wish to view bridge NCP, IP NCP, and/or link-status parameters. |
| <b>bridge-ncp</b>  | Specifies that you wish to view bridging NCP parameters for the given port.                    |
| <b>ip-ncp</b>      | Specifies that you wish to view IP NCP parameters for the given port.                          |
| <b>link-status</b> | Specifies that you wish to view link-status parameters for the given port.                     |
| <b>summary</b>     | Specifies that you wish to view summarized display.  |

## Restrictions

None.

## Example

To display the available link-status and IP NCP parameters for the PPP WAN interface located at slot 4, port 1:

```
xp# ppp show stats ports se.4.1 ip-ncp link-status
```



# Chapter 54

## pvst Commands

The **pvst** commands let you display and change settings for a VLAN spanning tree.

### Command Summary

[Table 46](#) lists the **pvst** commands. The sections following the table describe the command syntax.

**Table 46.** pvst Commands

|   |
|---|
| <b>pvst create spanningtree</b> <b>vlan-name</b> <i>&lt;string&gt;</i>  |
| <b>pvst enable port</b> <i>&lt;port-list&gt;</i> <b>spanning-tree</b> <i>&lt;string&gt;</i>   |
| <b>pvst set bridging</b> [ <b>forward-delay</b> <i>&lt;num&gt;</i> ] [ <b>hello-time</b> <i>&lt;num&gt;</i> ] [ <b>max-age</b> <i>&lt;num&gt;</i> ]<br>[ <b>priority</b> <i>&lt;num&gt;</i> ] <b>spanning-tree</b> <i>&lt;string&gt;</i>  |
| <b>pvst set port</b> <i>&lt;port-list&gt;</i> <b>priority</b> <i>&lt;num&gt;</i> <b>port-cost</b> <i>&lt;num&gt;</i> <b>spanning-tree</b> <i>&lt;string&gt;</i><br><b>point-to-point</b> [ <b>ForceTrue</b>   <b>ForceFalse</b>   <b>Auto</b> ] <b>edge-port</b> [ <b>True</b>   <b>False</b> ] |
| <b>pvst show bridging-info</b> <b>spanning-tree</b> <i>&lt;string&gt;</i>   |
| <b>pvst reset-rstp port</b> <i>&lt;port-list&gt;</i> <b>spanning-tree</b> <i>&lt;string&gt;</i>   |
| <b>pvst set protocol-version rstp</b> <b>spanning-tree</b> <i>&lt;string&gt;</i>  |
| <b>pvst set no-special-encap</b>  |

**Note:** The X-Pedition router does *not* support PVST over POS. However, the router *will* support STP over POS.

# pvst create spanningtree

## Purpose

Create an instance of spanning tree for a particular VLAN.

## Format

**pvst create spanningtree** **vlan-name** *<string>*

## Mode

Configure.

## Description

The **pvst create spanningtree** command creates a spanning tree instance for a particular VLAN.

## Parameters

---

|  |  |
|--|--|
| <b>vlan-name</b> <i>&lt;string&gt;</i> | The name of the VLAN for which a new instance of spanning tree is to be created. |
| <b>Note:</b>                           | The X-Pedition router displays VLAN names up to 32 characters in length.         |

---

## Restrictions

None.

# pvst enable port spanning-tree

## Purpose

Enable PVST on one or more ports on a particular spanning tree.

## Format

**pvst enable port** *<port-list>* **spanning-tree** *<string>*

## Mode

Configure.

## Description

The **pvst enable port** command enables STP on the specified port for the specified spanning tree.

## Parameters

|                          |   |
|--------------------------|---|
| <i>&lt;port-list&gt;</i> | The ports on which you are enabling STP. You can specify a single port or a comma-separated list of ports. Example: et.1.3,et.(1-3).(4,6-8).  |
| <i>&lt;string&gt;</i>    | The name of the spanning-tree instance. This name is the same as the VLAN name.<br><br><b>Note:</b> For default VLAN, use <b>stp</b> commands. The X-Pedition router displays VLAN names up to 32 characters in length. |

## Restrictions

For PVST, the spanning tree instance must have previously been created.

# pvst set bridging spanning-tree

## Purpose

Set STP bridging parameters for a particular VLAN.

## Format

```
pvst set bridging [forward-delay <num>] [hello-time <num>] [max-age <num>]  
[priority <num>] spanning-tree <string>
```

## Mode

Configure.

## Description

The **pvst set bridging spanning-tree** command lets you configure the following STP parameters for a particular VLAN:

- Bridging priority
- Hello time
- Maximum age
- Forward delay

## Parameters

|                                  |   |
|----------------------------------|---|
| <b>forward-delay</b><br><num>    | Sets the STP forward delay for the X-Pedition router. The forward delay is measured in seconds. Specify a number from 4– 30. The default is 15.   |
| <b>hello-time</b> <num>          | Sets the STP hello time for the X-Pedition router. The hello time is measured in seconds. Specify a number from 1– 10. The default is 2.  |
| <b>max-age</b> <num>             | Sets the STP maximum age for the X-Pedition router. Specify a number from 6–40. The default is 20.  |
| <b>priority</b> <num>            | Sets the STP bridging priority for the X-Pedition router. Specify a number from 0 – 65535. The default is 32768.  |
| <b>spanning-tree</b><br><string> | The name of the spanning-tree instance. This name is the same as the VLAN name.<br><br><b>Note:</b> For default VLAN, use <b>stp</b> commands. The X-Pedition router displays VLAN names up to 32 characters in length. |

## Restrictions

For PVST, the spanning tree instance must have previously been created.

## Examples

To set the bridging priority of Spanning Tree for VLAN ip1 to 1:

```
xp(config)# pvst set bridging priority 1 spanning-tree ip1
```

# pvst set port

## Purpose

Set PVST port priority and port cost for ports for a particular VLAN.

## Format

```
pvst set port <port-list> priority <num> port-cost <num> spanning-tree <string>  
point-to-point [forcetrue|forcefalse|auto] edge-port [true|false]
```

## Mode

Configure.

## Description

The **pvst set port** command sets the STP priority and port cost for individual ports for a particular VLAN.

## Parameters

|  |   |
|--|---|
| <b>port</b> <port-list>  | The port(s) for which you are setting STP parameters. You can specify a single port or a comma-separated list of ports.<br>Example: et.1.3,et.(1-3).(4,6-8).  |
| <b>priority</b> <num>  | The priority you are assigning to the port(s). Specify a number from 0– 16 inclusive. The default is 8.   |
| <b>port-cost</b> <num>   | The STP cost you are assigning to the port(s). Specify a number from 1– 65535. The default depends on the port speed: 1 for Gigabit (100-Mbps) ports, 10 for 100-Mbps ports, and 100 for 10-Mbps ports. |
| <b>spanning-tree</b> <string>  | The name of the spanning-tree instance. This name is the same as the VLAN name.<br><br><b>Note:</b> The X-Pedition router displays VLAN names up to 32 characters in length.                            |
| <b>point-to-point</b> [ <b>ForceTrue</b>   <b>ForceFalse</b>   <b>Auto</b> ] | Specify a point-to-point or a non-point-to-point link administratively. The default is <b>Auto</b> .  |
| <b>edge-port</b> [ <b>True</b>   <b>False</b> ]                              | Specify whether the port(s) should be initialized as an edge port or a non-edge port. The default is <b>False</b> .<br><br><b>Note:</b> For default VLAN, use <b>stp</b> commands.                      |



## Restrictions

- For PVST, the spanning tree instance must have previously been created.
- The X-Pedition ER16 router can support up to 480 ports, which exceeds the 256-port limit allowed by the 8-bit port number field specified in the IEEE 802.1D-1998 standard. To accommodate the increase in the number of supported ports, Enterasys extended the port field to a 12-bit value and decreased the port priority field to a 4-bit value. As a result, the X-Pedition router allows STP or PVST port configurations with a priority of 0 to 15 only. In spite of these changes, the X-Pedition router remains compatible with other switches.

# pvst show bridging-info spanning-tree

## Purpose

Display STP bridging information for a particular VLAN.

## Format

**pvst show bridging-info spanning-tree** *<string>*

## Mode

Enable.

## Description

The **pvst show bridging-info** command displays STP bridging information for a particular VLAN.

## Parameters

|   |   |
|---|---|
| <b>spanning-tree</b><br><i>&lt;string&gt;</i> | The name of the spanning-tree instance. This name is the same as the VLAN name.                                     |
| <b>Note:</b>                                  | For default VLAN, use <b>stp</b> commands. The X-Pedition router displays VLAN names up to 32 characters in length. |

## Restrictions

For PVST, the spanning tree instance must have previously been created.

# pvst reset-rstp spanning-tree

## Purpose

Reset RSTP.

## Format

**pvst reset-rstp port** *<port list>* **spanning-tree** *<string>*

## Mode

Enable.

## Description

The **pvst reset-rstp spanning-tree** command resets the point-to-point and edge port parameters to user-specified values and forces the specified ports to send RSTP BPDUs until a version 0 STP BPDU is received.

## Parameters

|   |   |
|---|---|
| <b>port</b> <i>&lt;port-list&gt;</i>          | The port(s) for which you are setting the STP parameters. You can specify a single port or a comma-separated list of ports.<br>For example: et.1.3, et.(1-3).(4,6-8).   |
| <b>spanning-tree</b><br><i>&lt;string&gt;</i> | The name of the spanning-tree instance. This name is the same as the VLAN name.<br><br><b>Note:</b> As a default, use the <b>stp</b> commands. The X-Pedition router displays VLAN names up to 32 characters in length. |

## Restrictions

For PVST, the spanning tree instance must have previously been created.

# pvst set protocol-version rstp spanning-tree

## Purpose

Set PVST version to 2 (IEEE 802.1w).

## Format

**stp set protocol-version rstp spanning-tree** <string>

## Mode

Configure.

## Description

The **stp set protocol-version** command changes the STP version from *STP compatible* (version 0) to *Rapid Spanning Tree Protocol* (version2).

## Parameters

|                                  |   |
|----------------------------------|---|
| <b>spanning-tree</b><br><string> | The name of the spanning-tree instance. This name is the same as the VLAN name. |
| <b>Note:</b>                     | The X-Pedition router displays VLAN names up to 32 characters in length.        |

## Restrictions

For PVST, the spanning tree instance must have previously been created.

# **pvst set no-special-encap**

## **Purpose**

To disable PVST encapsulation on all port-based VLANs.

## **Format**

**pvst set no-special-encap**

## **Mode**

Configure.

## **Description**

The **stp set no-special-encap** command forces the X-Pedition router's port-based VLAN to send and receive IEEE standard BPDU's. Issue this command if PVST needs to be compatible with STP.

## **Parameters**

None.

## **Restrictions**

None.



# Chapter 55

## qos Commands

The **qos** commands define and display Quality of Service (QoS) parameters. Use the command to classify Layer 2, Layer 3, and Layer 4 traffic into the following priorities:

- control
- high
- medium
- low

By assigning priorities to network traffic, you can ensure that critical traffic will reach its destination even if the exit ports for the traffic are experiencing greater than maximum utilization. Use the **qos set l2**, **qos set ip**, and **qos set ipx** commands to assign priorities for Layer-2, IP, and IPX traffic respectively.

### Flows

For Layer 3 (IP and IPX) traffic, you can define “flows”, blueprints or templates of IP and IPX packet headers.

- The IP fields are source IP address, destination IP address, UDP/TCP source port, UDP/TCP destination port, TOS (Type of Service), transport protocol (TCP or UDP) and a list of incoming interfaces.
- The IPX fields are source network, source node, destination network, destination node, source port, destination port, and a list of incoming interfaces.

The flows specify the contents of these fields. If you do not enter a value for a field, a wildcard value (all values acceptable) is assumed for the field.

## Precedence

A precedence from 1 – 7 is associated with each field in a flow. The X-Pedition router uses the precedence value associated with the fields to break ties if packets match more than one flow. The highest precedence is 1 and the lowest is 7. Here are the default precedences of the fields:

- **IP** – destination port (1), destination address (2), source port (3), source IP address (4), TOS (5), interface (6), protocol (7).
- **IPX** – destination network (1), source network (2), destination node (3), source node (4), destination port (5), source port (6), interface (7).

Use the **qos precedence ip** and **qos precedence ipx** commands to change the default precedences.

## Queuing Policies

You can use one of two queuing policies on the X-Pedition router:

- **strict priority** – assures the higher priorities of throughput but at the expense of lower priorities. For example, during heavy loads, low-priority traffic can be dropped to preserve throughput of control-priority traffic, and so on.
- **weighted fair queuing** – distributes priority throughput among the four priorities (control, high, medium, and low) based on percentages.

The X-Pedition router can use only one queuing policy at a time. The policy is used on the entire X-Pedition router. The default queuing policy is strict priority.

## Command Summary

[Table 47](#) lists the **qos** commands. The sections following the table describe the command syntax.

**Table 47. qos Commands**

|   |
|---|
| <b>qos apply priority-map</b> <string> <b>ports</b> <port list>   |
| <b>qos create priority-map</b> <string> <num> <b>control</b>   <b>low</b>   <b>med</b>   <b>high</b>  |
| <b>qos precedence ip</b> [sip <num>] [dip <num>] [srcport <num>] [destport <num>]<br>[tos <num>] [protocol <num>] [intf <num>]  |
| <b>qos precedence ipx</b> [srcnet <num>] [srcnode <num>] [srcport <num>] [dstnet <num>]<br>[dstnode <num>] [dstport <num>] [intf <num>]   |
| <b>qos priority-map off</b>   |
| <b>qos wred input</b> [port <port list> all-ports] [queue control high medium low]<br>[exponential-weighting-constant <num>] [min-queue-threshold <num>]<br>[max-queue-threshold <num>] [mark-prob-denominator <num>] |



Table 47. qos Commands (Continued)

|   |
|---|
| <b>qos set ip</b> <name> <priority>  <b>low</b>   <b>medium</b>   <b>high</b>   <b>control</b>   <b>num</b> <srcaddr/mask>  <b>any</b> <dstaddr/mask>  <b>any</b> <srcport>  <b>any</b> <dstport>  <b>any</b> <tos> <interface-list>  <b>any</b> <protocol>                           |
| <b>qos set ipx</b> <name> <priority>  <b>low</b>   <b>medium</b>   <b>high</b>   <b>control</b>   <b>num</b> <srcnet>  <b>any</b> <srcmask>  <b>any</b> <srcport>  <b>any</b> <dstnet>  <b>any</b> <dstmask>  <b>any</b> <dstport> <interface-list>  <b>any</b>                       |
| <b>qos set l2 name</b> <name> <b>source-mac</b> <MACaddr> <b>source-mac-mask</b> <b>dest-mac</b> <MACaddr> <b>dest-mac-mask</b> [ <b>vlan</b> <vlanID>  <b>any</b> ] <b>in-port-list</b> <port-list> <b>priority</b> <b>control</b>   <b>high</b>   <b>medium</b>   <b>low</b>  <num> |
| <b>qos set queuing-policy weighted-fair port</b> <port list>  <b>all-ports</b>  |
| <b>qos set weighted-fair control</b> <percentage> <b>high</b> <percentage> <b>medium</b> <percentage> <b>low</b> <percentage> <b>port</b> <port list>  <b>all-ports</b>   |
| <b>qos show ip</b>  |
| <b>qos show ipx</b>   |
| <b>qos show l2 all-destination all-flow ports</b> <port-list> <b>vlan</b> <vlanID> <b>source-mac</b> <MACaddr> <b>dest-mac</b> <MACaddr>  |
| <b>qos show precedence ip</b>   <b>ipx</b>  |
| <b>qos show priority-map</b> <string>   <b>all</b>  |
| <b>qos show wred</b> [ <b>input port</b> <port list>   <b>all-ports</b> ] [ <b>port</b> <port list>   <b>all-ports</b> ]  |
| <b>qos show wfq port</b> <port list>   <b>all-ports</b>   |

# qos apply priority-map

## Purpose

Applies a pre-defined priority map to a port(s).

## Format

**qos apply priority-map** <string> **ports** <port list>

## Mode

Configure.

## Description

The **qos apply priority-map** command allows you apply a previously defined priority map to a port or multiple ports. A priority map associates certain 802.1p tag values inside the frame to a certain internal priority queue. Use the **qos create priority-map** command to first create a priority map.

By default, the X-Pedition router maps the number to the four internal priorities as follows:  
0 or 1 = low; 2 or 3 = medium; 4 or 5 = high; 6 or 7 = control.

## Parameters

|                                 |  |
|---------------------------------|--|
| <b>priority-map</b><br><string> | Specifies the name of the map. Specify a string less than 25 characters. |
| <b>port</b> <port list>         | Specifies the port(s) on which you want to apply the priority map.       |

## Restrictions

None.

## Example

The following command applies the priority map 'map1' to port so.2.1:

```
xp(config)# qos apply priority-map 'map1' port so.2.1
```

# qos create priority-map

## Purpose

Creates a priority map to an 802.1p tag.

## Format

**qos create priority-map** <string> <num> **control** | **low** | **med** | **high**

## Mode

Configure.

## Description

The **qos create priority-map** command lets you map 802.1p tags from a frame to one of the four internal priority queue classes: **control**, **low**, **medium**, and **high**. Internal priority queue classes are used in to prioritize flows during traffic congestion situations. The flows with the higher priority is given precedence over lower priorities. The internal priority class **control** receives the highest precedence, while **low** receives the lowest precedence.

The 802.1p standard provides a way of tagging frames to a certain internal priority. With this command, you can set a particular 802.1p priority tag to map to a specific internal priority queue.

By default, the X-Pedition router maps the number to the four internal priorities as follows: 0 or 1 = low; 2 or 3 = medium; 4 or 5 = high; 6 or 7 = control.

## Parameters

|   |   |
|---|---|
| <b>priority-map</b><br><string>                                 | Specifies the name of the map. Specify a string less than 25 characters in length.  |
| <num>   | Specifies the 802.1p priority tag that you want to map. Specify a number between 0 and 7.                                     |
| <b>queue control</b>   <b>high</b>   <b>medium</b>   <b>low</b> | Specifies the internal priority queue. Specify either the <b>control</b> , <b>high</b> , <b>medium</b> , or <b>low</b> queue. |

## Restrictions

None.

## Example

The following command creates a priority map 'map1' that maps the 802.1p tags 0 and 1 to low, 2 and 3 to medium, 4 and 5 to high, and 6 and 7 to control queue:

```
xp(config)# qos create priority-map 'map1' 0 low 1 low 2 medium 3 medium 4 high 5 high 6 control 7 control
```

# qos precedence ip

## Purpose

Set the precedence of the IP flow fields.

## Format

```
qos precedence ip [sip <num>] [dip <num>] [srcport <num>] [destport <num>]  
[tos <num>] [protocol <num>] [intf <num>]
```

## Mode

Configure.

## Description

The **qos precedence ip** command lets you set the QoS precedence for various flow fields in IP traffic. You can set a precedence from 1 – 7 for the following IP fields:

- IP source address
- IP destination address
- Source TCP or UDP port
- Destination TCP or UDP port
- Type of Service (TOS) for the packet
- Protocol (TCP or UDP)
- Incoming interface

The precedence 1 is the highest priority. IP interfaces or flow fields within IP packets that have a precedence of 1 are given first priority. The default priorities are as follows:

- destination port (1)
- destination address (2)
- source port (3)
- source IP address (4)
- TOS (5)
- interface (6)
- protocol (7).

## Parameters

|                       |   |
|-----------------------|---|
| <b>sip</b> <num>      | Specifies the precedence of the source address field in IP flows. Specify a precedence from 1 – 7.                |
| <b>dip</b> <num>      | Specifies the precedence of the destination address field in IP flows. Specify a precedence from 1 – 7.           |
| <b>srcport</b> <num>  | Specifies the precedence of the source port field in IP flows. Specify a precedence from 1 – 7.                   |
| <b>dstport</b> <num>  | Specifies the precedence of the destination port field in IP flows. Specify a precedence from 1 – 7.              |
| <b>tos</b> <num>      | Specifies the precedence of the TOS field in IP flows. Specify a precedence from 1 – 7.                           |
| <b>protocol</b> <num> | Specifies the precedence of the transport layer protocol name field in IP flows. Specify a precedence from 1 – 7. |
| <b>intf</b> <num>     | Specifies the precedence of the IP interface based on the interface's name. Specify a precedence from 1 – 7.      |

## Restrictions

None.

## Example

To change the precedence for fields within IP flows from the default precedences listed above:

```
xp(config)# qos precedence ip sip 3 dip 1 srcport 2 destport 4 tos 5 protocol 6 intf 7
```

# qos precedence ipx

## Purpose

Set the precedence of the IPX flow fields.

## Format

```
qos precedence ipx [srcnet <num>] [srcnode <num>] [srcport <num>] [dstnet <num>]  
[dstnode <num>] [dstport <num>] [intf <num>]
```

## Mode

Configure.

## Description

The **qos precedence ipx** command lets you set the precedence of the following fields in IPX flows.

- Source network
- Source port
- Source node
- Destination network
- Destination node
- Destination port
- Incoming interface

You can set the precedence of the following fields from 1 – 7. The precedence 1 has the highest priority and 7 has the lowest. The default priorities are as follows:

- destination network (1)
- source network (2)
- destination node (3)
- source node (4)
- destination port (5)
- source port (6)
- interface (7).

## Parameters

|                      |   |
|----------------------|---|
| <b>srcnet</b> <num>  | Specifies the precedence of the source network field in IPX flows. Specify a precedence from 1 – 7.           |
| <b>srcport</b> <num> | Specifies the precedence of the source port field in IPX flows. Specify a precedence from 1 – 7.              |
| <b>srcnode</b> <num> | Specifies the precedence of the source node field in IPX flows. Specify a precedence from 1 – 7.              |
| <b>dstnet</b> <num>  | Specifies the precedence of the destination network field in IPX flows. Specify a precedence from 1 – 7.      |
| <b>dstnode</b> <num> | Specifies the precedence of the destination node field in IPX flows. Specify a precedence from 1 – 7.         |
| <b>dstport</b> <num> | Specifies the precedence of the destination port field in IPX flows. Specify a precedence from 1 – 7.         |
| <b>intf</b> <num>    | Specifies the precedence of the IPX interface based on the interface's name. Specify a precedence from 1 – 7. |

## Restrictions

None.

## Example

To change the precedence for fields within IPX flows from the default precedences listed above:

```
xp(config)# qos precedence ipx srcnet 1 srcnode 2 srcport dstnet 3 srcport 4 dstnode 5 dstport 6 intf 7
```



# **qos priority-map off**

## **Purpose**

Turns off priority mapping on a port(s).

## **Format**

**qos priority-map off**

## **Mode**

Configure.

## **Description**

The **qos priority-map off** command allows you disable any priority maps applied on a port using the **qos apply priority-map** command and reverts back to the default priority mapping.

By default, the X-Pedition router maps the number to the four internal priorities as follows: 0 or 1 = low; 2 or 3 = medium; 4 or 5 = high; 6 or 7 = control.

## **Parameters**

None.

## **Restrictions**

None.

## **Example**

The following command disables all priority mapping:

```
xp(config)# qos priority-map off
```

# qos wred input

## Purpose

Enable WRED on input queues of specific ports.

## Format

```
qos wred input [port <port list>|all-ports] [queue control|high|medium|low]
[exponential-weighting-constant <num>] [min-queue-threshold <num>]
[max-queue-threshold <num>] [mark-prob-denominator <num>]
```

## Mode

Configure.

## Description

The **qos wred input** command lets you set the parameters for Weighted Random Early Detection algorithm and allow you to apply them to input queues of specific ports.

Weighted Random Early Detection alleviates traffic congestion issues by selectively dropping packets before the queue becomes completely flooded. WRED parameters allow you to set conditions and limits for dropping packets in the queue.

## Parameters

|  |   |
|--|---|
| <b>port</b> <port list>  <br><b>all-ports</b>                      | Specifies the port on which the WRED algorithm will be applied. Specify <b>all-ports</b> to apply WRED algorithm to all ports.  |
| <b>queue control</b>   <b>high</b>  <br><b>medium</b>   <b>low</b> | Allows you to specify which queue to apply the WRED algorithm. Specify either the <b>control</b> , <b>high</b> , <b>medium</b> , or <b>low</b> queue.                                 |
| <b>exponential-weighting-constant</b><br><num>                     | Sets the queue weight. Specify a number from 7-10. The default is 8.  |
| <b>min-queue-threshold</b> <num>                                   | Sets the minimum queue length. When the queue length rises above this threshold, packets begin to drop. Specify any number between 5 and 652.   |
| <b>max-queue-threshold</b> <num>                                   | Sets the maximum queue length. When the queue length reaches this threshold, packets are dropped according to the mark probability denominator. Specify any number between 5 and 652. |
| <b>mark-prob-denominator</b> <num>                                 | Specifies the fraction of the packets to be dropped when the queue length reaches the maximum threshold. Specify a number from 10-100. The default is 50.                             |

## Restrictions

WRED should only be applied for TCP/IP traffic.

## Examples

The following command sets WRED on port et.2.1 for the input high queue, sets the queue weight at 8, minimum queue length at 10, maximum queue length at 100, and the fraction of packets dropped to be 50:

```
xp(config)# qos wred input port et.2.1 queue high exponential-weighting-constant 8  
min-queue-threshold 10 max-queue-threshold 100 mark-prob-denominator 50
```

## qos set ip

### Purpose

Set a priority for an IP flow.

### Format

```
qos set ip <name> <priority> [<srcaddr/mask>|any] [<dstaddr/mask>|any] [<srcport>|any]  
[<dstport>|any] [<tos>|any] [<port list>|<interface-list>|any] [<protocol>|any] [<tos-mask>|any]  
[<tos-precedence-rewrite>|any] [<tos-rewrite>|any]
```

### Mode

Configure.

### Description

The **qos set ip** command sets the priority for an IP flow based on the following fields in the flow:

- Flow name
- Source IP address and network mask
- Destination IP address and network mask
- Source port
- Destination port
- TOS
- Layer 4 bridging port list or interface list
- Transport layer protocol (TCP or UDP)

You can set the priority of each field to control, low, medium, or high. The default is low.

## Parameters

|                                       |  |
|---------------------------------------|--|
| <code>&lt;name&gt;</code>             | Specifies the IP flow name.  |
| <code>&lt;priority&gt;</code>         | <p>Specifies the priority you are assigning to the flow parameters you specified from the list above. You can specify one of the following priorities:</p> <p><b>control</b> Assigns control priority to the IP flow parameters you have specified. This is the highest priority.</p> <p><b>high</b> Assigns high priority to the IP flow parameters you have specified.</p> <p><b>medium</b> Assigns medium priority to the IP flow parameters you have specified.</p> <p><b>low</b> Assigns low priority to the IP flow parameters you have specified. This is the default.</p>                          |
| <code>&lt;srcaddr/mask&gt; any</code> | <p>Specifies the source IP address and network mask for which you are assigning a priority. You can specify the mask using the traditional IP address format (“255.255.0.0”) or the CIDR format (“/16”).</p> <p>If you specify <b>any</b> instead of a network mask, the X-Pedition router assumes a wildcard “don’t care” condition. If you do not specify a mask, then the X-Pedition router assumes a mask of 255.255.255.255. You cannot substitute the mask with the <b>any</b> keyword. The keyword <b>any</b> is for the entire <code>&lt;srcaddr/mask&gt;</code> pair.</p>                         |
| <code>&lt;dstaddr/mask&gt; any</code> | <p>Specifies the destination IP address and network mask for which you are assigning a priority. The same requirements and restrictions for <code>&lt;srcaddr/mask&gt;</code> <b>apply to</b> <code>&lt;dstaddr/mask&gt;</code>.</p> <p>If you specify <b>any</b> instead of a network mask, the X-Pedition router assumes a wildcard “don’t care” condition. If you do not specify a mask, then the X-Pedition router assumes a mask of 255.255.255.255. You cannot substitute the mask with the <b>any</b> keyword. The keyword <b>any</b> is for the entire <code>&lt;dstaddr/mask&gt;</code> pair.</p> |
| <code>&lt;srcport&gt; any</code>      | <p>Specifies the source TCP or UDP port for which you are assigning a priority. Specify a port number from 1 – 65535 or <b>any</b> to allow any value. You may also specify a range of port numbers using operator symbols; for example, 10-20 (between 10 and 20 inclusive), &gt;1024 (greater than 1024), &lt;1024 (less than 1024), !=1024 (not equal to 1024).</p>   |
| <code>&lt;dstport&gt; any</code>      | <p>Specifies the destination TCP or UDP port for which you are assigning a priority. Specify a port number from 1 – 65535 or <b>any</b> to allow any value. You may also specify a range of port numbers using operator symbols; for example, 10-20 (between 10 and 20 inclusive), &gt;1024 (greater than 1024), &lt;1024 (less than 1024), !=1024 (not equal to 1024).</p>  |
| <code>&lt;tos&gt; any</code>          | <p>Specifies the TOS for which you are assigning a priority. Specify a number from 0– 255 or <b>any</b> to allow any value.</p>  |

|  |   |
|--|---|
| <port list>  <br><interface-list> <b>any</b> | <p>Specifies one or more Layer 4 bridging ports or one or more IP interface names for which you are assigning priority. If you specify a list, delimit the interface names with commas. Specify <b>any</b> to allow any IP interface name.</p> <p><b>Note:</b> Enterasys recommends that you use alphabetic characters when defining interface names—purely numeric interfaces will be interpreted as IP addresses. The X-Pedition router displays interface names up to 32 characters in length.</p>   |
| <protocol> <b>any</b>                        | <p>Specifies the transport layer protocol for which you are assigning priority. You can specify one of the following values:</p> <p><b>tcp</b> Assigns the priority parameters to the TCP protocol.</p> <p><b>udp</b> Assigns the priority parameters to the UDP protocol.</p> <p><b>any</b> Assigns the priority parameters to both the TCP and UDP protocols.</p>   |
| <tos-mask>                                   | <p>Specifies the mask that is used for the TOS byte. Specify a number from 1-255 or <b>any</b> to specify any TOS value. The default is 30.</p>   |
| <tos-precedence-rewrite>                     | <p>Rewrites the precedence portion of the TOS field with a new value. Specify a number from 0-7 or <b>any</b> to specify any TOS value.</p>   |
| <tos-rewrite>                                | <p>Rewrites the entire TOS field with a new value. Specify a number from 0-31 or <b>any</b> to specify any TOS value.</p> <p><b>Note:</b> If you set <b>any</b> for the TOS precedence rewrite and specify a value for &lt;tos-rewrite&gt;, then the precedence portion of the TOS field remains the same as in the packet, but the rest of the TOS field is rewritten. If you specify values for both &lt;tos-precedence-rewrite&gt; and &lt;tos-rewrite&gt;, then the precedence portion of the TOS field is rewritten to the new &lt;tos-precedence-rewrite&gt; number and the rest of the TOS field is rewritten to the new &lt;tos-rewrite&gt; number.</p> |

## Restrictions

None.

## Example

The following command creates a flow called “flow1”. This flow provides a template for an IP packet with the IP address 1.1.1.1, network mask 255.255.0.0, destination address 2.2.2.2 (and implied destination mask 255.255.255.255). The flow includes source TCP/UDP port 3010, destination port 3000, a TOS of 15, the interfaces mls1 and mls2, and the TCP protocol as transport layer. This very explicit flow has the highest priority—control.

```
xp(config)# qos set ip flow1 control 1.1.1.1/255.255.0.0 2.2.2.2 3010 3000 15 mls1,mls2 tcp
```

# qos set ipx

## Purpose

Set a priority for an IPX flow.

## Format

```
qos set ipx <name> <priority> [<srcnet>|any] [<srcmask>|any] [<srcport>|any] [<dstnet>|any]  
[<dstmask>|any] [<dstport>|any] [<port list>|<interface-list>|any]
```

## Mode

Configure.

## Description

The **qos set ipx** command lets you set the priority for an IPX flow based on the following fields in the flow:

- Flow name
- Source network
- Source network mask
- Source port
- Destination network
- Destination network mask
- Destination port
- Layer 4 bridging port list or interface list

You can set the priority of each field to control, low, medium, or high. The default is low.

## Parameters

---

|        |                              |
|--------|------------------------------|
| <name> | Specifies the IPX flow name. |
|--------|------------------------------|

---

|   |  |
|---|--|
| <priority>                                    | Specifies the priority you are assigning to the flow parameters. You can specify one of the following priorities:  |
| <b>control</b>                                | Assigns control priority to the IPX flow parameters you have specified. This is the highest priority.  |
| <b>high</b>                                   | Assigns high priority to the IPX flow parameters you have specified.   |
| <b>medium</b>                                 | Assigns medium priority to the IPX flow parameters you have specified.   |
| <b>low</b>                                    | Assigns low priority to the IPX flow parameters you have specified. This is the default.   |
| <srcnet>  <b>any</b>                          | Specifies the IPX source network and node address. Specify them in the following format: <netaddr>.<macaddr>; for example:<br>a1b2c3d4.aa:bb:cc:dd:ee:ff.<br><br>If you specify <b>any</b> instead of a .<macaddr>, the X-Pedition router assumes a wildcard value. All MAC addresses are then valid.  |
| <srcmask>  <b>any</b>                         | Specifies the IPX source network mask. Specify the mask in hexadecimal digits. If you do not specify a mask value and instead use the value <b>any</b> , the X-Pedition router internally sets the mask to FFFFFFFF.   |
| <srcport>  <b>any</b>                         | Specifies a port number from 1 – 65535 or <b>any</b> to allow any value. You may also specify a range of port numbers using operator symbols; for example, 10-20 (between 10 and 20 inclusive), >1024 (greater than 1024), <1024 (less than 1024), !=1024 (not equal to 1024).   |
| <dstnet>  <b>any</b>                          | Specifies the IPX destination network and node address. The same requirements and restrictions for <dstaddr> apply to <srcaddr>.   |
| <dstmask>  <b>any</b>                         | Specifies the IPX destination network mask. Specify the mask in hexadecimal digits or <b>any</b> to allow any value.   |
| <dstport>  <b>any</b>                         | Specifies a port number from 1 – 65535 or <b>any</b> to allow any value. You may also specify a range of port numbers using operator symbols; for example, 10-20 (between 10 and 20 inclusive), >1024 (greater than 1024), <1024 (less than 1024), !=1024 (not equal to 1024).   |
| <port list>  <br><interface-list>  <b>any</b> | Specifies one or more Layer 4 bridging ports or one or more IPX interface names for which you are assigning priority. If you specify a list, delimit the interface names with commas. Specify <b>any</b> to allow any IPX interface name.<br><br><b>Note:</b> Enterasys recommends that you use alphabetic characters when defining interface names—purely numeric interfaces will be interpreted as IP addresses. The X-Pedition router displays interface names up to 32 characters in length. |

## Restrictions

None.



## Example

The following command creates an IPX flow called “abc”. This flow gives a high priority to IPX traffic on interface mls1 from network 12345678.00:01:00:00:00:00, mask 0000ff00, port 55 to network 22222222.02:00:00:00:00:00, mask 0000ff00, port 65.

```
xp(config)# qos set ipx abc high 12345678.00:01:00:00:00:00 0000ff00 55 22222222.02:00:00:00:00:00  
0000ff00 65 mls1
```

## qos set l2

### Purpose

Configure priority for a Layer 2 flow.

### Format

**qos set l2 name** <name> **source-mac** <MACaddr> **dest-mac** <MACaddr> [**vlan** <vlanID> **any**]  
**in-port-list** <port-list> **priority control** | **high** | **medium** | **low** | <trunk-priority>

### Mode

Configure.

### Description

The **qos set l2** command lets you set a QoS priority for a Layer 2 flow. You can set a priority for a flow based on the following fields in the flow:

- L2 flow name
- Source MAC address
- Destination MAC address
- VLAN ID
- Incoming port(s)

You can set the priority in one of the following ways:

- The flow is assigned a priority within the X-Pedition router. In this case you specify a priority of control, low, medium, or high. The default is low.
- The flow is assigned a priority within the X-Pedition router, but in addition, if the exit ports are VLAN trunk ports, the flow is assigned an 802.1Q priority. In this case you specify a number from 0 – 7. The X-Pedition router maps the number to the four internal priorities as follows: 0 or 1 = low; 2 or 3 = medium; 4 or 5 = high; 6 or 7 = control.

**Note:** A packet entering a Q-trunk has an 802.1Q header containing a priority field. Typically, users can change the 802.1Q priority using the **qos set l2** commands. However, current hardware restrictions ignore any request to overwrite the packet's priority—the packet simply replicates at the exit port and continues with its original priority.

## Parameters

|   |  |
|---|--|
| <b>name</b> <name>  | Specifies the L2 flow name.  |
| <b>source-mac</b><br><MACaddr>                                      | Specifies the L2 source MAC address. Specify the MAC address in either of the following formats:<br><br>xx:xx:xx:xx:xx:xx<br>xxxxxxxx:xxxxxxxx   |
| <b>dest-mac</b><br><MACaddr>  | Specifies the L2 destination MAC address.  |
| <b>vlan</b> <vlanID>  | Specifies the name of a VLAN.<br><br><b>Note:</b> The X-Pedition router displays VLAN names up to 32 characters in length.   |
| <b>in-port-list</b><br><port-list>                                  | Specifies the X-Pedition ports for which you are setting priority for this flow. The priority applies when the L2 packet enters the X-Pedition router on one of the specified ports. The priority does not apply to exit ports.  |
| <b>priority control <br/>high  medium  low </b><br><trunk-priority> | Specifies the priority you are assigning to the flow parameters you specified from the list above. You can specify one of the following priorities:<br><br><b>control</b> Assigns control priority to the IP flow parameters you have specified. This is the highest priority.<br><br><b>high</b> Assigns high priority to the IP flow parameters you have specified.<br><br><b>medium</b> Assigns medium priority to the IP flow parameters you have specified.<br><br><b>low</b> Assigns low priority to the IP flow parameters you have specified. This is the default.<br><br><trunk-priority> Assigns n 802.1Q VLAN trunk priority when the exit port is a VLAN trunk port. The X-Pedition router maps the number to the four internal priorities as follows: 0 = low; 1, 2, or 3 = medium; 4, 5, or 6 = high; 7 = control. |

## Restrictions

None.

# qos set queuing-policy

## Purpose

Change the queueing policy from strict priority to weighted fair.

## Format

**qos set queuing-policy weighted-fair port** <port list>|**all-ports**

## Mode

Configure.

## Description

The **qos set queuing-policy** command lets you override the default queuing policy (strict priority) in favor of weighted fair queuing on specific ports or on all ports. Only one type of queuing policy can be active at a time.

To set the queuing policy back to strict priority, enter the following command:

```
xp(config)# no qos set queuing-policy weighted-fair port <port list>
```

## Parameters

|   |   |
|---|---|
| <b>weighted-fair</b>                          | Sets the queuing policy to weighted fair.   |
| <b>port</b> <port list>  <br><b>all-ports</b> | Specifies the Ethernet ports or WAN modules and ports on which weighted fair queuing apply. Specify <b>all-ports</b> to apply weighted fair queuing to all ports. |

## Restrictions

None.

# qos set weighted-fair

## Purpose

Set percentages for weighted-fair queuing.

## Format

**qos set weighted-fair control** <percentage> **high** <percentage> **medium** <percentage>  
**low** <percentage> **port** <port list>|**all-ports**

## Mode

Configure.

## Description

The **qos set weighted-fair** command lets you set the percentage of X-Pedition bandwidth allocated to the control, high, medium, and low priorities. The percentages apply to specific ports or to all ports. Make sure the total percentages for all four priorities equals 100.

## Parameters

|  |   |
|--|---|
| <b>control</b> <percentage>                | Specifies the percentage of X-Pedition bandwidth allocated to the control priority. Specify a number from 1 – 100. The default is 25.                         |
| <b>high</b> <percentage>                   | Specifies the percentage of X-Pedition bandwidth allocated to the high priority. Specify a number from 1 – 100. The default is 25.                            |
| <b>medium</b> <percentage>                 | Specifies the percentage of X-Pedition bandwidth allocated to the medium priority. Specify a number from 1 – 100. The default is 25.                          |
| <b>low</b> <percentage>                    | Specifies the percentage of X-Pedition bandwidth allocated to the low priority. Specify a number from 1 – 100. The default is 25.                             |
| <b>port</b> <port list>   <b>all-ports</b> | Specifies the Ethernet ports or WAN modules and ports on which the defined percentages apply. Specify <b>all-ports</b> to apply the percentages to all ports. |

## Restrictions

The total percentages for all four QoS levels must equal 100%.

## **qos show ip**

### **Purpose**

Show QoS information for IP flows.

### **Format**

**qos show ip**

### **Mode**

Enable.

### **Description**

The **qos show ip** command lets you display QoS information for IP flows.

### **Parameters**

None.

### **Restrictions**

None.

# **qos show ipx**

## **Purpose**

Show QoS information for IPX flows.

## **Format**

**qos show ipx**

## **Mode**

Enable.

## **Description**

The **qos show ipx** command lets you display QoS information for IPX flows.

## **Parameters**

None.

## **Restrictions**

None.

# qos show l2

## Purpose

Show QoS information for L2 flows.

## Format

**qos show l2 all-destination all-flow ports** <port-list> **vlan** <vlanID> **source-mac** <MACaddr>  
**dest-mac** <MACaddr>

## Mode

Enable.

## Description

The **qos show l2** command displays QoS information for L2 flows. You can filter the display according to the following:

- Destinations
- Flows
- Ports
- VLANs
- Source MAC addresses
- Destination MAC addresses
- Priority

## Parameters

|                                |   |
|--------------------------------|---|
| <b>all-destination</b>         | Filters the display to show all the L2 destination priorities.                              |
| <b>all-flow</b>                | Filters the display to show all the L2 flow priorities.                                     |
| <b>ports</b> <port-list>       | Filters the display to show L2 priority information for specific ports.                     |
| <b>vlan</b> <vlanID>           | Filters the display to show L2 priority information for specific VLANs.                     |
| <b>source-mac</b><br><MACaddr> | Filters the display to show L2 priority information for specific source MAC addresses.      |
| <b>dest-mac</b><br><MACaddr>   | Filters the display to show L2 priority information for specific destination MAC addresses. |



## **Restrictions**

None.

## qos show precedence

### Purpose

Shows IP or IPX precedence values.

### Format

**qos show precedence ip | ipx**

### Mode

Enable.

### Description

The **qos show precedence** command lets you display the precedence values for all fields in a flow.

IP flows consist of the following fields: destination port, destination address, source port, source IP address, TOS, interface, protocol.

IPX flows consist of the following fields: destination network, source network, destination node, source node, destination port, source port, interface.

### Parameters

|            |   |
|------------|---|
| <b>ip</b>  | Displays the precedence values for IP flows.  |
| <b>ipx</b> | Displays the precedence values for IPX flows. |

### Restrictions

None.

# qos show priority-map

## Purpose

Shows the priority mapping and the ports that it is applied.

## Format

**qos show priority-map** *<string>* | **all**

## Mode

Enable.

## Description

The **qos show priority-map** command lets you display the priority mapping that is configured on a port. The command shows how each 802.1p tag values are mapped to a specific internal priority queue.

## Parameters

|                       |   |
|-----------------------|---|
| <i>&lt;string&gt;</i> | Specifies the name of the priority map. |
| <b>all</b>            | Displays all priority maps.             |

## Restrictions

None.

# qos show wred

## Purpose

Shows WRED parameters for each port.

## Format

**qos show wred** [**input port** <port list> | **all-ports**] [**port** <port list> | **all-ports**]

## Mode

Enable.

## Description

The **qos show wred** command lets you display WRED information for a certain port or all ports. You can display WRED parameter information according to the following:

- Input ports
- All Ports

## Parameters

|  |   |
|--|---|
| <b>input port</b> <port list>   <b>all-ports</b> | Displays input port WRED parameters. Specify <b>all-ports</b> to display parameters for all ports.    |
| <b>port</b> <port list>   <b>all-ports</b>       | Displays WRED parameters for each port. Specify <b>all-ports</b> to display parameters for all ports. |

## Restrictions

None.

# qos show wfq

## Purpose

Shows bandwidth allocated for each port.

## Format

**qos show wfq** [**port** <port list> | **all-ports**] [**input** <slot num> | **all-modules**]

## Mode

Enable.

## Description

The **qos show wfq** command lets you display the bandwidth for each port allocated with weighted-fair queuing.

## Parameters

|   |   |
|---|---|
| <b>port</b> <port list>  <br><b>all-ports</b>   | Displays bandwidth allocated for each port. Specify a list of ethernet or wan ports. Specify <b>all-ports</b> to display bandwidth for all ports. |
| <b>input</b> <slot num>  <br><b>all-modules</b> | Displays bandwidth allocated for each slot. Specify a list of occupied slots. Specify <b>all-modules</b> to display bandwidth for all modules.    |

## Restrictions

None.



# Chapter 56

## radius Commands

The **radius** commands let you secure access to the X-Pedition router using the Remote Authentication Dial-In User Service (RADIUS) protocol. When users log in to the router or try to access Enable mode, they are prompted for a password. If RADIUS authentication is enabled on the router, it will contact a RADIUS server to verify the user. If the user is verified, he or she is granted access to the router at the authorized mode (Login, Enable, or Configure).

### Command Summary

[Table 48](#) lists the **radius** commands. The sections following the table describe the command syntax.

**Table 48. radius Commands**

|   |
|---|
| <b>radius accounting command level</b> <level>  |
| <b>radius accounting shell</b> start  stop  all   |
| <b>radius accounting snmp</b> active  startup   |
| <b>radius accounting system</b> fatal  error  warning  info   |
| <b>radius authentication</b> login  enable  |
| <b>radius enable</b>  |
| <b>radius set server</b> <IPaddr> [acct-port <number>] [auth-port <number>]<br>[timeout <number>] [retries <number>] [deadtime <number>] [key <string>]<br>[source <IFname_IPaddr>] |
| <b>radius set</b> [timeout <number>] [retries <number>] [deadtime <number>] [key <string>]<br>[source <IFname_IPaddr>] last-resort password  succeed  deny                          |
| <b>radius show</b> stats all  |

# radius accounting command level

## Purpose

Causes the specified types of commands to be logged to the RADIUS server.

## Format

**radius accounting command level** *<level>*

## Mode

Configure.

## Description

The **radius accounting command level** command allows you specify the types of commands that are logged to the RADIUS server. The user ID and timestamp are also logged.

## Parameters

|                      |   |
|----------------------|---|
| <i>&lt;level&gt;</i> | Specifies the type(s) of commands that are logged to the RADIUS server.<br>Enter one of the following values: |
| 5                    | Log Configure commands.   |
| 10                   | Log all Configure and Enable commands.  |
| 15                   | Log all Configure, Enable, and User commands.   |

## Restrictions

None.

## Example

To cause Configure, Enable, and User mode commands to be logged on the RADIUS server:

```
xp(config)# radius accounting command level 15
```



# radius accounting shell

## Purpose

Causes an entry to be logged on the RADIUS server when a shell is stopped or started on the X-Pedition router.

## Format

**radius accounting shell start|stop|all**

## Mode

Configure.

## Description

The **radius accounting shell** command allows you to track shell usage on the X-Pedition router. It causes an entry to be logged on the RADIUS server when a shell is started or stopped. You can specify that an entry be logged when a shell is started, when a shell is stopped, or when a shell is either started or stopped.

## Parameters

|              |   |
|--------------|---|
| <b>start</b> | Logs an entry when a shell is started.                  |
| <b>stop</b>  | Logs an entry when a shell is stopped                   |
| <b>all</b>   | Logs an entry when a shell is either started or stopped |

## Restrictions

None.

## Example

To cause an entry to be logged on the RADIUS server when a shell is either started or stopped on the X-Pedition router:

```
radius accounting shell all
```

# radius accounting snmp

## Purpose

Logs to the RADIUS server any changes made to the startup or active configuration via SNMP.

## Format

**radius accounting snmp active|startup**

## Mode

Configure.

## Description

The **radius accounting snmp** command allows you to track changes made to the active or startup configuration through SNMP. It causes an entry to be logged on the RADIUS server whenever a change is made to the ACL configuration. You can specify that an entry be logged to the active or startup configuration.

## Parameters

|                |   |
|----------------|---|
| <b>active</b>  | Logs an entry when a change is made to the active configuration.  |
| <b>startup</b> | Logs an entry when a change is made to the startup configuration. |

## Restrictions

None.

## Example

To cause an entry to be logged on the RADIUS server whenever an ACL configuration change is made via SNMP to the active configuration:

```
xp(config)# radius accounting snmp active
```

# radius accounting system

## Purpose

Specifies the type(s) of messages to be logged on the RADIUS server.

## Format

**radius accounting system fatal|error|warning|info**

## Mode

Configure.

## Description

The **radius accounting system** command allows you to specify the types of messages that are logged on the RADIUS server.

## Parameters

|                |  |
|----------------|--|
| <b>fatal</b>   | Logs only fatal messages.                                  |
| <b>error</b>   | Logs fatal messages and error messages.                    |
| <b>warning</b> | Logs fatal messages, error messages, and warning messages. |
| <b>info</b>    | Logs all messages, including informational messages.       |

## Restrictions

None.

## Example

To log only fatal and error messages on the RADIUS server:

```
xp(config)# radius accounting system error
```

# radius authentication

## Purpose

Causes RADIUS authentication to be performed at either the X-Pedition login prompt or when the user tries to access Enable mode.

## Format

**radius authentication login|enable**

## Mode

Configure.

## Description

The **radius authentication** command allows you to specify when RADIUS authentication is performed: either when a user logs in to the X-Pedition router, or tries to access Enable mode.

## Parameters

|               |  |
|---------------|--|
| <b>login</b>  | Authenticates users at the X-Pedition login prompt.      |
| <b>enable</b> | Authenticates users when they try to access Enable mode. |

## Restrictions

None.

## Example

To perform RADIUS authentication at the X-Pedition login prompt:

```
radius authentication login
```

# radius enable

## Purpose

Enables RADIUS authentication on the X-Pedition router. RADIUS authentication is disabled by default on the X-Pedition router.

## Format

**radius enable**

## Mode

Configure.

## Description

The **radius enable** command causes RADIUS authentication to be activated on the X-Pedition router. You set RADIUS-related parameters with the **radius set**, **radius accounting shell**, and **radius authentication** commands, then use the **radius enable** command to activate RADIUS authentication.

## Parameters

None.

## Restrictions

None.

## Example

The following commands set RADIUS-related parameters on the X-Pedition router. The commands are then activated with the **radius enable** command:

```
radius set server 207.135.89.15
radius set timeout 30
radius authentication login
radius accounting shell all
radius enable
```

# radius set

## Purpose

Sets parameters for authenticating the X-Pedition router through a RADIUS server.

## Format

**radius set** [**timeout** <number>] [**retries** <number>] [**deadtime** <number>] [**key** <string>]  
[**source** <IFname\_IPaddr>] **last-resort password** |**succeed** |**deny**

## Mode

Configure.

## Description

The **radius set** command allows you to set default RADIUS-related parameters on the X-Pedition router, how long to wait for the RADIUS server to authenticate the user, an encryption key, and what to do if the RADIUS server does not reply by a given time.

## Parameters

|                                  |  |
|----------------------------------|--|
| <b>timeout</b> <number>          | Is the maximum time (in seconds) to wait for a RADIUS server to reply. The default is 3 seconds.   |
| <b>retries</b> <number>          | The number of times (1-10) to try contacting this RADIUS server.   |
| <b>deadtime</b> <number>         | The length of time for transaction requests to skip over a RADIUS server—up to a maximum of 1440 minutes (24 hours). This command causes the X-Pedition router to mark as “dead” any RADIUS server that fails to respond to authentication requests, thus avoiding the wait for the request to timeout before trying the next configured server. Additional requests for a RADIUS server marked as “dead” will skip the server for the duration of minutes specified (unless all servers are marked “dead”). |
| <b>key</b> <string>              | Is an encryption key to be shared with the RADIUS server.  |
| <b>source</b><br><IFname_IPaddr> | Sets the source interface name or IP address for RADIUS messages.<br><br><b>Note:</b> Enterasys recommends that you use alphabetic characters when defining interface names—purely numeric interfaces will be interpreted as IP addresses. The X-Pedition router will display interface names up to 32 characters in length.   |

---

|                    |   |
|--------------------|---|
| <b>last-resort</b> | Is the action to take if a RADIUS server does not reply within the time specified by the <b>timeout</b> parameter. If this parameter is <i>not</i> specified, user authentication will always fail if the RADIUS server does not reply within the specified timeout period.<br><br>Specify one of the following keywords: |
| <b>password</b>    | The user is prompted for the password set with <b>system set password</b> command. This keyword is <i>recommended</i> for optimal security, however, note that you must set a password with the <b>system set password</b> command.   |
| <b>succeed</b>     | Access to the X-Pedition router is granted.   |
| <b>deny</b>        | Unable to connect to RADIUS server, access to the X-Pedition router is denied.  |

---

## Restrictions

None.

## Example

The following commands specify that hosts 137.72.5.9 and 137.72.5.41 are RADIUS servers, and the X-Pedition router should wait no more than 30 seconds for a response from one of these servers. If a response from a RADIUS server doesn't arrive in 30 seconds, the user is prompted for the password that was set with the X-Pedition **system set password** command.

```
radius set server 137.72.5.9
radius set server 137.72.5.41
radius set timeout 30
radius set last-resort password
```

# radius set server

## Purpose

Sets parameters for authenticating the X-Pedition router through a specific RADIUS server.

## Format

**radius set server** <IPaddr> [**acct-port** <number>] [**auth-port** <number>] [**timeout** <number>] [**retries** <number>] [**deadtime** <number>] [**key** <string>] [**source** <IFname\_IPaddr>]

## Mode

Configure.

## Description

The **radius set server** command allows you to set RADIUS-related parameters on the X-Pedition router, including the IP address of a specific RADIUS server, how long to wait for the RADIUS server to authenticate the user, an encryption key, and what to do if the RADIUS server does not reply by a given time.

## Parameters

|                           |  |
|---------------------------|--|
| <b>server</b> <IPaddr>    | Is the IP address of a specific RADIUS server. You can enter up to five RADIUS servers. Enter one server per <b>radius set server</b> command.   |
| <b>acct-port</b> <number> | Enter the accounting port number. The default <b>Acct-port</b> number is 1813.   |
| <b>auth-port</b> <number> | Enter the authentication port number. The default <b>Auth-port</b> number is 1812.   |
| <b>timeout</b> <number>   | Is the maximum time (in seconds) to wait for a RADIUS server to reply. The default is 3 seconds.   |
| <b>retries</b> <number>   | The number of times (1-10) to try contacting this RADIUS server.   |
| <b>deadtime</b> <number>  | The length of time for transaction requests to skip over a RADIUS server—up to a maximum of 1440 minutes (24 hours). This command causes the X-Pedition router to mark as “dead” any RADIUS server that fails to respond to authentication requests, thus avoiding the wait for the request to timeout before trying the next configured server. Additional requests for a RADIUS server marked as “dead” will skip the server for the duration of minutes specified (unless all servers are marked “dead”). |
| <b>key</b> <string>       | Is an encryption key to be shared with the RADIUS server.  |



|                                  |  |
|----------------------------------|--|
| <b>source</b><br><Ifname_IPaddr> | Sets the source interface name or IP address for RADIUS messages.<br><br><b>Note:</b> Enterasys recommends that you use alphabetic characters when defining interface names—purely numeric interfaces will be interpreted as IP addresses. The X-Pedition router will display interface names up to 32 characters in length. |
|----------------------------------|--|

## Restrictions

None.

## Example

The following commands specify that hosts 137.72.5.9 and 137.72.5.41 are RADIUS servers, and the X-Pedition router should wait no more than 30 seconds for a response from one of these servers. If a response from a RADIUS server doesn't arrive in 30 seconds, the user is prompted for the password that was set with the X-Pedition **system set password** command.

```
radius set server 137.72.5.9
radius set server 137.72.5.41
radius set timeout 30
radius set last-resort password
```

# radius show

## Purpose

Displays information about RADIUS configuration on the X-Pedition router.

## Format

**radius show stats|all**

## Mode

Enable.

## Description

The **radius show** command displays statistics and configuration parameters related to RADIUS configuration on the X-Pedition router. The statistics displayed include:

|          |   |
|----------|---|
| accepts  | Number of times each server responded and validated the user successfully.  |
| rejects  | Number of times each server responded and denied the user access, either because the user wasn't known, or the wrong password was supplied. |
| timeouts | Number of times each server did not respond.  |

## Parameters

|              |   |
|--------------|---|
| <b>stats</b> | Displays the accepts, rejects, and timeouts for each RADIUS server.   |
| <b>all</b>   | Displays the configuration parameters set with the <b>radius set</b> command, in addition to the accepts, rejects, and timeouts for each RADIUS server. |

## Restrictions

None.

## Example

To display configuration parameters and RADIUS server statistics:

```
radius show all
RADIUS status:                ACTIVE
RADIUS last resort:           Succeed when server fails
Command Level Logging:        15 - Log Configure, Enable and User Commands
Default RADIUS timeout (seconds): 3
Default RADIUS retries:        3
Default RADIUS deadtime (minutes): 0
Default RADIUS key:            net
Default RADIUS source IP address: Let system decide

RADIUS servers listed in order of priority:

Server:                        10.136.16.102
Port:                          49
Timeout (seconds):              <Default>
Retries:                        <Default>
Deadtime (minutes):             3
Key:                            net
Source IP:                      <Default>
Server is dead. Will be made tested again in 2 minutes

Server:                        10.136.15.100
Port:                          49
Timeout (seconds):              <Default>
Retries:                        <Default>
Deadtime (minutes):             <Default>
Key:                            <Default>
Source IP:                      <Default>

Server:                        10.136.15.101
Port:                          49
Timeout (seconds):              <Default>
Retries:                        <Default>
Deadtime (minutes):             <Default>
Key:                            net
Source IP:                      <Default>

RADIUS server host statistics:

Host      Accepts  Rejects  Timeouts
10.136.16.102  0      0      3
10.136.15.100  1      0      0    * Sever being used
10.136.15.101  0      0      0
```



# Chapter 57

## rarpd Commands

The **rarpd** commands let you configure and display information about Reverse Address Resolution Protocol (RARP) on the X-Pedition router.

### Command Summary

[Table 49](#) lists the **rarpd** commands. The sections following the table describe the command syntax.

**Table 49. rarpd Commands**

|  |
|--|
| <b>rarpd add hardware-address</b> <mac-address> <b>ip-address</b> <IPaddr> |
| <b>rarpd set interface</b> <name>  <b>all server-ip</b> <IPaddr>           |
| <b>rarpd show interface</b>  mappings                                      |

# rarpd add

## Purpose

Maps a MAC address to an IP address.

## Format

**rarp add hardware-address** <mac-address> **ip-address** <IPaddr>

## Mode

Configure.

## Description

The **rarpd add** command allows you to map a MAC address to an IP address for use with RARP. When a host makes a RARP request on the X-Pedition router, and its MAC address has been mapped to an IP address with the **rarp add** command, the RARP server on the X-Pedition router responds with the IP address that corresponds to the host's MAC address.

## Parameters

|  |   |
|--|---|
| <b>hardware-address</b><br><mac-address> | Is a MAC address in the form <i>xx:xx:xx:xx:xx:xx</i> or <i>xxxxxx:xxxxxx</i> . |
| <b>ip-address</b><br><IPaddr>            | Is the IP address to be mapped to the MAC address.                              |

## Restrictions

None.

## Example

To map MAC address 00:C0:4F:65:18:E0 to IP address 10.10.10.10:

```
xp(config)# rarpd add hardware-address 00:C0:4F:65:18:E0 ip-address 10.10.10.10
```

# rarpd set interface

## Purpose

Specifies the interface(s) to which the X-Pedition router's RARP server responds.

## Format

**rarpd set interface** <name>|**all server-ip** <IPaddr>

## Mode

Configure.

## Description

The **rarpd set interface** command allows you to specify which interfaces the X-Pedition router's RARP server responds to when sent RARP requests. You can specify individual interfaces or all interfaces.

## Parameters

|                  |   |
|------------------|---|
| <name>           | Is the name of an interface.<br><br><b>Note:</b> Enterasys recommends that you use alphabetic characters when defining interface names—purely numeric interfaces will be interpreted as IP addresses. The X-Pedition router will display interface names up to 32 characters in length. |
| <b>all</b>       | Causes the RARP server to respond to RARP requests from all interfaces.   |
| <b>server-ip</b> | The server IP address to use in replies.  |

## Restrictions

None.

## Example

To cause the X-Pedition router's RARP server to respond to RARP requests from interface int1:

```
xp(config)# rarpd set interface int1
```

# rarpd show

## Purpose

Displays information about the X-Pedition router's RARP configuration.

## Format

**rarpd show interface|mappings**

## Mode

Enable.

## Description

The **rarpd show** command displays information about the configuration of the X-Pedition router's RARP server. You can list the MAC-to-IP address mappings or the interfaces to which the X-Pedition router responds to RARP requests.

## Parameters

|                  |   |
|------------------|---|
| <b>interface</b> | Lists the interfaces to which the X-Pedition router responds to RARP requests.                  |
| <b>mappings</b>  | Displays the list of MAC-to-IP address mappings that was set with the <b>rarp add command</b> . |

## Restrictions

None.

## Example

To display the RARP server's list of MAC-to-IP address mappings:

```
xp# rarpd show mappings
```



# Chapter 58

## rate-limit Command

The **rate-limit** commands allow you to define rate limits and apply them to IP interfaces or ports. There are several types of rate limiting supported:

- Per-flow rate limiting—limits individual flows to a specified rate.
- Flow-aggregate rate limiting—software-based rate limiting that limits an aggregation of flows (i.e., all flows that match an ACL) to a specific rate.
- VLAN rate limiting—rate limiting for traffic that enters or leaves a particular VLAN.
- Aggregate rate limiting—rate limiting for an aggregation of flows enabled on a per-line card basis.

**Note:** Since aggregate rate limiting is performed completely in hardware and must be enabled on a per-line card basis—if you enable aggregate rate limiting on a line card, you cannot use per-flow or flow-aggregate rate limiting with that card. Aggregate and flow-aggregate rate limiting are not supported on 802.1q trunk ports.

- Port-level rate limiting—rate limiting for individual ports.

**Note:** For a complete list of hardware and the features they support, consult the Release Notes on the Enterasys Networks web site: **[www.enterasys.com](http://www.enterasys.com)**

## Command Summary

[Table 50](#) lists the **rate-limit** commands. The sections following the table describe the command syntax.

**Table 50. rate-limit Commands**

|  |
|--|
| <b>rate-limit</b> <name> <b>aggregate acl</b> <acl list> <b>rate</b> <num> [ <b>drop-packets</b>   <b>no-action</b>   <b>lower-priority</b>   <b>lower-priority-except-control</b>   <b>tos-precedence-rewrite</b> <num>  <b>tos-precedence-rewrite-lower-priority</b> <num>] [ <b>allocate-resources-during-apply</b>   <b>allocate-resources-during-traffic</b> ]  [ <b>burst-compensating</b> ] |
| <b>rate-limit</b> <name> <b>apply interface</b> <interface>  <b>all</b>  |
| <b>rate-limit</b> <name> <b>flow-aggregate acl</b> <acl list> <b>rate</b> <rate> <b>exceed-action</b> <action> [ <b>sequence</b> <number>]  [ <b>burst-compensating</b> ] <b>min-bandwidth</b> <min-bw>  <b>distribute-among</b> <number-of-flows>]  |
| <b>rate-limit</b> <name> <b>input acl</b> <acl list> <b>rate</b> <number> <b>exceed-action</b> <b>drop-packets</b>   <b>set-priority-low</b>   <b>set-priority-medium</b>   <b>set-priority-high</b> [ <b>sequence</b> <number>]  [ <b>burst-compensating</b> ]  |
| <b>rate-limit</b> <name> <b>port-level input port</b> <port list> <b>rate</b> <num> [ <b>drop-packets</b>   <b>no-action</b>   <b>lower-priority</b>   <b>lower-priority-except-control</b>   <b>tos-precedence-rewrite</b> <num>  <b>tos-precedence-rewrite-lower-priority</b> <num>] [ <b>burst-compensating</b> ]   |
| <b>rate-limit</b> <name> <b>port-level slot</b> <num> <b>ignore-control-priority</b>   |
| <b>rate-limit</b> <name> <b>port-level output port</b> <port list> <b>rate</b> <num> <b>drop-packets</b>   |
| <b>rate-limit show</b> [ <b>all</b> ]  [ <b>policy-type</b> <b>flow-policies</b>   <b>flow-aggregate-policies</b>   <b>aggregate-policies</b>   <b>portlevel-policies</b>   <b>all</b> ]  [ <b>policy-name</b> <name>]  [ <b>interface</b> <interface>]  [ <b>port-level port</b> <port list>   <b>all-port</b> ]  [ <b>port-level policy-name</b> <name>]  [ <b>rate-limiting-mode</b> ]          |
| <b>rate-limit</b> <name> <b>vlan</b> <name> <b>port</b> <port list>   <b>all-ports</b> <b>destport</b> <port list>   <b>all-ports</b> <b>rate</b> <num> <b>exceed-action</b> <b>drop-packets</b>   <b>set-priority-low</b>   <b>set-priority-medium</b>   <b>set-priority-high</b> [ <b>burst-compensating</b> ] [ <b>aggregate</b> ]  |

# rate-limit aggregate acl

## Purpose

Defines an aggregate rate-limiting policy.

## Format

```
rate-limit <name> aggregate acl <acl list> rate <num> [drop-packets| no-action|
lower-priority| lower-priority-except-control| tos-precedence-rewrite <num>|
tos-precedence-rewrite-lower-priority <num>] [allocate-resources-during-apply|
allocate-resources-during-traffic] [burst-compensating <num>]
```

## Mode

Configure.

## Description

The **rate-limit aggregate acl** command allows you to specify the rate limiting policy for an aggregation of flows. An aggregation of flows is all the flows with the same ACLs. The rate limiting policy affects the whole aggregation and not an individual flow. Example of this type of policy is rate limiting traffic from one subnet to another. The line card to which you apply this command must be in Aggregate rate limiting mode. See [system enable aggregate-rate-limiting on page 1341](#).

## Parameters

|  |  |
|--|--|
| <b>&lt;name&gt;</b>                            | The name of the rate limit.  |
| <b>acl &lt;acl list&gt; <br/>all-ports</b>     | Specifies the ACL which will identify the flows to aggregate and rate limit. The keyword <b>all</b> specifies all ACLs.  |
| <b>rate &lt;num&gt;</b>                        | Specifies the rate limit, in bps, for the flow. This value can be between 1000 and 1000000000.   |
| <b>drop-packets</b>                            | Specifies that if the rate-limit is exceeded, then packets will be dropped.  |
| <b>no-action</b>                               | Specifies that if the rate-limit is exceeded, then no action will be taken.  |
| <b>lower-priority</b>                          | Specifies that if the rate-limit is exceeded, the packets priority is lowered.   |
| <b>lower-priority-<br/>except-control</b>      | Specifies that if the rate-limit is exceeded, then the packets priority is lowered, except control packets.  |
| <b>tos-precedence-<br/>rewrite &lt;num&gt;</b> | Specifies that if the rate-limit is exceeded, then the tos precedence in the IP packet header will be rewritten to a specified value. This value can be between 0 and 7. |

|  |   |
|--|---|
| <b>tos-precedence-rewrite-lower-priority</b> <num> | Specifies that if the rate-limit is exceeded, then the tos precedence in the IP packet header will be rewritten to a specified value and the packet priority will be lowered. This value can be between 0 and 7.  |
| <b>allocate-resources during-apply</b>             | Allocates resources to the policy when its applied to an interface.   |
| <b>allocate-resources during-traffic</b>           | Allocates resources to the policy when actual traffic flow is present.  |
| <b>burst-compensating</b> <num>                    | <p>When you choose the burst-compensating option, the X-Pedition router invokes a different algorithm for calculating the rate limit values used by the hardware. This algorithm is better at compensating for <i>burst capacity</i>—the ability to maintain an average close to the specified rate—even with large bursts of traffic. The burst-compensating option is available on all rate-limiting policies except port-level output and requires that you enter a burst-compensator value of 1-100 to represent how much burst capacity (in Mbps) to build into the rate limit. For example, setting a low burst-compensator value on a rate limit policy to restrict the flow of an FTP server and client that are capable of very high transfer rates will choke off the flow and produce realized rates that are smaller than the specified rate limit. Conversely, setting a higher burst-compensator value than the flow’s unrestricted capabilities will result in realized rates that are higher than the specified rate limit.</p> <p><b>Note:</b> Due to hardware constraints, the realized rates for rate limits set above 20 Mbps will become increasingly less consistent and accurate.</p> <p>The router uses a <i>credit bucket</i> bandwidth policing scheme to perform rate limiting. This policy creates a <i>credit bucket</i> and <i>time slice</i> in the Input Packet Processor hardware and, for a given rate limit, calculates a credit bucket size to represent the amount of traffic that can pass through the processor within a specific time period (i.e., the time slice value). When you specify the burst-compensating option, the credit bucket and time slice values are calculated to take into account traffic spikes or <i>bursts</i> and to achieve an average rate that is as close as possible to the specified rate. When the bucket is <i>filled</i> within the specified time slice, the router drops packets or changes the priority of the packets, depending on the exceed-action specified. Because the burst compensating option allows you to create larger credit buckets and smaller time slices, you can prevent constricting the flow of rate-limited, bursty traffic.</p> <p><b>Note:</b> If you do not specify this option, rate-limiting will provide accurate results (to within 10-15%) for “smooth” traffic only (e.g., traffic created by a traffic generator). For example, if you use a small credit bucket and a large time slice, a burst of traffic can fill the bucket and cause the X-Pedition router to drop traffic (until the time slice expires and refreshes the credit bucket). This can choke off the traffic rate. For bursty traffic such as TCP and most traffic running on a live network, use the burst-compensating option.</p> |

## Restrictions

Aggregate and flow-aggregate rate limiting are not supported on 802.1q trunk ports.

## Example

To define an aggregate rate limiting policy based on the ACL 'engacl':

```
xp(config)# rate-limit eng aggregate acl engacl rate 10000000 drop-packets allocate-resources  
during-apply
```

# rate-limit apply

## Purpose

Applies a rate limiting policy to an interface.

## Format

**rate-limit** <name> **apply interface** <interface>| **all**

## Mode

Configure.

## Description

The **rate-limit apply** command allows you to apply a previously-defined rate limiting policy to an interface.

## Parameters

|   |  |
|---|--|
| <name>                                      | The name of the rate limiting policy.  |
| <b>interface</b><br><interface>  <b>all</b> | The name of the IP interface. The keyword <b>all</b> applies the policy to all IP interfaces.<br><br><b>Note:</b> Enterasys recommends that you use alphabetic characters when defining interface names—purely numeric interfaces will be interpreted as IP addresses. The X-Pedition router will display interface names up to 32 characters in length. |

## Restrictions

Port-level and VLAN policies do not use this command in conjunction with their policy commands.

## Example

To apply the rate limiting policy 'engacl' to the interface 'ip16':

```
xp(config)# rate-limit engacl apply interface ip16
```

# rate-limit flow-aggregate

## Purpose

Used to specify a profile for software-based aggregate rate limiting.

**Note:** You cannot use Flow-Aggregate Rate Limiting on line cards that support Aggregate Rate Limiting. Flow-Aggregate Rate Limiting allows you to rate limit the aggregation of flows where the hardware does not support aggregate rate limiting.

## Format

**rate-limit** <name> **flow-aggregate acl** <acl list> **rate** <rate> **exceed-action** <action> [sequence <number>] | [burst-compensating] | min-bandwidth <min-bw> | distribute-among <number-of-flows>]

## Mode

Configure.

## Description

The **rate-limit flow-aggregate** command is used to specify a profile for software-based aggregate rate limiting. Use the rate-limit apply command to apply the profile to an IP interface. The line card to which you apply this command must be in Per-flow rate limiting mode. See [system enable aggregate-rate-limiting on page 1341](#).

## Parameters

|                               |   |  |
|-------------------------------|---|--|
| <b>rate-limit</b> <name>      | The name of the rate limiting policy. The maximum length for this name is 30 bytes.   |  |
| <b>acl</b> <acl list>         | The ACL(s) that define a rate limiting policy. The <b>rate-limit flow-aggregate</b> command disregards the permit/deny keywords in the ACL rule definition. However, it does look at all parameters in the ACL rule.  |  |
| <b>rate</b> <rate>            | Rate limit, in bps, for the aggregation of flows. The range for <rate> is 3000 to 1000000000.   |  |
| <b>exceed-action</b> <action> | The action taken if the rate limit is exceeded.<br>drop-packets                      Drop the packets.<br>set-priority-low                      Set packet priority to low.<br>set-priority-medium                      Set packet priority to medium.<br>set-priority-high                      Set packet priority to high. |  |
| <b>sequence</b> <number>      | Sequence number for this policy. The range for <number> is 1 to 65535.  |  |

---

**burst-compensating** When you choose the burst-compensating option, the X-Pedition router invokes a different algorithm for calculating the rate limit values used by the hardware. This algorithm is better at compensating for *burst capacity*—the ability to maintain an average close to the specified rate—even with large bursts of traffic. The burst-compensating option is available on all rate-limiting policies except port-level output and requires that you enter a burst-compensator value of 1-100 to represent how much burst capacity (in Mbps) to build into the rate limit. For example, setting a low burst-compensator value on a rate limit policy to restrict the flow of an FTP server and client that are capable of very high transfer rates will choke off the flow and produce realized rates that are smaller than the specified rate limit. Conversely, setting a higher burst-compensator value than the flow’s unrestricted capabilities will result in realized rates that are higher than the specified rate limit.

<num>

**Note:** Due to hardware constraints, the realized rates for rate limits set above 20 Mbps will become increasingly less consistent and accurate.

The router uses a *credit bucket* bandwidth policing scheme to perform rate limiting. This policy creates a *credit bucket* and *time slice* in the Input Packet Processor hardware and, for a given rate limit, calculates a credit bucket size to represent the amount of traffic that can pass through the processor within a specific time period (i.e., the time slice value). When you specify the burst-compensating option, the credit bucket and time slice values are calculated to take into account traffic spikes or *bursts* and to achieve an average rate that is as close as possible to the specified rate. When the bucket is *filled* within the specified time slice, the router drops packets or changes the priority of the packets, depending on the exceed-action specified. Because the burst compensating option allows you to create larger credit buckets and smaller time slices, you can prevent constricting the flow of rate-limited, bursty traffic.

**Note:** If you do not specify this option, rate-limiting will provide accurate results (to within 10-15%) for “smooth” traffic only (e.g., traffic created by a traffic generator). For example, if you use a small credit bucket and a large time slice, a burst of traffic can fill the bucket and cause the X-Pedition router to drop traffic (until the time slice expires and refreshes the credit bucket). This can choke off the traffic rate. For bursty traffic such as TCP and most traffic running on a live network, use the burst-compensating option.

---

|  |   |
|--|---|
| <b>min-bandwidth</b><br><min-bw>             | The minimum bandwidth for each flow. The range for <min-bw> is 3000 to 1000000000.  |
| <b>distribute-among</b><br><number-of-flows> | The number of flows among which freed bandwidth is distributed. The range for <number-of-flows> is 1 to 10. The default is 1. |

---



## Restrictions

Aggregate and flow-aggregate rate limiting are not supported on 802.1q trunk ports.

## Example

The following example defines a rate limit profile client1 for traffic from the 10.10.10.0 network. Packets will be dropped if the rate limit of 10 million bps is exceeded, and each flow will have a minimum bandwidth of 10,000 bps.

```
xp(config)# acl 100 permit ip 10.10.10.0/24 any  
xp(config)# rate-limit client1 flow-aggregate acl 100 rate 10000000 exceed-action drop-packets  
           min-bandwidth  
xp(config)# rate-limit apply client1 interface in1
```

# rate-limit input acl

## Purpose

Defines a policy to enable per flow rate limiting.

## Format

**rate-limit** <name> **input acl** <acl list> **rate** <number> **exceed-action** **drop-packets** | **set-priority-low** | **set-priority-medium** | **set-priority-high** [sequence <number>] | [burst-compensating]

## Mode

Configure.

## Description

The **rate-limit input** command allows you to specify the profile for per flow rate limiting by specifying IP ACLs, the rate limit, and the action to be performed if the rate limit is reached. You then use the **rate-limit apply** command to apply the rate limit to an IP interface. The line card to which you apply this command must be in Per-flow rate limiting mode. See [system enable aggregate-rate-limiting on page 1341](#)

## Parameters

|                               |   |                             |
|-------------------------------|---|-----------------------------|
| <name>                        | The name of the rate limiting policy. The maximum length for this name is 30 bytes or less.   |                             |
| <b>input acl</b> <acl list>   | The ACL(s) that define a per flow rate limiting policy. The <b>rate-limit input</b> command disregards the <b>permit/deny</b> keywords in the ACL rule definition, however, it does look at all parameters in the ACL rule. |                             |
| <b>rate</b> <number>          | Rate limit, in bps, for the flow. This value can be between 1000 and 1000000000.  |                             |
| <b>exceed-action</b> <action> | The action to be taken if the rate limit is exceeded. Specify one of the following keywords:  |                             |
|                               | <b>drop-packets</b>   | Drop the packets.           |
|                               | <b>set-priority-low</b>   | Set the priority to low.    |
|                               | <b>set-priority-medium</b>  | Set the priority to medium. |
|                               | <b>set-priority-high</b>  | Set the priority to high.   |
| <b>sequence</b> <number>      | Sequence number for this policy. This value can be between 1 and 65535.   |                             |

---

**burst-compensating** *<num>* When you choose the burst-compensating option, the X-Pedition router invokes a different algorithm for calculating the rate limit values used by the hardware. This algorithm is better at compensating for *burst capacity*—the ability to maintain an average close to the specified rate—even with large bursts of traffic. The burst-compensating option is available on all rate-limiting policies except port-level output and requires that you enter a burst-compensator value of 1-100 to represent how much burst capacity (in Mbps) to build into the rate limit. For example, setting a low burst-compensator value on a rate limit policy to restrict the flow of an FTP server and client that are capable of very high transfer rates will choke off the flow and produce realized rates that are smaller than the specified rate limit. Conversely, setting a higher burst-compensator value than the flow’s unrestricted capabilities will result in realized rates that are higher than the specified rate limit.

**Note:** Due to hardware constraints, the realized rates for rate limits set above 20 Mbps will become increasingly less consistent and accurate.

The router uses a *credit bucket* bandwidth policing scheme to perform rate limiting. This policy creates a *credit bucket* and *time slice* in the Input Packet Processor hardware and, for a given rate limit, calculates a credit bucket size to represent the amount of traffic that can pass through the processor within a specific time period (i.e., the time slice value). When you specify the burst-compensating option, the credit bucket and time slice values are calculated to take into account traffic spikes or *bursts* and to achieve an average rate that is as close as possible to the specified rate. When the bucket is *filled* within the specified time slice, the router drops packets or changes the priority of the packets, depending on the exceed-action specified. Because the burst compensating option allows you to create larger credit buckets and smaller time slices, you can prevent constricting the flow of rate-limited, bursty traffic.

**Note:** If you do not specify this option, rate-limiting provides accurate results (to within 10-15%) for “smooth” traffic only (e.g., traffic created by a traffic generator). For example, if you use a small credit bucket and a large time slice, a burst of traffic can fill the bucket and cause the router to drop traffic (until the time slice expires and refreshes the credit bucket). This can choke off the traffic rate. For bursty traffic such as TCP and most traffic running on a live network, use the burst-compensating option.

---

## Restrictions

None.

## Example

To define a rate limit profile 'client1' for the ACL '100' that causes packets to be dropped if the rate limit of 10 million bps is exceeded:

```
xp(config)# rate-limit client1 input acl 100 rate-limit 10000000 exceed-action drop-packets
```

# rate-limit port-level input

## Purpose

Defines a rate limiting policy on a per-port basis for incoming traffic.

## Format

**rate-limit** <name> **port-level input** **port** <port list> **rate** <num> [**drop-packets**|**no-action**|**lower-priority**|**lower-priority-except-control**|**tos-precedence-rewrite** <num>|**tos-precedence-rewrite-lower-priority** <num>]

## Mode

Configure.

## Description

The **rate-limit port-level input** command allows you to specify the profile for a rate limiting policy on a per-port basis. This policy only affects incoming traffic to the port. The defined policy will only apply to that specific port and not an aggregation of flows. The line card to which you apply this command must be in Aggregate rate limiting mode. See [system enable aggregate-rate-limiting on page 1341](#).

## Parameters

|  |   |
|--|---|
| <name>                                       | The name of the rate limit.   |
| <b>port</b> <port list> <br><b>all-ports</b> | Specifies which ports to apply the rate-limiting policy. Specify <b>all-ports</b> to enable rate-limiting on all the ports.   |
| <b>rate</b> <num>                            | Specifies the rate limit, in bps, for the flow. This value can be between 1000 and 1000000000.  |
| <b>drop-packets</b>                          | Specifies that if the rate-limit is exceeded, then packets will be dropped.   |
| <b>no-action</b>                             | Specifies that if the rate-limit is exceeded, then no action will be taken.   |
| <b>lower-priority</b>                        | Specifies that if the rate-limit is exceeded, the packets priority is lowered.  |
| <b>lower-priority-except-control</b>         | Specifies that if the rate-limit is exceeded, then the packets priority is lowered, except for control packets.   |
| <b>tos-precedence-rewrite</b> <num>          | Specifies that if the rate-limit is exceeded, the tos precedence in the IP packet header will be rewritten to a specified value. This value can be between 0 and 7. |

|  |  |
|--|--|
| <b>tos-precedence-rewrite-lower-priority</b> <num> | Specifies that if the rate-limit is exceeded, then the tos precedence in the IP packet header will be rewritten to a specified value and the packet priority will be lowered. This value can be between 0 and 7.   |
| <b>burst-compensating</b> <num>                    | <p>When you choose the burst-compensating option, the X-Pedition router invokes a different algorithm for calculating the rate limit values used by the hardware. This algorithm is better at compensating for <i>burst capacity</i>—the ability to maintain an average close to the specified rate—even with large bursts of traffic. The burst-compensating option is available on all rate-limiting policies except port-level output and requires that you enter a burst-compensator value of 1-100 to represent how much burst capacity (in Mbps) to build into the rate limit. For example, setting a low burst-compensator value on a rate limit policy to restrict the flow of an FTP server and client that are capable of very high transfer rates will choke off the flow and produce realized rates that are smaller than the specified rate limit. Conversely, setting a higher burst-compensator value than the flow’s unrestricted capabilities will result in realized rates that are higher than the specified rate limit.</p> <p><b>Note:</b> Due to hardware constraints, the realized rates for rate limits set above 20 Mbps will become increasingly less consistent and accurate.</p> <p>The router uses a <i>credit bucket</i> bandwidth policing scheme to perform rate limiting. This policy creates a <i>credit bucket</i> and <i>time slice</i> in the Input Packet Processor hardware and, for a given rate limit, calculates a credit bucket size to represent the amount of traffic that can pass through the processor within a specific time period (i.e., the time slice value). When you specify the burst-compensating option, the credit bucket and time slice values are calculated to take into account traffic spikes or <i>bursts</i> and to achieve an average rate that is as close as possible to the specified rate. When the bucket is <i>filled</i> within the specified time slice, the router drops packets or changes the priority of the packets, depending on the exceed-action specified. Because the burst compensating option allows you to create larger credit buckets and smaller time slices, you can prevent constricting the flow of rate-limited, bursty traffic.</p> <p><b>Note:</b> If you do not specify this option, rate-limiting provides accurate results (to within 10-15%) for “smooth” traffic only (e.g., traffic created by a traffic generator). For example, if you use a small credit bucket and a large time slice, a burst of traffic can fill the bucket and cause the router to drop traffic (until the time slice expires and refreshes the credit bucket). This can choke off the traffic rate. For bursty traffic such as TCP and most traffic running on a live network, use the burst-compensating option.</p> |

## Restrictions

None.

## Example

To define the port level rate limiting policy 'department' for the input port et.2.1 that causes packets to be dropped if the rate limit of 10 million bps is exceeded:

```
xp(config)# rate-limit department port-level input port et.2.1 rate 10000000 drop-packets
```

# rate-limit port-level slot

## Purpose

Sets rate limiting options for a module.

## Format

**rate-limit** <name> **port-level slot** <num> **ignore-control-priority**

## Mode

Configure.

## Description

The **rate-limit port-level slot** command allows you to set the output port level rate limiting policy to ignore the control priority traffic. This means that there will be no rate limiting for control priority traffic. Note that this policy does not actually try and rate limit the traffic.

## Parameters

|                                |   |
|--------------------------------|---|
| <name>                         | The name of the rate limiting policy.   |
| <b>slot</b> <num>  <b>all</b>  | Specifies the module or slot. This value can be between 0 and 32. Specify <b>all</b> to enable rate-limiting on all modules or slots. |
| <b>ignore-control-priority</b> | This optional parameter specifies that if the rate-limit is exceeded, then the control priority packets will not be dropped.          |

## Restrictions

None.

## Example

To define a rate limiting policy 'dontdrop' for all module or slots to prevent control priority packets from being dropped if the rate limit of 10 million bps is exceeded:

```
xp(config)# rate-limit dontdrop port-level slot all ignore-control-priority
```



# rate-limit port-level output

## Purpose

Defines a rate limiting policy on a per-port basis for outgoing traffic.

## Format

**rate-limit** <name> **port-level output** **port** <port list> **rate** <num> **drop-packets**

## Mode

Configure.

## Description

The **rate-limit port-level output** command allows you to specify the profile for a rate limiting policy on a per-port basis. This policy only affects outgoing traffic to the port, and the only exceed action available is dropping packets. The defined policy will only apply to that specific port and not an aggregation of flows.

## Parameters

|  |   |
|--|---|
| <name>                                       | The name of the rate limit.   |
| <b>port</b> <port list> <br><b>all-ports</b> | Specifies which ports to apply the rate-limiting policy. Specify <b>all-ports</b> to enable rate-limiting on all the ports. |
| <b>rate</b> <number>                         | The rate limit, in bps, for the flow. This value can be between 1000-10000000.  |
| <b>drop-packets</b>                          | This optional parameter specifies that if the rate-limit is exceeded, then packets will be dropped.                         |

## Restrictions

None.

## Example

To define a rate limit policy 'department' for the output port et.2.1 that causes packets to be dropped if the rate limit of 10 million bps is exceeded:

```
xp(config)# rate-limit department port-level output port et.2.1 rate 10000000 drop-packets
```

# rate-limit show

## Purpose

Displays rate limiting policies.

## Format

```
rate-limit show [all] [[policy-type flow-policies| flow-aggregate-policies| aggregate-policies|
portlevel-policies|all]][policy-name <name>]][interface <interface>]|
[port-level port <port list> |all-port] | [port-level policy-name <name>]][rate-limiting-mode]
```

## Mode

Enable.

## Description

The **rate-limit show** command shows information about rate limiting policies.

## Parameters

|  |   |
|--|---|
| <b>all</b>   | Displays information on all rate limit policies configured on the X-Pedition router.  |
| <b>policy-type</b>                                 | The type of the rate limit policy. The keyword <b>all</b> shows all rate limit types. You can specify the following types of policies:<br><br><b>flow-policies</b> All flow policies<br><br><b>flow-aggregate-policies</b> All software-based flow-aggregate policies<br><br><b>aggregate-policies</b> All aggregate policies<br><br><b>portlevel-policies</b> All port level policies<br><br><b>all</b> All policies |
| <b>policy-name &lt;name&gt;</b><br>  <b>all</b>    | The name of the rate limiting policy. The keyword <b>all</b> shows all rate limit policies.   |
| <b>interface &lt;interface&gt;</b><br>  <b>all</b> | The name of the IP interface. The keyword <b>all</b> shows rate limiting policies for all IP interfaces.<br><br><b>Note:</b> Enterasys recommends that you use alphabetic characters when defining interface names—purely numeric interfaces will be interpreted as IP addresses. The X-Pedition router displays interface names up to 32 characters in length.   |

|  |  |
|--|--|
| <b>port-level port</b><br><port list>   <b>all-ports</b> | The name of the port. The keyword <b>all-ports</b> shows rate limiting policies for all ports.   |
| <b>port-level policy-name</b> <name>                     | The name of the rate limiting policy name.   |
| <b>rate-limiting-mode</b>                                | Shows the current rate limiting mode, whether per-flow rate limiting or aggregate rate limiting. |

## Restrictions

None.

## Example

To show all configured rate limit policies:

|                                  |                 |               |               |         |       |       |
|----------------------------------|-----------------|---------------|---------------|---------|-------|-------|
| xp# <b>rate-limit show all</b>   |                 |               |               |         |       |       |
| -----                            |                 |               |               |         |       |       |
| Rate Limit Policy name : rlpol ❶ |                 |               |               |         |       |       |
| Applied Interfaces : if0 ❷       |                 |               |               |         |       |       |
| ❸                                | ❹               | ❺             | ❻             | ❼       | ❽     | ❾     |
| ACL                              | Source IP/Mask  | Dest. IP/Mask | SrcPort       | DstPort | TOS   | Prot  |
| -----                            | -----           | -----         | -----         | -----   | ----- | ----- |
| 100                              | 10.212.10.11/32 | anywhere      | any           | any     | any   | IP    |
| 200                              | 10.212.10.12/32 | anywhere      | any           | any     | any   | IP    |
| 300                              | 10.212.10.13/32 | anywhere      | any           | any     | any   | IP    |
| 400                              | 10.212.10.14/32 | anywhere      | any           | any     | any   | IP    |
| 500                              | 10.212.10.10/32 | anywhere      | any           | any     | any   | IP    |
| ❿                                | ⓫               | ⓬             | ⓭             |         |       |       |
| Seq                              | ACL             | Rate Limit    | Exceed Action |         |       |       |
| ----                             | -----           |               |               |         |       |       |
| 10                               | 100             | 26000         | Low           |         |       |       |
| 10                               | 200             | 26000         | Low           |         |       |       |
| 10                               | 300             | 26000         | Low           |         |       |       |
| 10                               | 400             | 26000         | Low           |         |       |       |
| 10                               | 500             | 26000         | Low           |         |       |       |

### Legend:

1. The name of the rate limit.
2. The IP interface to which the rate limit is applied.
3. The name of the ACL(s) that define the rate limit.
4. The source address and filtering mask specified by the ACL.

5. The destination address and filtering mask specified by the ACL.
6. The number of the TCP or UDP source port.
7. The number of the TCP or UDP destination port.
8. The Type of Service value.
9. The protocol for the ACL.
10. The sequence number for this policy.
11. The name of the ACL.
12. The rate limit for the flow.
13. The action to be taken if the rate limit is reached: packets can be dropped or the priority set to low, medium, or high.

# rate-limit vlan port

## Purpose

Defines a rate limit policy on a per-vlan basis for *incoming* or per-port *outgoing* traffic.

## Format

**rate-limit** <name> **vlan** <name> **port** <port list> | **all-ports** **destport** <port list> | **all-ports** **rate** <num> **exceed-action** **drop-packets** | **set-priority-low** | **set-priority-medium** | **set-priority-high** [**burst-compensating**] [**aggregate**]

## Mode

Configure.

## Description

The **rate-limit vlan port** command specifies the rate limiting policy for incoming traffic on a particular vlan, or outgoing traffic on a port belonging to a specific vlan. Like Port rate limiting policies, you do not specify an ACL when defining this type of policy. Vlan rate limiting policies do not need to be applied to an interface and take affect when they are created. The line card to which you apply this command must be in Per-flow rate limiting mode. See [system enable aggregate-rate-limiting on page 1341](#).

**Note:** When you use the VLAN rate limiting policy to limit outgoing traffic on a port belonging to a specified VLAN, multicast and broadcast traffic will not be rate limited.

## Parameters

|  |   |
|--|---|
| <name>   | The name of the rate limit.   |
| <b>vlan</b> <name>                             | The name of the VLAN.   |
|  | <b>Note:</b> The X-Pedition router displays VLAN names up to 32 characters in length.   |
| <b>port</b> <port-list>   <b>all-ports</b>     | Specifies which ports to apply the rate-limiting policy. Specify <b>all-ports</b> to enable rate-limiting on all the ports belonging to the specified VLAN.           |
| <b>destport</b> <port-list>   <b>all-ports</b> | Specifies which exit ports to apply the rate-limiting policy. Specify <b>all-ports</b> to enable rate-limiting on all the exit ports belonging to the specified VLAN. |
| <b>rate</b> <num>                              | Specifies the rate limit, in bps, for the VLAN or VLAN port. This value can be between 1000 and 1000000000.   |

|                                    |   |                     |                  |                         |                         |                            |                            |                          |                          |
|------------------------------------|---|---------------------|------------------|-------------------------|-------------------------|----------------------------|----------------------------|--------------------------|--------------------------|
| <b>exceed-action</b><br><action>   | <p>The action to be taken if the rate limit is exceeded. Specify one of the following keywords:</p> <table><tr><td><b>drop-packets</b></td><td>Drop the packets</td></tr><tr><td><b>set-priority-low</b></td><td>Set the priority to low</td></tr><tr><td><b>set-priority-medium</b></td><td>Set the priority to medium</td></tr><tr><td><b>set-priority-high</b></td><td>Set the priority to high</td></tr></table>  | <b>drop-packets</b> | Drop the packets | <b>set-priority-low</b> | Set the priority to low | <b>set-priority-medium</b> | Set the priority to medium | <b>set-priority-high</b> | Set the priority to high |
| <b>drop-packets</b>                | Drop the packets  |                     |                  |                         |                         |                            |                            |                          |                          |
| <b>set-priority-low</b>            | Set the priority to low   |                     |                  |                         |                         |                            |                            |                          |                          |
| <b>set-priority-medium</b>         | Set the priority to medium  |                     |                  |                         |                         |                            |                            |                          |                          |
| <b>set-priority-high</b>           | Set the priority to high  |                     |                  |                         |                         |                            |                            |                          |                          |
| <b>burst-compensating</b><br><num> | <p>When you choose the burst-compensating option, the X-Pedition router invokes a different algorithm for calculating the rate limit values used by the hardware. This algorithm is better at compensating for <i>burst capacity</i>—the ability to maintain an average close to the specified rate—even with large bursts of traffic. The burst-compensating option is available on all rate-limiting policies except port-level output and requires that you enter a burst-compensator value of 1-100 to represent how much burst capacity (in Mbps) to build into the rate limit. For example, setting a low burst-compensator value on a rate limit policy to restrict the flow of an FTP server and client that are capable of very high transfer rates will choke off the flow and produce realized rates that are smaller than the specified rate limit. Conversely, setting a higher burst-compensator value than the flow’s unrestricted capabilities will result in realized rates that are higher than the specified rate limit.</p> <p><b>Note:</b> Due to hardware constraints, the realized rates for rate limits set above 20 Mbps will become increasingly less consistent and accurate.</p> <p>The router uses a <i>credit bucket</i> bandwidth policing scheme to perform rate limiting. This policy creates a <i>credit bucket</i> and <i>time slice</i> in the Input Packet Processor hardware and, for a given rate limit, calculates a credit bucket size to represent the amount of traffic that can pass through the processor within a specific time period (i.e., the time slice value). When you specify the burst-compensating option, the credit bucket and time slice values are calculated to take into account traffic spikes or <i>bursts</i> and to achieve an average rate that is as close as possible to the specified rate. When the bucket is <i>filled</i> within the specified time slice, the router drops packets or changes the priority of the packets, depending on the exceed-action specified. Because the burst compensating option allows you to create larger credit buckets and smaller time slices, you can prevent constricting the flow of rate-limited, bursty traffic.</p> <p><b>Note:</b> If you do not specify this option, rate-limiting will provide accurate results (to within 10-15%) for “smooth” traffic only (e.g., traffic created by a traffic generator). For example, if you use a small credit bucket and a large time slice, a burst of traffic can fill the bucket and cause the X-Pedition router to drop traffic (until the time slice expires and refreshes the credit bucket). This can choke off the traffic rate. For bursty traffic such as TCP and most traffic running on a live network, use the burst-compensating option.</p> |                     |                  |                         |                         |                            |                            |                          |                          |

|                  |  |
|------------------|--|
| <b>aggregate</b> | Specifying the aggregate option will aggregate all flows matching this policy and distribute the specified rate among these flows. If you do not specify this option, each matching flow will be limited to the full rate. |
|------------------|--|

## Restrictions

When using the VLAN rate limiting policy to limit outgoing traffic on a port belonging to a specified VLAN, multicast and broadcast traffic will not be rate limited.

## Example

To define a rate limit policy “client1” for the VLAN “red” that causes packets to be dropped if the rate limit of 10 million bps is exceeded.

```
xp(config)# rate-limit client1 vlan red port all-ports rate 10000000 exceed-action drop-packets
```





# Chapter 59

## rdisc Commands

The **rdisc** commands allow you to configure router advertisement on the X-Pedition router.

### Command Summary

[Table 51](#) lists the **rdisc** commands. The sections following the table describe the command syntax.

**Table 51. rdisc Commands**

|   |
|---|
| <b>rdisc add address</b> <i>&lt;hostname-or-ipaddr&gt;</i>  |
| <b>rdisc add interface all</b>  |
| <b>rdisc set address</b> <i>&lt;ipaddr&gt;</i> <b>type</b> multicast broadcast <b>advertise</b> enable disable<br><b>preference</b> <i>&lt;number&gt;</i>  ineligible |
| <b>rdisc set interface all min-adv-interval</b> <i>&lt;number&gt;</i> <b>max-adv-interval</b> <i>&lt;number&gt;</i><br><b>lifetime</b> <i>&lt;number&gt;</i>          |
| <b>rdisc show all</b>   |
| <b>rdisc start</b>  |

## rdisc add address

### Purpose

Defines the IP address(es) that are to be included in router advertisements sent by the X-Pedition router.

### Format

**rdisc add address** *<hostname-or-ipaddr>*

### Mode

Configure.

### Description

The **rdisc add address** command lets you define addresses to be included in router advertisements. If you configure this command, only the specified hostname(s) or IP address(es) are included in the router advertisements.

### Parameters

|                                   |   |
|-----------------------------------|---|
| <i>&lt;hostname-or-ipaddr&gt;</i> | Defines the hostname or IP address(es) to be included in the router advertisements. |
|-----------------------------------|---|

### Restrictions

None.

### Example

To define an address to be included in router advertisements:

```
xp(config)# rdisc add address 10.10.5.254
```

# rdisc add interface

## Purpose

Enables router advertisement on all interfaces.

## Format

**rdisc add interface all**

## Mode

Configure.

## Description

The **rdisc add interface** command lets you enable router advertisement on all interfaces. By default, all addresses on the interface are included in router advertisements sent by the X-Pedition router. If you want to have only specific addresses included in router advertisements, use the **rdisc add address** command to specify those addresses.

## Parameters

|            |   |
|------------|---|
| <b>all</b> | Enables router advertisement on all interfaces. By default, router advertisement is disabled on all interfaces. |
|------------|---|

## Restrictions

None.

## Example

To enable router advertisement on all interfaces:

```
xp(config)# rdisc add interface all
```

# rdisc set address

## Purpose

Configures router advertisement parameters that apply to a specific address.

## Format

**rdisc set address** <ipaddr> **type** multicast|broadcast **advertise** enable|disable  
**preference** <number> |ineligible

## Mode

Configure.

## Description

The **rdisc set address** command lets you specify the type of router advertisement in which the address is included and the preference of the address for use as a default route.

## Parameters

|   |   |   |
|---|---|---|
| <ipaddr>                                  | Specifies the IP address.   |   |
| <b>type</b><br><b>multicast broadcast</b> | Specifies the type of router advertisement in which the IP address is to be included:   |   |
|   | <b>multicast</b>  | Specifies that the IP address should only be included in a multicast router advertisement. This is the default.               |
|   | <b>broadcast</b>  | Specifies that the IP address should only be included in a broadcast router advertisement, even if IP multicast is available. |
| <b>advertise</b><br><b>enable disable</b> | Specifies whether the IP address is included in the router advertisements:  |   |
|   | <b>enable</b>   | Include the IP address in router advertisements. This is the default.   |
|   | <b>disable</b>  | Do not include the IP address in router advertisements.   |
| <b>preference</b><br><number> ineligible  | Specifies the degree of preference of the IP address as a default route. The higher the value, the more preference. If the IP address is ineligible to be a default route, specify <b>ineligible</b> . Valid values are -2147483647 to +2147483647. The default value is 0. |   |

## Restrictions

None.

## Example

To specify that an address be included only in broadcast router advertisements and that the address is ineligible to be a default route:

```
xp(config)# rdisc set address 10.20.36.0 type broadcast preference ineligible
```

## rdisc set interface

### Purpose

Configures router advertisement parameters applying to all interfaces.

### Format

**rdisc set interface all min-adv-interval** *<number>* **max-adv-interval** *<number>*  
**lifetime** *<number>*

### Mode

Configure.

### Description

The **rdisc set interface** command lets you specify the intervals between the sending of router advertisements and the lifetime of addresses sent in a router advertisement.

### Parameters

|  |   |
|--|---|
| <b>all</b>                                       | Applies parameters to all interfaces.   |
| <b>min-adv-interval</b><br><i>&lt;number&gt;</i> | Specifies the minimum time, in seconds, allowed between the sending of unsolicited broadcast or multicast router advertisements. This value can be between 3-1800. The default is 0.75 times the <b>max-adv-interval</b> value. |
| <b>max-adv-interval</b><br><i>&lt;number&gt;</i> | Specifies the maximum time, in seconds, allowed between the sending of unsolicited broadcast or multicast router advertisements. This value can be between 4-1800. The default value is 600 seconds.                            |
| <b>lifetime</b> <i>&lt;number&gt;</i>            | Specifies the lifetime, in seconds, of addresses in a router advertisement. This value can be between 4-9000. The default is 3 times the <b>max-adv-interval</b> value.   |

### Restrictions

None.

## Example

To specify the maximum time between the sending of router advertisements on all interfaces:

```
xp(config)# rdisc set interface all max-adv-interval 1200
```

Note that since the **min-adv-interval** and **lifetime** parameters were not specified, the default values for those parameters become 900 seconds and 3600 seconds, respectively.

## **rdisc show**

### **Purpose**

Shows the state of router discovery on the X-Pedition router.

### **Format**

**rdisc show all**

### **Mode**

Enable.

### **Description**

The **rdisc show** command shows the state of router discovery on the X-Pedition router.

### **Parameters**

|            |  |
|------------|--|
| <b>all</b> | Displays all router discovery information. |
|------------|--|

### **Restrictions**

None.



## Example

To display router discovery information:

```

xp# rdisc show all

Task State: <Foreground NoResolv NoDetach> ❶

  Send buffer size 2048 at 812C68F8
  Recv buffer size 2048 at 812C60D0

Timers:

  RouterDiscoveryServer Priority 30

    RouterDiscoveryServer_xp2_xp3_IP <OneShot>
      last: 10:17:21 next: 10:25:05 ❷

Task RouterDiscoveryServer:
  Interfaces:
    Interface xp2_xp3_IP: ❸
      Group 224.0.0.1: ❹
        minadvint 7:30 maxadvint 10:00 lifetime 30:00 ❺

        Address 10.10.5.254: Preference: 0 ❻

  Interface policy:
    Interface xp2_xp3_IP* MaxAdvInt 10:00 ❼

```

### Legend:

1. Information about the RDISC task.
2. Shows when the last router advertisement was sent and when the next advertisement will be sent.
3. The interface on which router advertisement is enabled.
4. Multicast address.
5. Current values for the intervals between the sending of router advertisements and the lifetime of addresses sent in a router advertisement.
6. IP address that is included in router advertisement. The preference of this address as a default route is 0, the default value.
7. Shows configured values for the specified interface.

## **rdisc start**

### **Purpose**

Starts router discovery on the X-Pedition router.

### **Format**

**rdisc start**

### **Mode**

Configure.

### **Description**

The **rdisc start** command lets you start router discovery on the X-Pedition router. When router discovery is started, the X-Pedition router multicasts or broadcasts periodic router advertisements on each configured interface. The router advertisements contain a list of addresses on a given interface and the preference of each address for use as the default route on the interface. By default, router discovery is disabled.

### **Parameters**

None.

### **Restrictions**

None.

# Chapter 60

## reboot Command

The **reboot** command reboots the X-Pedition router.

### Format

**reboot**

### Mode

Enable.

### Parameters

None.

### Restrictions

None.



# Chapter 61

## rip Commands

The Routing Information Protocol, Version 1 and Version 2 (RIPv1 and RIPv2), is the most commonly used interior gateway protocol. RIP selects the route with the lowest metric as the best route. The metric is a hop count representing the number of gateways through which data must pass in order to reach its destination. The longest path that RIP accepts is 15 hops. If the metric is greater than 15, a destination is considered unreachable and the X-Pedition router discards the route. RIP assumes that the best route is the one that uses the fewest gateways, that is, the shortest path. RIPv1 is described in RFC 1058 and RIPv2 is described in RFC 1723.

**Note:** The X-Pedition router supports a maximum of 120 RIP interfaces.

### Command Summary

[Table 52](#) lists the **rip** commands. The sections following the table describe the command syntax.

**Table 52. rip Commands**

|  |
|--|
| <b>rip add interface</b> <interfacename-or-IPaddr>   <b>source-gateways</b>   <b>trusted-gateways</b> <hostname-or-IPaddr>   |
| <b>rip set auto-summary</b> disable   enable   |
| <b>rip set broadcast-state</b> always   choose   never   |
| <b>rip set check-zero</b> disable   enable   |
| <b>rip set check-zero-metric</b> disable   enable  |
| <b>rip set default-metric</b> <num>  |
| <b>rip set interface</b> <interfacename-or-IPaddr>   <b>all</b> [ <b>receive-rip</b> enable   disable] [ <b>send-rip</b> enable   disable] [ <b>metric-in</b> <num>] [ <b>metric-out</b> <num>] [ <b>version</b> 1  <b>version</b> 2 [ <b>type</b> broadcast multicast]] <b>authentication-method</b> [none (simple md5 <b>key-chain</b> <num-or-string>)] |

**Table 52. rip Commands (Continued)**

|   |
|---|
| <b>rip set max-routes</b> <i>&lt;num&gt;</i>  |
| <b>rip set multipath off</b>  |
| <b>rip set poison-reverse</b> <b>disable</b>   <b>enable</b>  |
| <b>rip set preference</b> <i>&lt;num&gt;</i>  |
| <b>rip show</b> { <b>all</b>   <b>globals</b>   <b>timers</b>   <b>interface</b>   <b>active-gateways</b>   <b>interface-policies</b>   <b>import-policies</b>   <b>export-policies</b> } [ <b>to-terminal</b>   <b>to-file</b> ] |
| <b>rip start</b>  |
| <b>rip stop</b>   |
| <b>rip trace</b> [ <b>packets</b>   <b>request</b>   <b>response</b>   <b>local-options</b> ] [ <b>detail</b> ] [ <b>send</b>   <b>receive</b> ]  |

# rip add

## Purpose

Adds RIP entities.

**Note:** By default, RIP is disabled on all X-Pedition interfaces. To enable RIP on an interface, you must use the **rip add interface** command.

## Format

**rip add interface** <interfacename-or-IPaddr> | **source-gateways** |  
**trusted-gateways** <hostname-or-IPaddr>

## Mode

Configure.

## Description

The **rip add** command lets you add the following RIP entities:

- Interfaces that will run RIP
- Routers that send RIP updates directly, rather than through broadcast or multicast
- Trusted gateways, from which the X-Pedition router will accept RIP updates. when you add trusted gateways, the X-Pedition router does not accept RIP updates from sources other than those trusted gateways.

## Parameters

|   |   |
|---|---|
| <b>interface</b><br><interfacename-or-IPaddr> | Informs the RIP process about the specified interfaces. You can specify a list of interface names or IP addresses or use the <b>all</b> keyword to specify all interfaces.<br><br><b>Note:</b> The X-Pedition router supports a maximum of 120 RIP interfaces. Enterasys recommends that you use alphabetic characters when defining interface names—purely numeric interfaces will be interpreted as IP addresses.<br><br><b>Note:</b> The X-Pedition router displays interface names up to 32 characters in length. |
|---|---|

|   |   |
|---|---|
| <b>source-gateways</b>                                      | <p>Adds a router that sends RIP updates directly, rather than using broadcasts or multicasts. You can specify a single interface name or IP address.</p> <p><b>Note:</b> Updates to source gateways are not affected by the RIP packet transmission state of the interface. Enterasys recommends that you use alphabetic characters when defining interface names—purely numeric interfaces will be interpreted as IP addresses. The X-Pedition router displays interface names up to 32 characters in length.</p>                                      |
| <b>trusted-gateway</b><br><i>&lt;hostname-or-IPaddr&gt;</i> | <p>The hostname or IP address of the source or trusted gateway. Adds a trusted source for RIP updates. When you add trusted gateways, the X-Pedition router will not accept RIP updates from any sources except the trusted gateways. You can specify a single interface name or IP address.</p> <p><b>Note:</b> Enterasys recommends that you use alphabetic characters when defining interface names—purely numeric interfaces will be interpreted as IP addresses. The X-Pedition router displays interface names up to 32 characters in length.</p> |

## Restrictions

The X-Pedition router supports a maximum of 120 RIP interfaces.



# **rip set auto-summary**

## **Purpose**

Enables automatic summarization and redistribution of RIP routes.

## **Format**

**rip set auto-summary disable | enable**

## **Mode**

Configure.

## **Description**

The **rip set auto-summary** command specifies that routes to subnets should be automatically summarized by the classful network boundary and redistributed into RIP.

**Note:** The **rip set auto-summary** command must be enabled if the router will act as a border gateway using RIP Version 1.

## **Parameters**

|                |  |
|----------------|--|
| <b>disable</b> | Disables automatic summarization and redistribution of RIP routes. |
| <b>enable</b>  | Enables automatic summarization and redistribution of RIP routes.  |

## **Restrictions**

None.

# rip set broadcast-state

## Purpose

Determines if RIP packets will be broadcast regardless of the number of interfaces present. This is useful when propagating static routes or routes learned from another protocol into RIP. In some cases, the use of broadcast when only one network interface is present can cause data packets to traverse a single network twice.

## Format

**rip set broadcast-state** **always** | **choose** | **never**

## Mode

Configure.

## Description

The **rip set broadcast-state** command specifies whether the X-Pedition router broadcasts RIP packets regardless of the number of interfaces present.

## Parameters

|               |   |
|---------------|---|
| <b>always</b> | Always sends RIP broadcasts regardless of the number of interfaces present.   |
| <b>choose</b> | Sends RIP broadcasts only if more than one interface is configured on the X-Pedition router. This is the default state. |
| <b>never</b>  | Never sends RIP broadcasts on attached interfaces.  |

## Restrictions

The X-Pedition router supports a maximum of 120 RIP interfaces.

# rip set check-zero

## Purpose

Specifies whether RIP should make sure that reserved fields in incoming RIP V1 packets are zero. Normally, RIP will reject packets where the reserved fields are non-zero.

## Format

**rip set check-zero disable | enable**

## Mode

Configure.

## Description

The **rip set check-zero** command specifies whether RIP should make sure that reserved fields in incoming RIP V1 packets are zero. RIP will reject packets where the reserved fields are non-zero.

- If you use the **disable** keyword, RIP does not check the reserved field.
- If you use the **enable** keyword, RIP on the X-Pedition router checks to ensure that the reserved fields in incoming RIP packets are zero. If the reserved field in a RIP packet is not zero, the X-Pedition router discards the packet. This is the default state.

## Parameters

|                |  |
|----------------|--|
| <b>disable</b> | Disables checking of the reserved field. |
| <b>enable</b>  | Enables checking of the reserved field.  |

## Restrictions

None.

# rip set check-zero-metric

## Purpose

Specifies whether RIP should accept routes with a metric of zero. Normally, RIP will reject routes with a metric of zero.

## Format

**rip set check-zero-metric disable | enable**

## Mode

Configure.

## Description

The **rip set check-zero-metric** command specifies whether RIP should accept routes with a metric of zero. This may be necessary for interoperability with other RIP implementations that send routes with a metric of zero.

- If you use the **disable** keyword, RIP accepts routes that have a metric of zero and treats them as though they were received with a metric of 1.
- If you use the **enable** keyword, RIP rejects routes that have a metric of zero. This is the default state.

## Parameters

|                |   |
|----------------|---|
| <b>disable</b> | Disables acceptance of RIP routes that have a metric of zero. |
| <b>enable</b>  | Enables acceptance of RIP routes that have a metric of zero.  |

## Restrictions

None.

# rip set default-metric

## Purpose

Defines the metric used when advertising routes via RIP that were learned from other protocols. If not specified, the default value is 1. This metric may be overridden by a metric specified in the export command.

## Format

**rip set default-metric** *<num>*

## Mode

Configure.

## Description

The **rip set default metric** command defines the metric used when advertising routes via RIP that were learned from other protocols.

## Parameters

---

|                    |   |
|--------------------|---|
| <i>&lt;num&gt;</i> | Specifies the metric. Specify a number from 1 – 16. The default is 1. |
|--------------------|---|

---

## Restrictions

None.

# rip set interface

## Purpose

Set the RIP state, version, type of update messages, metric and authentication scheme used for each interface running RIP.

## Format

```
rip set interface <interfacename-or-IPaddr> | all [advertise-classfull enable | disable]  
[receive-rip enable | disable] [send-rip enable | disable] [metric-in <num>]  
[metric-out <num>] [version 1|version 2 [type broadcast|multicast]]  
[authentication-method none|(simple|md5 key-chain <num-or-string>)]
```

## Mode

Configure.

## Description

The **rip set interface** command lets you set the following parameters for RIP interfaces:

- Whether the interface will accept RIP updates
- Whether the interface will send RIP updates
- The RIP version (RIP V1 or RIP V2)
- The packet type used for RIP V2 updates (broadcast or multicast)
- The metric added to incoming RIP updates
- The metric added to outgoing RIP updates
- The key-chain for RIP update authentication
- The authentication method used for RIP updates (none, simple, or MD5)

## Parameters

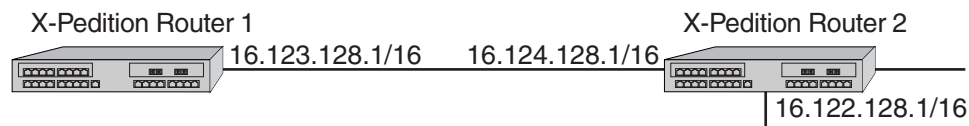
|   |  |
|---|--|
| <code>&lt;interfacename-or-IPaddr&gt; all</code>                      | <p>The interface names or IP addresses of the interfaces for which you are setting RIP parameters. Specify the <b>all</b> keyword if you want to set RIP parameters for all IP interfaces on the X-Pedition router.</p> <p><b>Note:</b> The X-Pedition router supports a maximum of 120 RIP interfaces.</p> <p><b>Note:</b> Enterasys recommends that you use alphabetic characters when defining interface names—purely numeric interfaces will be interpreted as IP addresses. The X-Pedition router displays interface names up to 32 characters in length.</p>   |
| <code>advertise-classfull<br/>enable disable</code>                   | <p>This command is used to announce a classfull network onto a subnetted RIP Version 1 interface having the same classfull network.</p>  |
| <code>receive-rip<br/>enable disable</code>                           | <p>Specifies whether the interface(s) can receive RIP updates. Specify <b>enable</b> if you want to receive RIP updates on the interface. Otherwise, select <b>disable</b>. The default is <b>enable</b>.</p> <p><b>Note:</b> This option affects RIP updates sent from trusted gateways. If you specify <b>disable</b>, the X-Pedition router will not receive any RIP updates, including those sent from trusted gateways. If you specify <b>enable</b> and you have set up trusted gateways, the router will accept updates only from those trusted gateways.</p> |
| <code>send-rip<br/>enable disable</code>                              | <p>Specifies whether the interface(s) can send RIP updates. Specify <b>enable</b> to send RIP updates from this interface. Otherwise, specify <b>disable</b>. The default is <b>enable</b>.</p> <p><b>Note:</b> This option does not affect the sending of updates to source gateways.</p>   |
| <code>metric-in &lt;num&gt;</code>                                    | <p>Specifies a metric that the interface adds to incoming RIP routes before adding them to the interface table. Specify a metric from 1 – 16. Use this option to make the router prefer RIP routes learned from the specified interfaces less than RIP routes from other interfaces. The default is 1.</p>   |
| <code>metric-out &lt;num&gt;</code>                                   | <p>Specifies a metric that the interface adds to outgoing RIP routes sent through the specified interfaces. The default is 0. Use this option to make other routers prefer other sources of RIP routes over this router.</p>   |
| <code>version 1 version 2<br/>[type broadcast  <br/>multicast]</code> | <p>Specifies the RIP version used on the interface(s).</p>   |
| <code>broadcast</code>  | <p>Causes RIP V2 packets that are RIP V1-compatible to be broadcast on this interface.</p>   |
| <code>multicast</code>  | <p>Causes RIP V2 packets to be multicasted on this interface; this is the default.</p>   |

|   |   |   |
|---|---|---|
| <b>authentication-method</b> <b>none</b>   <b>(simple   md5 key-chain</b> <b>&lt;num-or-string&gt;)</b>   | The authentication method the interface uses to authenticate RIP updates. Specify one of the following: |   |
|   | <b>none</b>   | The interface does not use any authentication.  |
|   | <b>simple</b>   | The interface uses a simple password in which an authentication key of up to 8 characters is included in the packet.  |
|   | <b>md5</b>  | The interface uses MD5 authentication. This method uses the MD5 algorithm to create a crypto-checksum of a RIP packet and an authentication key of up to 16 characters. |
| <b>Note:</b> If you choose the <b>simple</b> or <b>md5</b> authentication method, you must specify a key-chain identifier using the key-chain option. |   |   |
|   | <b>key-chain</b> <b>&lt;num-or-string&gt;</b>   | The identifier of the key-chain containing the authentication keys. This parameter applies only if you specified simple or md5 for the authentication type.             |

## Restrictions

The X-Pedition router supports a maximum of 120 RIP interfaces.

## Example



In this example, Router 1 has the following three interfaces:

1. It is connected to Router 2 over interface 16.123.128.1/16. It is running RIP version 1 on this interface.
2. It has two other interfaces with the following addresses (16.124.128.1/16, 16.122.128.1/16).
3. Router 1 the entire class A network (16.0.0.0/8) behind it.

By default, Router 1 would not announce a classful network (16.0.0.0/8) over a subnet (16.123.128.1/16). If that is desired, then the following command should be entered.

```
rip set interface 16.123.128.1 advertise-classfull enable | disable
```

Typically, a user would enable automatic summarization for RIP. This would create an implicit aggregate 16.0.0.0/8. If it is desired, that this classfull network is announced over a subnetted RIP Version 1 interface, then the above command should be entered.



# **rip set max-routes**

## **Purpose**

Defines the maximum number of RIP routes.

## **Format**

**rip set default-metric** *<num>*

## **Mode**

Configure.

## **Description**

The **rip set max-routes** command defines the maximum number of RIP routes that can be maintained by the Routing Information Base (RIB).

## **Parameters**

---

|                    |   |
|--------------------|---|
| <i>&lt;num&gt;</i> | Specifies the maximum number of routes. Specify a number from 1 – 4.<br>The default is 4. |
|--------------------|---|

---

## **Restrictions**

None.

# rip set multipath

## Purpose

Disables multipath route calculation for RIP routes.

## Format

**rip set multipath off**

## Mode

Configure.

## Description

The **rip set multipath** command disables multipath route calculation for RIP routes. No multipath forwarding occurs when this command is used.

## Parameters

|            |                                       |
|------------|---------------------------------------|
| <b>off</b> | Disables multipath route calculation. |
|------------|---------------------------------------|

## Restrictions

If you negate this command from the configuration file, the X-Pedition router will not automatically recreate multipath routes. To recreate multipath routes, stop and restart RIP.

# **rip set poison-reverse**

## **Purpose**

Enables poison reverse on all X-Pedition interfaces.

## **Format**

**rip set poison-reverse disable | enable**

## **Mode**

Configure.

## **Description**

The **rip set poison-reverse** command allows you to enable or disable poison reverse on all X-Pedition interfaces. The X-Pedition router supports poison reverse as specified by RFC 1058.

**Note:** Turning on poison reverse will approximately double the amount of RIP updates.

## **Parameters**

|                |   |
|----------------|---|
| <b>disable</b> | Disables poison reverse on the X-Pedition router. |
| <b>enable</b>  | Enables poison reverse on the X-Pedition router.  |

## **Restrictions**

None.

# rip set preference

## Purpose

Sets the preference of routes learned from RIP. The default preference is 100. This preference may be overridden by a preference specified in the import command.

## Format

**rip set preference** <num>

## Mode

Configure.

## Description

The **rip set preference** command sets the preference for destinations learned through RIP. The preference you specify applies to all IP interfaces for which RIP is enabled on the X-Pedition router. The default preference is 100. You can override this preference by specifying a different preference in an import policy.

## Parameters

|       |   |
|-------|---|
| <num> | Specifies the preference. Specify a number from 0 – 255.<br>The default is 100. Lower numbers have higher preference. |
|-------|---|

## Restrictions

None.

---

# rip show

## Purpose

Display RIP information.

## Format

**rip show** { **all** | **globals** | **timers** | **interface** | **active-gateways** | **interface-policies** | **import-policies** | **export-policies** } [**to-terminal** | **to-file**]

## Mode

Enable.

## Description

The **rip show** command displays RIP information.

## Parameters

|                |                                |   |
|----------------|--------------------------------|---|
| <b>all</b>     | Displays all RIP tables.       |   |
| <b>globals</b> | Displays RIP globals.          |   |
| <b>timers</b>  | Displays the following timers: |   |
|                | <b>Flash Timer</b>             | The network sends and receives RIP responses each time it encounters a change to the network (e.g., a new interface) until it updates the routing table to reflect the changes. A Flash Timer consolidates the list of RIP response packets and sends them randomly every 1-5 seconds instead of as they appear. Once the routing table update is complete, the timer remains inactive until the next routing table change or until 30 seconds passes and the Update Timer solicits the network status. |
|                | <b>Update Timer</b>            | Returns the network status every 30 seconds, regardless whether or not your routing table changed.  |
|                | <b>Age Timer</b>               | The Age Timer is an automated process used to delete any expired routes. The Age Timer will fire every 3 minutes unless a route will expire within the 3-minute period. In this case, the timer will change to coincide with the route expiration.  |

|                           |  |
|---------------------------|--|
| <b>interface</b>          | Displays RIP interfaces.                       |
| <b>active-gateways</b>    | Displays active gateways running RIP.          |
| <b>interface-policies</b> | Displays RIP interface policies.               |
| <b>import-policies</b>    | Displays RIP import policies.                  |
| <b>export-policies</b>    | Displays RIP export policies.                  |
| <b>to-terminal</b>        | Displays the information on screen (default).  |
| <b>to-file</b>            | Writes the information to the gated dump file. |

## Restrictions

None.

## Example

The following examples show the timers over a period of time:

|                                    |          |          |          |       |        |          |
|------------------------------------|----------|----------|----------|-------|--------|----------|
| xp(enable)# <b>rip show timers</b> |          |          |          |       |        |          |
| Timers:                            |          |          |          |       |        |          |
| -----                              |          |          |          |       |        |          |
| Timer                              | State    | Last     | Next     | Intvl | Jitter | Flags    |
| -----                              |          |          |          |       |        |          |
| RIP.0.0.0.0+520_Flash              | Inactive | -        | -        | -     | -      | Inactive |
| RIP.0.0.0.0+520_Update             | Active   | 15:40:35 | 15:41:05 | 30    | -      |          |
| RIP.0.0.0.0+520_Age                | Active   | 15:39:00 | 15:42:00 | -     | -      | OneShot  |

|                                    |        |          |          |       |        |         |
|------------------------------------|--------|----------|----------|-------|--------|---------|
| xp(enable)# <b>rip show timers</b> |        |          |          |       |        |         |
| Timers:                            |        |          |          |       |        |         |
| -----                              |        |          |          |       |        |         |
| Timer                              | State  | Last     | Next     | Intvl | Jitter | Flags   |
| -----                              |        |          |          |       |        |         |
| RIP.0.0.0.0+520_Flash              | Active | 15:41:05 | 15:41:09 | 4     | -      |         |
| RIP.0.0.0.0+520_Update             | Active | 15:41:05 | 15:41:35 | 30    | -      |         |
| RIP.0.0.0.0+520_Age                | Active | 15:39:00 | 15:42:00 | -     | -      | OneShot |

```

xp(enable)# rip show timers

```

Timers:

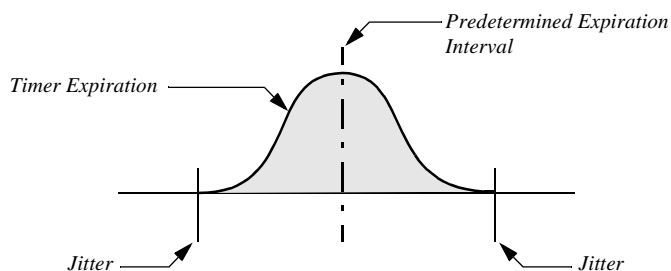
---

| Timer                  | State    | Last     | Next     | Intvl | Jitter | Flags    |
|------------------------|----------|----------|----------|-------|--------|----------|
| RIP.0.0.0.0+520_Flash  | Inactive | -        | -        | -     | -      | Inactive |
| RIP.0.0.0.0+520_Update | Active   | 15:41:05 | 15:41:35 | 30    | -      |          |
| RIP.0.0.0.0+520_Age    | Active   | 15:39:00 | 15:42:00 | -     | -      | OneShot  |

The following describes the show timer columns:

|                                   |   |
|-----------------------------------|---|
| <b>State (active or inactive)</b> | The state of the timer. Scheduled timers are inactive.  |
| <b>Last and Next</b>              | A timestamp of the last and next time the timer was and will be used.   |
| <b>Interval</b>                   | Time (in seconds) between timer activities that are periodic as opposed to OneShot. The Age Timer is considered a OneShot because the interval may not be consistent.   |
| <b>Jitter</b>                     | To prevent peak volumes of network activity associated with timers, the network uses a <i>Jitter</i> . Jitter is displayed when the next expiration will occur at the predetermined interval plus or minus a few microseconds. This helps reduce network congestion. <a href="#">Figure 1</a> depicts a jitter. |
| <b>Flags</b>                      | Indicate whether a timer is inactive or a OneShot.  |

**Figure 1. Jitter Example**



# **rip start**

## **Purpose**

Start RIP on the X-Pedition router.

**Note:** RIP is disabled by default.

## **Format**

**rip start**

## **Mode**

Configure.

## **Description**

The **rip start** command starts RIP on all IP interfaces on the X-Pedition router for which RIP is enabled.

## **Parameters**

None.

## **Restrictions**

None.



# **rip stop**

## **Purpose**

Stop RIP on the X-Pedition router.

## **Format**

**rip stop**

## **Mode**

Configure.

## **Description**

The **rip stop** command stops RIP on all IP interfaces on the X-Pedition router for which RIP is enabled.

## **Parameters**

None.

## **Restrictions**

None.

# rip trace

## Purpose

Trace RIP packets.

## Format

**rip trace** [**packets** | **request** | **response** | **local-options**] [**detail** | **send** | **receive**]

## Mode

Configure.

## Description

The **rip trace** command traces the following sets of RIP packets:

- RIP request packets sent or received by the X-Pedition router
- RIP response packets sent or received by the X-Pedition router

Depending on the options you specify, you can trace all packets, request packets only, or receive packets only. In addition, you can select to trace the request packets, receive packets, or both that are sent by the X-Pedition router, received by the router, or all packets (both sent packets and received packets).

For the **packets**, **request**, and **response** parameters, you can optionally specify one of the following: **detail**, **receive**, or **send**.

## Parameters

|                 |   |
|-----------------|---|
| <b>packets</b>  | Traces all RIP packets, both request packets and response packets. This is the default.   |
| <b>request</b>  | Traces only request packets, such as REQUEST, POLL and POLLENTY packets.  |
| <b>response</b> | Traces only response packets.   |
| <b>detail</b>   | Shows detailed information about the traced packets.  |
| <b>receive</b>  | Shows information about traced RIP packets received by the router.  |
| <b>send</b>     | Shows information about traced RIP packets sent by the X-Pedition router. The default is to show both send and receive packets. |

|                      |   |
|----------------------|---|
| <b>local-options</b> | Sets trace options for this protocol only. These trace options are inherited from those set by the <b>ip-router global set trace options</b> command, or you can override them here. Specify one or more of the following:<br><br><b>all</b> Turns on all tracing.<br><br><b>general</b> Turns on normal and route tracing.<br><br><b>state</b> Traces state machine transitions in the protocols.<br><br><b>normal</b> Traces normal protocol occurrences.<br><br><b>Note:</b> Abnormal protocol occurrences are always traced.<br><br><b>policy</b> Traces application of protocol and user-specified policies to routes being imported and exported.<br><br><b>task</b> Traces system processing associated with this protocol or peer.<br><br><b>timer</b> Traces timer usage by this protocol or peer.<br><br><b>route</b> Traces routing table changes for routes installed by this protocol or peer. |
|----------------------|---|

---

## Restrictions

None.



# Chapter 62

## ripng Commands

The Routing Information Protocol Next Generation (RIPng) is a simple extension of the RIP protocol to support distribution of IPv6 routes. RIPng functions much like RIPv2, using a distance vector scheme to find the shortest path through a network. RIPng tries to avoid loops by using split-horizon and poison-reverse. RIPng uses the counting-to-infinity method of discovering loops in certain situations. It listens on UDP port 521 for RIPng IPv6 packets, and communicates with IPv6 routers and hosts using the all-rip-routers Multicast Address (FF02::9) or unicast destinations addresses as appropriate. RIPng can make use of the IP Authentication Header to ensure the integrity and authenticity of routing exchanges.

RIPng is described in RFP 2080. Most of the concepts of RIPng come from RIPv1, described in RFC 1058, and RIPv2, described in RFC 2453.

### Command Summary

[Table 53](#) lists the **ripng** commands. The sections following the table describe the command syntax.

**Table 53. ripng Commands**

|   |
|---|
| <b>ripng add interface</b> <interfacename>   <b>all</b>   |
| <b>ripng set default-metric</b> <num>   |
| <b>ripng set expire-time</b> <num>  |
| <b>ripng set interface</b> <interfacename>   <b>all</b> [ <b>receive-rip enable</b>   <b>disable</b> ] [ <b>send-rip enable</b>   <b>disable</b> ] [ <b>metric-in</b> <num>] [ <b>metric-out</b> <num>] |
| <b>ripng set poison-reverse enable disable</b>  |
| <b>ripng set preference</b> <num>   |
| <b>ripng set update-time</b> <num>  |

**Table 53. ripng Commands (Continued)**

|   |
|---|
| <b>ripng show</b> <i>&lt;option-list&gt;</i>  |
| <b>ripng start</b>  |
| <b>ripng trace</b> [packets  request  response  local-options] [detail   send  receive] |

# ripng add interface

## Purpose

Enables RIPng on IPv6 interfaces.

## Format

**ripng add interface** <interfacename> | **all**

## Mode

Configure.

## Description

The **ripng add interface** command lets you enable RIPng on IPv6 interfaces.

By default, RIPng is disabled on IPv6 interfaces on the X-Pedition router. To enable RIPng on an interface, you must use this command.

The **no** form of the command is used to delete the configuration previously specified by a matching command that did not include the **no** keyword.

## Parameters

|                 |   |
|-----------------|---|
| <interfacename> | Enables RIPng on the specified interfaces. You can specify a list of interface names.       |
| <b>all</b>      | Use the <b>all</b> keyword to enable RIPng on all IPv6 interfaces on the X-Pedition router. |

## Restrictions

The X-Pedition router supports a maximum of 120 RIP interfaces.

# ripng set default-metric

## Purpose

Defines the metric used when advertising routes via RIPng that were learned from other IPv6 protocols.

## Format

**ripng set default-metric** *<num>*

## Mode

Configure.

## Description

The **ripng set default metric** command defines the metric used when advertising routes via RIPng that were learned from other IPv6 protocols. The only other IPv6 routing protocol currently supported in static routing.

If not specified, the default value is 1.

The **no** form of the command is used to delete the configuration previously specified by a matching command that did not include the **no** keyword. The **no** form of this command restores the default metric of 1 — that is, disables the export of routes from other IPv6 routing protocols into RIPng.

## Parameter

---

|                    |   |
|--------------------|---|
| <i>&lt;num&gt;</i> | Specifies the metric. Specify a number from 1 – 16. The default is 1. |
|--------------------|---|

---

## Restrictions

None.



# ripng set expire-time

## Purpose

Sets the expiration time for routes received via RIPng.

## Format

**ripng set expire-time** *<num>*

## Mode

Configure.

## Description

The **ripng set expire-time** command defines the expiration time (in seconds) for routes received via RIPng. The expiration time for a RIPng route is initialized to *<num>* when the route is first established, and each time a RIPng update message is received for the route. If *<num>* seconds elapse after the expiration time for a route was last initialized, the route is considered to have expired, and the deletion process for that route is begun. By default, the expire-time parameter takes a value of 180 seconds.

The **no** form of the command is used to delete the configuration previously specified by a matching command that did not include the **no** keyword. The **no** form of this command restores the expire-time parameter to the default of 180 seconds.

## Parameters

---

|                    |  |
|--------------------|--|
| <i>&lt;num&gt;</i> | Specifies the value of the expire-time parameter in seconds. Specify a number in the range 5 to 180. The default is 180 seconds. |
|--------------------|--|

---

## Restrictions

None.

# ripng set interface

## Purpose

Sets the RIPng metrics and controls the reception and transmission of RIPng messages on an interface.

## Format

**ripng set interface** <interfacename> | **all** [**receive-rip enable** | **disable**]  
[**send-rip enable** | **disable**] [**metric-in** <num>] [**metric-out** <num>]

## Mode

Configure.

## Description

The **ripng set interface** command lets you set the following parameters for RIPng interfaces:

- Whether the interface will accept RIPng updates
- Whether the interface will send RIPng updates
- The metric added to incoming RIPng updates
- The metric added to outgoing RIPng updates

## Parameters

|                                   |   |
|-----------------------------------|---|
| <interfacename>   <b>all</b>      | The interface names of the interfaces for which you are setting RIPng parameters. Specify the <b>all</b> keyword if you want to set the parameters for all IPv6 interfaces on the X-Pedition router.  |
| <b>receive-rip enable disable</b> | Specifies whether the interface(s) can receive RIPng updates. Specify <b>enable</b> if you want to receive RIP updates on the interface. Otherwise, select <b>disable</b> . Reception and transmission of RIPng updates is enabled by default, whenever RIPng is enabled on an interface. |
| <b>send-rip enable disable</b>    | Specifies whether the interface(s) can send RIPng updates. Specify <b>enable</b> if you want to send RIP updates from this interface. Otherwise, specify <b>disable</b> . Reception and transmission of RIPng updates is enabled by default, whenever RIPng is enabled on an interface.   |

|                         |  |
|-------------------------|--|
| <b>metric-in</b> <num>  | <p>Specifies a metric that the interface adds to incoming RIPng routes before adding them to the routing table. Specify a metric from 1 to 16. The default is 1.</p> <p>Use this option to make the RIPng routes learned from the specified interfaces less preferred than RIPng routes learned from other interfaces.</p>   |
| <b>metric-out</b> <num> | <p>Specifies a metric that the interface adds to outgoing RIPng routes sent over the specified interfaces. You can specify a metric from 1 to 16.</p> <p>The default is 0. To reset the value to 0, prepend the <b>no</b> or <b>negate</b> command.</p> <p>Use this option to make the RIPng routes sent from this router less preferred to receiving routers than RIPng routes received from other routers.</p> |

## Restrictions

None.

# ripng set poison-reverse

## Purpose

Enables or disables poison reverse on all IPv6 interfaces on the X-Pedition router.

## Format

**ripng set poison-reverse disable | enable**

## Mode

Configure.

## Description

The **ripng set poison-reverse** command allows you to enable or disable poison reverse on all IPv6 interfaces on the router. The X-Pedition router supports poison reverse as specified by RFC 1058.

The **no** form of the command is used to delete the configuration previously specified by a matching command that did not include the **no** keyword.

**Note:** Turning on poison reverse could significantly increase the total size of RIPng updates.

## Parameters

|                         |   |
|-------------------------|---|
| <b>disable   enable</b> | Enables or disables poison reverse for IPv6 interfaces on the X-Pedition router. It is disabled by default. |
|-------------------------|---|

## Restrictions

None.

# ripng set preference

## Purpose

Sets the preference of routes learned from RIPng.

## Format

**ripng set preference** *<num>*

## Mode

Configure.

## Description

The **ripng set preference** command sets the preference for routes learned through RIPng. The preference you specify applies to all IPv6 interfaces for which RIPng is enabled on the X-Pedition router. The default preference is 100. You can override this preference by specifying a different preference in an import policy.

The **no** form of the command is used to delete the configuration previously specified by a matching command that did not include the **no** keyword.

## Parameters

---

|                    |   |
|--------------------|---|
| <i>&lt;num&gt;</i> | Specifies the preference. Specify a number from 0 to 255. The default is 100. Lower numbers have higher preference. |
|--------------------|---|

---

## Restrictions

None.

## ripng set update-time

### Purpose

Sets the update time for unsolicited route responses.

### Format

**ripng set update-time** *<num>*

### Mode

Configure.

### Description

The **ripng set update-time** command defines the interval (in seconds) between unsolicited RIPvng route updates sent by this router. By default, the update-time parameter takes a value of 30 seconds.

The **no** form of the command is used to delete the configuration previously specified by a matching command that did not include the **no** keyword. The **no** form of this command restores the update-time parameter to the default of 30 seconds.

### Parameters

---

|                    |  |
|--------------------|--|
| <i>&lt;num&gt;</i> | Specifies the value of the update-time parameter in seconds. Specify a number in the range 1 to 30. The default is 30 seconds. |
|--------------------|--|

---

### Restrictions

None.

# ripng show

## Purpose

Display RIPng information.

## Format

**ripng show** <option> [**to-terminal** | **to-file**]

## Mode

Enable.

## Description

The **ripng show** command displays RIPng information. You can specify the type of information to display by using the options available with this command.

## Parameters

|                                     |   |
|-------------------------------------|---|
| <option>                            | Specifies the RIPng dump information you want to display. Specify one of the following:   |
| <b>all</b>                          | Displays all RIPng tables.  |
| <b>globals</b>                      | Displays RIPng globals.   |
| <b>timers</b>                       | Displays RIPng timers.  |
| <b>interface</b>                    | Displays RIPng interfaces.  |
| <b>active-gateways</b>              | Displays active gateways running RIPng.   |
| <b>interface-policies</b>           | Displays RIPng interface policies.  |
| <b>import-policies</b>              | Displays RIPng import policies.   |
| <b>export-policies</b>              | Displays RIPng export policies.   |
| <b>to-terminal</b>   <b>to-file</b> | Specifies whether output of the selected option should be displayed on the terminal or sent to the file named /cfg/gated.dmp. Default behavior is to display to the terminal. |

## Restrictions

None.

## Examples

The following example displays the RIPng global parameter values:

```
xp# ripng show globals  
RIPng Globals:  
  Task Name: RIPng.::+521  
  Flags: ON  
  Default metric: 1  
  Preference: 100  
  Expire time: 180  
  Update time: 30  
  Poison reverse: Disabled
```

The following example displays RIPng information about interface IPv6\_1:

```
xp# ripng show interface IPv6_1  
Target 1:  
  
  I/f Name: IPv6_1  
  I/f Address: fe80::2e0:63ff:fe13:2003%IPv6_1  
  Source: fe80::2e0:63ff:fe13:2003%IPv6_1  
  Destination: ff02::9  
  I/f Flags: Multicast Poll Broadcast Supply Policy  
  Bit: 9  
  
  Routes: 2 route(s)  
    Prefix/Length: 22:33:44:55::/64  
    Metric: 1  
    Flags:  
  
    Prefix/Length: 11:22:33:44::/64  
    Metric: 1  
    Flags:
```



# **ripng start**

## **Purpose**

Start RIPng on the X-Pedition router.

## **Format**

**ripng start**

## **Mode**

Configure.

## **Description**

The **ripng start** command starts RIPng on all IPv6 interfaces on the X-Pedition router for which RIPng is enabled. The RIPng process is not started by default. The user has to explicitly issue this command to start RIPng on the X-Pedition router.

Use the **no** form of this command to stop RIPng on the X-Pedition router.

## **Parameters**

None.

## **Restrictions**

None.

# ripng trace

## Purpose

Trace RIPng packets.

## Format

**ripng trace** [**packets**| **request**| **response**| **local-options**] [**detail** | **send**| **receive**]

## Mode

Configure.

## Description

The **ripng trace** command traces the following sets of RIPng packets:

- RIPng request packets sent or received by the X-Pedition router
- RIPng response packets sent or received by the X-Pedition router

Depending on the options you specify, you can trace all packets, request packets only, or receive packets only. In addition, you can select to trace only packets that are sent by the X-Pedition router, received by the X-Pedition router, or both sent and received packets.

For the **packets**, **request**, and **response** parameters, you can optionally specify one of the following: **detail**, **receive**, or **send**.

## Parameters

|  |   |
|--|---|
| <b>packets</b>   | Traces all RIPng packets, both request packets and response packets. This is the default. |
| <b>request</b>   | Traces only request packets.  |
| <b>response</b>  | Traces only response packets.   |
| <b>detail</b>  | Shows detailed information about the traced packets.                                      |
| <b>receive</b>   | Shows information about traced RIPng packets received by the X-Pedition router.           |
| <b>Note:</b> The default is to show both send and receive packets. |   |

|                      |  |
|----------------------|--|
| <b>send</b>          | Shows information about traced RIPng packets sent by the X-Pedition router.<br><br><b>Note:</b> The default is to show both send and receive packets.  |
| <b>local-options</b> | Sets trace options for this protocol only. These trace options are inherited from those set by the <b>ip-router global set trace options</b> command, or you can override them here. Specify one or more of the following: |
| <b>all</b>           | Turns on all tracing.  |
| <b>general</b>       | Turns on normal and route tracing.   |
| <b>state</b>         | Traces state machine transitions in the protocols.   |
| <b>normal</b>        | Traces normal protocol occurrences.<br><br><b>Note:</b> Abnormal protocol occurrences are always traced.   |
| <b>policy</b>        | Traces application of protocol and user-specified policies to routes being imported and exported.  |
| <b>task</b>          | Traces system processing associated with this protocol or peer.  |
| <b>timer</b>         | Traces timer usage by this protocol or peer.   |
| <b>route</b>         | Traces routing table changes for routes installed by this protocol or peer.  |

## Restrictions

None.



# Chapter 63

## rmon Commands

The **rmon** commands let you display and set parameters for RMON statistics on a per-port basis. RMON1 (RFC1757) accounts for bridged traffic in host and matrix statistics, but **not** routed traffic. RMON2 (RFC2021) accounts for routed traffic in host, matrix, and protocol distribution statistics, but **not** bridged traffic. This is a hardware limitation.

**Note:** Do not run NetFlow and RMON simultaneously.

### Command Summary

Table 54 lists the **rmon** commands. The sections following the table describe the command syntax.

Table 54. rmon Commands

|  |
|--|
| <b>rmon address-map index</b> <index-number> { <b>port</b> <port> [ <b>owner</b> <string>]<br>[ <b>status enable disable</b> ]} [ <b>max-number</b> <number>   |
| <b>rmon al-matrix-top-n index</b> <index-number> <b>matrix-index</b> <number> <b>ratebase terminal-packets terminal-octets all-packets all-octets duration</b> <number> <b>size</b> <number><br>[ <b>owner</b> <string>] [ <b>status enable disable</b> ]  |
| <b>rmon alarm index</b> <index-number> <b>variable</b> <string> [ <b>interval</b> <seconds>] [ <b>falling-event-index</b> <num>] [ <b>falling-threshold</b> <num>] [ <b>owner</b> <string>] [ <b>rising-event-index</b> <num>]<br>[ <b>rising-threshold</b> <num>] [ <b>startup rising falling both</b> ] [ <b>status enable disable</b> ]<br>[ <b>type absolute-value delta-value</b> ] |
| <b>rmon apply cli-filters</b> <filter id>  |
| <b>rmon capture index</b> <index-number> <b>channel-index</b> <number> [ <b>full-action lock wrap</b> ]<br>[ <b>slice-size</b> <number>] [ <b>download-slice-size</b> <number>] [ <b>download-offset</b> <number>]<br>[ <b>max-octets</b> <number>] [ <b>owner</b> <string>] [ <b>status enable disable</b> ]  |

Table 54. rmon Commands

|  |
|--|
| <b>rmon channel index</b> <index-number> <b>port</b> <port> [ <b>accept-type</b> matched failed] [ <b>data-control</b> on off] [ <b>turn-on-event-index</b> <number>] [ <b>turn-off-event-index</b> <number>] [ <b>event-index</b> <number>] [ <b>channel-status</b> ready always-ready] [ <b>description</b> <string>] [ <b>owner</b> <string>] [ <b>status</b> enable disable] |
| <b>rmon clear cli-filter</b>   |
| <b>rmon enable</b>   |
| <b>rmon etherstats index</b> <index-number> <b>port</b> <port> [ <b>owner</b> <string>] [ <b>status</b> enable disable]  |
| <b>rmon event index</b> <index-number> <b>type</b> none log trap both [ <b>community</b> <string>] [ <b>description</b> <string>] [ <b>owner</b> <string>] [ <b>status</b> enable disable]   |
| <b>rmon filter index</b> <index-number> <b>channel-index</b> <number> [ <b>data-offset</b> <number>] [ <b>data</b> <string>] [ <b>data-mask</b> <string>] [ <b>data-not-mask</b> <string>] [ <b>pkt-status</b> <number>] [ <b>status-mask</b> <number>] [ <b>status-not-mask</b> <number>] [ <b>owner</b> <string>] [ <b>status</b> enable disable]                              |
| <b>rmon history index</b> <index-number> <b>port</b> <port> [ <b>interval</b> <seconds>] [ <b>owner</b> <string>] [ <b>samples</b> <num>] [ <b>status</b> enable disable]  |
| <b>rmon hl-host index</b> <index-number> <b>port</b> <port> <b>nl-max-entries</b> <number> <b>al-max-entries</b> <number> [ <b>owner</b> <string>] [ <b>status</b> enable disable]   |
| <b>rmon hl-matrix index</b> <index-number> <b>port</b> <port> <b>nl-max-entries</b> <number> <b>al-max-entries</b> <number> [ <b>owner</b> <string>] [ <b>status</b> enable disable]   |
| <b>rmon host index</b> <index-number> <b>port</b> <port> [ <b>owner</b> <string>] [ <b>status</b> enable disable]  |
| <b>rmon host-top-n index</b> <index-number> <b>host-index</b> <number> [ <b>base</b> <statistics>] [ <b>duration</b> <time>] [ <b>size</b> <size>] [ <b>owner</b> <string>] [ <b>status</b> enable disable]  |
| <b>rmon matrix index</b> <index-number> [ <b>port</b> <port>] [ <b>owner</b> <string>] [ <b>status</b> enable disable]   |
| <b>rmon nl-matrix-top-n index</b> <index-number> <b>matrix-index</b> <number> <b>ratebase</b> <b>terminal-packets</b>   <b>terminal-octets</b>   <b>all-packets</b>   <b>all-octets</b> <b>duration</b> <number> <b>size</b> <number> [ <b>owner</b> <string>] [ <b>status</b> enable disable]   |
| <b>rmon protocol-distribution index</b> <index-number> <b>port</b> <port> [ <b>owner</b> <string>] [ <b>status</b> enable disable]   |
| <b>rmon set</b> lite  standard  professional <b>default-tables</b> yes  no   |
| <b>rmon set cli-filter</b> <filter-id> <parameter>   |
| <b>rmon set memory</b> <number>  |
| <b>rmon set ports</b> <port list>  <b>all-ports</b>  |
| <b>rmon set protocol-directory</b> <protocol>  <b>all-protocols</b> [ <b>address-map</b> on  off  na] [ <b>host</b> on  off  na] [ <b>matrix</b> on  off  na]  |
| <b>rmon show address-map-control</b> <port-list >  <b>all-ports</b>  |

Table 54. rmon Commands

|   |
|---|
| <b>rmon show address-map-logs</b> <i>&lt;port-list&gt;</i>   <b>all-ports</b>   |
| <b>rmon show al-host</b> <i>&lt;port-list&gt;</i>   <b>all-ports</b> [summary]  |
| <b>rmon show al-matrix</b> <i>&lt;port-list&gt;</i>   <b>all-ports</b> [order-by srcdst  dstsrc] [summary]  |
| <b>rmon show al-matrix-top-n</b>  |
| <b>rmon show alarms</b>   |
| <b>rmon show channels</b>   |
| <b>rmon show cli-filters</b>  |
| <b>rmon show etherstats</b> <i>&lt;port-list&gt;</i>   <b>all-ports</b>   |
| <b>rmon show events</b>   |
| <b>rmon show filters</b>  |
| <b>rmon show history</b> <i>&lt;port-list&gt;</i>   <b>all-ports</b>  |
| <b>rmon show host-top-n</b>   |
| <b>rmon show hosts</b> <i>&lt;port-list&gt;</i>   <b>all-ports</b> [summary]  |
| <b>rmon show matrix</b> <i>&lt;port-list&gt;</i>   <b>all-ports</b> [summary] [order-by srcdst  dstsrc]   |
| <b>rmon show nl-host</b> <i>&lt;port-list&gt;</i>   <b>all-ports</b> [summary]  |
| <b>rmon show nl-matrix</b> <i>&lt;port-list&gt;</i>   <b>all-ports</b> [order-by srcdst  dstsrc] [summary]  |
| <b>rmon show nl-matrix-top-n</b> rmon show  |
| <b>rmon show packet-capture control-table</b> [captured-packets <i>&lt;control-index&gt;</i> ]  |
| <b>rmon show probe-config</b> [basic] [net-config] [trap-dest]  |
| <b>rmon show protocol-directory</b> <i>&lt;protocol&gt;</i>   <b>all-protocols</b>  |
| <b>rmon show protocol-distribution</b> <i>&lt;port-list&gt;</i>   <b>all-ports</b>  |
| <b>rmon show status</b>   |
| <b>rmon</b> <i>&lt;string&gt;</i> show user-history [all-indexes]   |
| <b>rmon user-history-apply</b> <i>&lt;groupname&gt;</i> to <i>&lt;user-history-index&gt;</i> [status enable  disable]   |
| <b>rmon user-history-control index</b> <i>&lt;index-number&gt;</i> <b>objects</b> <i>&lt;number&gt;</i> <b>samples</b> <i>&lt;number&gt;</i> <b>interval</b> <i>&lt;number&gt;</i> [owner <i>&lt;string&gt;</i> ] [status enable disable] |
| <b>rmon user-history-objects</b> <i>&lt;groupname&gt;</i> <b>variable</b> <i>&lt;oid&gt;</i> <b>type</b> absolute-value  delta-value [status enable disable]  |

## rmon address-map

### Purpose

Configures the RMON 2 Address Map group.

### Format

```
rmon address-map index <index-number> {port <port> [owner <string>]  
[status enable|disable]} [max-number <number>
```

### Mode

Configure.

### Description

The Address Map group maps MAC addresses to network address bindings that are discovered by the X-Pedition router on a per-port basis. The **rmon address-map** command sets various parameters of the RMON 2 Address Map table. If the default tables are turned on for the Professional group, an entry in the Address Map control table is created for each available port. Use the **rmon show address-map** command to display the address map.

### Parameters

|                               |   |
|-------------------------------|---|
| <index-number>                | Is a number between 1 and 65535 that uniquely identifies a row in the Address Map table.  |
| <port>                        | Specifies the port from which to collect data.  |
| <b>owner</b> <string>         | Specifies the owner of the event; for example, an IP address, machine name or person's name.  |
| <b>status enable disable</b>  | Enables or disables this matrix. The default is <b>enable</b> .   |
| <b>max-number</b><br><number> | The maximum number of entries (1 to 2147483647) to allow in address-map tables. This is helpful for controlling memory used by the RMON task. |

### Restrictions

None.



## Example

To create an entry in the Address Map table for port et.1.3:

```
xp(config)# rmon address-map index 20 port et.1.3
```

# rmon al-matrix-top-n

## Purpose

Gathers the top *n* Application Layer Matrix entries.

## Format

```
rmon al-matrix-top-n index <index-number> matrix-index <number>  
ratebase terminal-packets|terminal-octets|all-packets|all-octets duration <number>  
size <number> [owner <string>] [status enable|disable]
```

## Mode

Configure.

## Description

The **rmon al-matrix-top-n** command gathers the top *n* Application Layer Matrix entries sorted by a specified statistic. To do this, you must first configure the Application Layer/Network Layer Matrix table using the **rmon hl-matrix** command.

Use the **rmon show al-matrix-top-n** command to display the top *n* Application Layer Matrix entries.

## Parameters

|   |   |                           |
|---|---|---------------------------|
| <index-number>  | Is a number between 1 and 65535 that uniquely identifies a row in the application layer matrix table.   |                           |
| <b>matrix-index</b> <number>  | Specifies the index into the hl-matrix table. The default is 0.   |                           |
| <b>ratebase</b><br><b>terminal-packets</b>  <br><b>terminal-octets</b>  <br><b>all-packets</b>  <br><b>all-octets</b> | <b>terminal-packets</b>   | Sort by terminal packets. |
|   | <b>terminal-octets</b>  | Sort by terminal octets.  |
|   | <b>all-packets</b>  | Sort by all packets.      |
|   | <b>all-octets</b>   | Sort by all octets.       |
| <b>duration</b> <number>  | Specifies the duration, in seconds, between reports. If the duration is 0 (the default), this implies that no reports have been requested for this entry. The default is 0. |                           |

|                              |  |
|------------------------------|--|
| <b>size</b> <number>         | Specifies the maximum number of matrix entries to include in the report. The default is 150. |
| <b>owner</b> <string>        | Specifies the owner of the event; for example, an IP address, machine name or person's name. |
| <b>status</b> enable disable | Enables or disables this matrix. The default is enable.                                      |

## Restrictions

None.

## Example

To monitor the top  $n$  entries in the Application Layer Matrix, you should first configure the Application Layer/Network Layer Matrix table using the **rmon hl-matrix** command. Then, to gather the top 100 Application Layer Matrix entries sorted by all packets, use the following command:

```
xp(config)# rmon al-matrix-top-n index 25 matrix-index 50 ratebase all-packets duration 60 size 100
```

## rmon alarm

### Purpose

Configures the RMON 1 Alarm group.

### Format

```
rmon alarm index <index-number> variable <string> [interval <seconds>]
[falling-event-index <num>] [falling-threshold <num>] [owner <string>]
[rising-event-index <num>] [rising-threshold <num>] [startup rising|falling|both]
[status enable|disable] [type absolute-value|delta-value]
```

### Mode

Configure.

### Description

The Alarm group takes periodic statistical samples and compares them with previously-configured thresholds. If a monitored variable crosses a threshold, an alarm is generated. The **rmon alarm** command sets various parameters of the RMON 1 Alarm control table.

Use the **rmon show alarm** command to display the alarm data.

### Parameters

|                                     |  |
|-------------------------------------|--|
| <b>index</b><br><index-number>      | A number that uniquely identifies an entry in the alarm table. The value must be between 1 and 65535, inclusive.   |
| <b>interval</b> <seconds>           | Specifies the sampling interval in seconds when statistical samples of variables are collected and compared to the rising and falling thresholds. The value must be between 1 and 2147483647, inclusive.   |
| <b>falling-event-index</b><br><num> | Action to be taken as defined by the row with this index in the event table when a falling threshold is crossed. The value must be between 1 and 65535, inclusive.   |
| <b>falling-threshold</b><br><num>   | Specifies that the sample's value must be less than or equal to the threshold to trigger an alarm. When the sample's value is less than or equal to this threshold, and the value at the last sampling interval was greater than this threshold, a single event is generated. The value must be between 1 and 2147483647, inclusive. |
| <b>owner</b> <string>               | Specifies the owner of the alarm resource; for example, an IP address, machine name or person's name.  |

|                                    |  |
|------------------------------------|--|
| <b>rising-event-index</b><br><num> | Action to be taken as defined by the row with this index in the event table when a rising threshold is crossed. The value must be between 1 and 65535, inclusive.  |
| <b>rising-threshold</b><br><num>   | Specifies that the sample's value must be greater than or equal to the threshold to trigger an alarm. When the sample's value is greater than or equal to this threshold, and the value at the last sampling interval was less than this threshold, a single event is generated. The value must be between 1 and 2147483647, inclusive.  |
| <b>startup</b> <keyword>           | Specifies the condition for which the alarm is to be generated. The condition can be one of the following: <div> <div><b>rising</b> Causes an alarm to be generated if the sampled variable is greater than or equal to the rising threshold.</div> <div><b>falling</b> Causes an alarm to be generated if the sampled variable is less than or equal to the falling threshold.</div> <div><b>both</b> Causes an alarm to be generated if the sampled variable is greater than or equal to the rising threshold or less than or equal to the falling threshold.</div> </div> |
| <b>status enable disable</b>       | Enables or disables this alarm.  |
| <b>type</b> <keyword>              | Specifies the method of sampling the selected variable and calculating the value to be compared against the thresholds. The sampling method can be one of the following: <div> <div><b>absolute-value</b> Monitor the absolute value over the sample interval of the variable against the threshold value.</div> <div><b>delta-value</b> Monitor the change in value over the sample interval of the variable against the threshold value.</div> </div>  |
| <b>variable</b> <string>           | Specifies the object identifier of the variable to be sampled. Only variables that resolve to an ASN.1 primitive type of INTEGER may be sampled.   |

## Restrictions

None.

## Examples

To cause an alarm event if the variable defined in alarm 10 crosses the rising threshold:

```
xp(config)# rmon alarm index 10 startup rising interval 30 variable 1.3.6.1.2.1.5.14.0 rising-threshold
40 rising-event-index 1
```

To monitor the absolute value of the variable against a threshold value:

```
xp(config)# rmon alarm index 10 type absolute-value startup rising interval 30 variable  
1.3.6.1.2.1.5.14.0 rising-threshold 40 rising-event-index 1
```

To specify Mike as the owner of alarm 10:

```
xp(config)# rmon alarm index 10 owner Mike type absolute-value startup rising interval 30 variable  
1.3.6.1.2.1.5.14.0 rising-threshold 40 rising-event-index 1
```

To specify a 5-second interval on alarm 10:

```
xp(config)# rmon alarm index 10 interval 5 type absolute-value startup rising interval 30 variable  
1.3.6.1.2.1.5.14.0 rising-threshold 40 rising-event-index 1
```

To specify the rising threshold at 10 on alarm 10:

```
xp(config)# rmon alarm index 10 rising-threshold 10 type delta-value startup rising interval 30  
variable 1.3.6.1.2.1.5.14.0 rising-event-index 1
```

# rmon apply cli-filters

## Purpose

Apply a specific CLI RMON filter.

## Format

**rmon apply cli-filters** *<filter id>*

## Mode

Enable.

## Description

The **rmon apply cli-filters** command applies a specific CLI RMON filter to the current Telnet or Console session. This enables different users to select the different CLI filters which you should define using the **rmon set cli-filter** command.

Use the **rmon show cli-filters** command to see the RMON CLI filters that have been defined on the X-Pedition router. Use the **rmon clear cli-filter** command to clear the applied filter.

## Parameter

---

|                          |   |
|--------------------------|---|
| <i>&lt;filter id&gt;</i> | Is a number between 1 and 65535 that identifies the filter ID to apply. |
|--------------------------|---|

---

## Restrictions

None.

## Example

To apply filter ID 2:

```
xp> rmon apply cli-filters 2
```

To see a list of CLI RMON filters:

```
xp> rmon show cli-filters
RMON CLI Filters
Id  Filter
--  -----
1   (inpks >= 0)
2   (inpks >= 0 and outoctets >= 0)
3   srcmac 222222222222 and (outoctets >= 0)
You have selected a filter: (inpks >= 0)
```



# rmon capture

## Purpose

Configures the RMON 1 Packet Capture group.

## Format

```
rmon capture index <index-number> channel-index <number> [full-action lock|wrap]
[slice-size <number>] [download-slice-size <number>] [download-offset <number>]
[max-octets <number>] [owner <string>] [status enable|disable]
```

## Mode

Configure.

## Description

The Packet Capture group allows packets to be captured after they have flowed through a channel. The **rmon capture** command sets various parameters of the RMON 1 Packet Capture table.

Use the **rmon show packet-capture** command to display the Packet Capture table.

**Note:** **Rmon capture** cannot capture bad Jumbo Frames, Runt Packets, or CRC packets. This is due to a Hardware limitation.

## Parameters

|                                     |   |             |   |             |  |
|-------------------------------------|---|-------------|---|-------------|--|
| <b>index</b> <index-number>         | A number between 1 and 65535 that uniquely identifies a row in the Packet Capture table.  |             |   |             |  |
| <b>channel-index</b> <number>       | A number between 1 and 65535 that identifies the channel that is the source of packets. The default is 0.   |             |   |             |  |
| <b>full-action lock wrap</b>        | Specifies the action of the buffer when it reaches the full status: <table> <tr> <td><b>lock</b></td><td>Stop capturing packets when the buffer reaches the full status.</td></tr> <tr> <td><b>wrap</b></td><td>Wrap around when the buffer reaches the full status.</td></tr> </table> | <b>lock</b> | Stop capturing packets when the buffer reaches the full status. | <b>wrap</b> | Wrap around when the buffer reaches the full status. |
| <b>lock</b>                         | Stop capturing packets when the buffer reaches the full status.   |             |   |             |  |
| <b>wrap</b>                         | Wrap around when the buffer reaches the full status.  |             |   |             |  |
| <b>slice-size</b> <number>          | A number between 0 and 2147483647 that is the maximum number of octets that will be saved in this capture buffer. The default is 100.   |             |   |             |  |
| <b>download-slice-size</b> <number> | A number between 0 and 2147483647 that is the maximum number of octets that will be returned in an SNMP retrieval. The default is 100.  |             |   |             |  |
| <b>download-offset</b> <number>     | The offset of the first octet number (between 0 and 2147483647) of each packet that will be returned in an SNMP retrieval. The default is 0.  |             |   |             |  |

|                               |  |
|-------------------------------|--|
| <b>max-octets</b><br><number> | The maximum number of octets (between 0 and 2147483647) to use to hold captured packets and their control information. The default is 1.<br><br><b>Note:</b> The <b>max-octets</b> default value allows packet capture to continue indefinitely until all available RMON memory resources are exhausted. If these resources exhaust, RMON features will be disabled. |
| <b>owner</b> <string>         | Specifies the owner of the event; for example, an IP address, machine name or person's name.   |
| <b>status enable disable</b>  | Enables or disables this channel. The default is enable.   |

## Restrictions

Packet capture using RMON uses considerable CPU cycles. For best results, enable packet capture when the CPU is not busy running other important tasks and CPU utilization is low.

## Example

To create an entry in the Packet Capture table:

```
xp(config)# rmon capture index 20 channel-index 1 full-action wrap
```

# rmon channel

## Purpose

Configures the RMON 1 Filter Channel group.

## Format

```
rmon channel index <index-number> port <port> [accept-type matched|failed]
[data-control on|off] [turn-on-event-index <number>] [turn-off-event-index <number>]
[event-index <number>] [channel-status ready|always-ready] [description <string>]
[owner <string>] [status enable|disable]
```

## Mode

Configure.

## Description

The Filter Channel group must be configured in order to configure the Filter group. The **rmon channel** command sets various parameters of the RMON 1 Filter Channel table. After a channel row has been created, a filter must be defined with the **rmon filter** command.

Use the **rmon show channels** command to display all the channels configured on the X-Pedition router.

## Parameters

|   |  |
|---|--|
| <b>index</b><br><index-number>              | Is a number between 1 and 65535 that uniquely identifies a row in the Filter Channel table.  |
| <b>port</b> <port>                          | Identifies the port from which data is collected.  |
| <b>accept-type</b><br><b>matched failed</b> | Specifies the action of the filters associated with this channel: <div> <div><b>matched</b></div> <div>Packets will be accepted if they are accepted by both the packet data and packet status matches of an associated filter.</div> <div><b>failed</b></div> <div>Packets will be accepted only if they fail either the packet data match or the packet status match of each of the associated filters.</div> </div> |
| <b>data-control</b> on off                  | Specifies the flow control of the data: <div> <div><b>on</b></div> <div>Implies data, status, and events flow through this channel.</div> <div><b>off</b></div> <div>Implies data, status, and events will not flow through this channel.</div> </div>   |

|  |   |
|--|---|
| <b>turn-on-event-index</b><br><number>             | A number between 0 and 65535 that identifies the event configured to turn the associated data control from off to on.                             |
| <b>turn-off-event-index</b><br><number>            | A number between 0 and 65535 that identifies the event configured to turn the associated data control from on to off.                             |
| <b>event-index</b><br><number>                     | A number between 0 and 65535 that identifies the event configured to be generated when the associated data control is on and a packet is matched. |
| <b>channel-status</b><br><b>ready always-ready</b> | Specifies the status:<br><br><b>ready</b> A single event is generated.<br><br><b>always-ready</b> Allows events to be generated at will.          |
| <b>description</b> <string>                        | Describes this channel in a maximum of 127 bytes.   |
| <b>owner</b> <string>                              | Specifies the owner of packet capture; for example, an IP address, machine name or person's name.   |
| <b>status</b> <b>enable disable</b>                | Enables or disables this channel. The default is <b>enable</b> .  |

## Restrictions

None.

## Example

To create an entry in the Filter Channel table:

```
xp(config)# rmon channel index 25 port et.1.3 accept-type matched data-control on turn-on-event-  
index 30 turn-off-event-index 55 event-index 60 channel-status ready
```

# **rmon clear cli-filter**

## **Purpose**

Clear the currently-selected CLI RMON filter.

## **Format**

**rmon clear cli-filter**

## **Mode**

Enable.

## **Description**

The **rmon clear cli-filter** command clears the CLI RMON filter that was applied with the **rmon apply cli-filters** command.

## **Parameters**

None.

## **Restrictions**

None.

# **rmon enable**

## **Purpose**

Enables RMON.

## **Format**

**rmon enable**

## **Mode**

Configure.

## **Description**

When the X-Pedition router is booted, RMON is off by default. The **rmon enable** command turns RMON on. At least one of the Lite, Standard, or Professional RMON groups must be configured first before you can turn on RMON. Use the **rmon set** command to configure the Lite, Standard, or Professional RMON groups.

To disable RMON, the **rmon enable** command must be negated. This frees up all resources associated with RMON, including any memory allocated to RMON.

## **Parameters**

None.

## **Restrictions**

If the SNMP agent is disabled, RMON cannot be enabled. If RMON is enabled and the SNMP agent is disabled, then RMON will be turned off.

## rmon etherstats

### Purpose

Configures the RMON 1 Ethernet Statistics (Etherstats) group.

### Format

**rmon etherstats index** *<index-number>* **port** *<port>* [**owner** *<string>*] [**status enable|disable**]

### Mode

Configure.

### Description

The Etherstats group contains statistics for X-Pedition ports. The **rmon etherstats** command sets various parameters of the RMON 1 Etherstats control table. If default tables were turned on for the Lite group, a entry is created in the Etherstats control table for each available port.

Use the **rmon show etherstats** command to display the Etherstats data.

### Parameters

|   |  |
|---|--|
| <b>index</b><br><i>&lt;index-number&gt;</i> | A number between 1 and 65535 that uniquely identifies a row in the Etherstats control table. |
| <b>port</b> <i>&lt;port&gt;</i>             | Specifies the physical port from which to collect data.                                      |
| <b>owner</b> <i>&lt;string&gt;</i>          | Specifies the owner of the event; for example, an IP address, machine name or person's name. |
| <b>status enable disable</b>                | Enables or disables this Etherstat. The default is enable.                                   |

### Restrictions

The RMON agent reports only traffic *received* on a port.

### Example

To create an entry in the Etherstats control table:

```
xp(config)# rmon etherstats index 10 port et.1.3
```

## rmon event

### Purpose

Configures the RMON 1 Event group.

### Format

```
rmon event index <index-number> type none|log|trap|both [community <string>]  
[description <string>] [owner <string>] [status enable|disable]
```

### Mode

Configure.

### Description

The Event group controls the generation and notification of events. The **rmon event** command sets various parameters of the RMON 1 Event control table.

Use the **rmon show event** command to display the event data.

### Parameters

|                                |   |
|--------------------------------|---|
| <b>index</b><br><index-number> | A number between 1 and 65535 that uniquely identifies an entry in the Event table.  |
| <b>community</b> <string>      | Specifies the SNMP community string to be sent with the trap. If an SNMP trap is to be sent, it will go to the SNMP community specified in this string. |
| <b>description</b> <string>    | Specifies a comment describing this event.  |
| <b>owner</b> <string>          | Specifies the owner of the event; for example, an IP address, machine name or person's name.  |
| <b>status</b> enable disable   | Enables or disables this event. The default is enable.  |



| <b>type</b><br><b>none log trap both</b> | Specifies what action to be taken when the event occurs. The action can be one of the following:                 |
|--|--|
| <b>none</b>                              | Causes no notification to be sent for the event.   |
| <b>log</b>                               | Causes an entry for the event to be made in the log table for each event.  |
| <b>trap</b>                              | Causes an SNMP trap to be sent to one or more management stations for the event.                                 |
| <b>both</b>                              | Causes both an entry to be made in the log table and an SNMP trap to be sent to one or more management stations. |

## Restrictions

None.

## Examples

To set the event community string to public:

```
xp(config)# rmon event index 10 community public
```

To add the description “num-pkts” to event 10:

```
xp(config)# rmon event index 10 description num-pkts
```

To specify Ed as the owner of event 10:

```
xp(config)# rmon event index 10 owner Ed
```

To send an SNMP trap when event 10 is triggered:

```
xp(config)# rmon event index 10 type trap
```

# rmon filter

## Purpose

Configures the RMON 1 Filter group.

## Format

```
rmon filter index <index-number> channel-index <number> [data-offset <number>]  
[data <string>] [data-mask <string>] [data-not-mask <string>] [pkt-status <number>]  
[status-mask <number>] [status-not-mask <number>] [owner <string>] [status enable|disable]
```

## Mode

Configure.

## Description

The Filter group allows packets to be matched on certain criteria. The **rmon filter** command sets various parameters of the RMON 1 Filter table. To configure the Filter group, the Filter Channel group must first be configured with the **rmon channel** command.

Use the **rmon show filters** command to display the filters defined on the X-Pedition router.

## Parameters

|                                  |  |
|----------------------------------|--|
| <b>index</b><br><index-number>   | A number between 1 and 65535 that uniquely identifies a row in the Filter table.   |
| <b>channel-index</b><br><number> | A number between 1 and 65535 that identifies the channel of which this filter is a part.   |
| <b>data-offset</b><br><number>   | A number between 0 and 2147483647 that is the offset from the beginning of each packet where a match of packet data will be attempted. |
| <b>data</b> <string>             | A string of up to 512 characters that is the data that is to be matched with the input packet.   |
| <b>data-mask</b> <string>        | A string of up to 512 characters that is the mask that is applied to the match process.  |
| <b>data-not-mask</b><br><string> | A string of up to 512 characters that is the inversion mask that is applied to the match process.                                      |
| <b>pkt-status</b> <number>       | A number between 0 and 2147483647 that is the status that is to be matched with the input packet.                                      |
| <b>status-mask</b><br><number>   | A number between 0 and 2147483647 that is the mask that is applied to the status match process.  |

|                                    |   |
|------------------------------------|---|
| <b>status-not-mask</b><br><number> | A number between 0 and 2147483647 that is the inversion mask that is applied to the status match process. |
| <b>owner</b> <string>              | Specifies the owner of the event; for example, an IP address, machine name or person's name.              |
| <b>status enable disable</b>       | Enables or disables this channel. The default is enable.  |

## Restrictions

None.

## Example

To create an entry in the Filter table:

```
xp(config)# rmon filter index 25 channel-index 35 data kgreen
```

# rmon history

## Purpose

Configures the RMON 1 History group.

## Format

```
rmon history index <index-number> port <port> [interval <seconds>] [owner <string>]  
[samples <num>] [status enable|disable]
```

## Mode

Configure.

## Description

The RMON History group periodically records samples of variables and stores them for later retrieval. You use the **rmon history** command to specify the X-Pedition port to collect data from, the number of samples, the sampling interval, and the owner. If default tables were turned on for the Lite group, an entry is created in the History control table for each available port.

Use the **rmon show history** command to display the history data.

## Parameters

|                              |   |
|------------------------------|---|
| <b>index</b> <index-number>  | A number between 1 and 65535 that uniquely identifies an entry in the History table.  |
| <b>interval</b> <seconds>    | Specifies the sampling interval in seconds. This value must be between 1 and 3600, inclusive. The default value is 1800.                              |
| <b>owner</b> <string>        | Specifies the owner of the history resource; for example, an IP address, machine name or person's name.   |
| <b>port</b> <port>           | Specifies the port from which to collect data.  |
| <b>samples</b> <num>         | Specifies the number of samples to be collected before wrapping counters. This value must be between 1 and 65535, inclusive. The default value is 50. |
| <b>status enable disable</b> | Enables or disables this history control row.   |

## Restrictions

None.

## Example

To specify that port et.3.1 collect 60 samples at an interval of 30 seconds:

```
xp(config)# rmon history index 10 port et.3.1 samples 60 interval 30
```

# rmon hl-host

## Purpose

Configures the RMON 2 Application Layer and Network Layer Host groups.

## Format

```
rmon hl-host index <index-number> port <port> nl-max-entries <number>  
al-max-entries <number> [owner <string>] [status enable|disable]
```

## Mode

Configure.

## Description

The **rmon hl-host** command sets various parameters of the RMON 2 Application Layer and Network Layer Host groups. The Application Layer Host group monitors traffic from the network layer up to the application layer for any protocol communication defined in the protocol directory. The Network Layer Host group monitors traffic at the network layer for any protocol defined in the protocol directory.

Configuration of the Application Layer/Network Layer Host table involves configuring only one control row in the Application Layer Host control table. This table, when configured, captures both application layer and network layer host data. If the default tables were turned on for the Professional group, an entry is created in the Application Layer Host control table for each available port.

Use the **rmon show al-host** command to display the Application Layer Host table. Use the **rmon show nl-host** command to display the Network Layer Host table.

## Parameters

|                                |  |
|--------------------------------|--|
| <b>index</b><br><index-number> | A number between 1 and 65535 that uniquely identifies a row in the application layer host control table. |
| <port>                         | Specifies the port from which to collect data.   |
| <b>nl-max-entries</b>          | Specifies the maximum number of network layer entries. The default is 1.                                 |
| <b>al-max-entries</b>          | Specifies the maximum number of application layer entries. The default is 1.                             |
| <b>owner</b> <string>          | Specifies the owner of the event; for example, an IP address, machine name or person's name.             |
| <b>status enable disable</b>   | Enables or disables this matrix. The default is enable.  |

## Restrictions

None.

## Example

To create an entry in the Application Layer Host control table:

```
xp(config)# rmon hl-host index 20 port et.1.3
```

# rmon hl-matrix

## Purpose

Configures the RMON 2 Application Layer Matrix and Network Layer Matrix groups.

## Format

```
rmon hl-matrix index <index-number> port <port> nl-max-entries <number>  
al-max-entries <number> [owner <string>] [status enable|disable]
```

## Mode

Configure.

## Description

The **rmon hl-matrix** command sets various parameters of the RMON 2 Application Layer Matrix and Network Layer Matrix groups. The Application Layer Matrix group monitors traffic from the network layer up to the application layer for any protocol communication defined in the protocol directory. The Network Layer Matrix group monitors traffic at the network layer for any protocol defined in the protocol directory.

Configuration of the Application Layer/Network Layer Matrix table involves configuring only one control row in the Application Layer Matrix control table. When configured, this table captures both application layer and network layer matrix data. If the default tables were turned on for the Professional group, an entry is created in the Application Layer Matrix control table for each available port.

Use the **rmon show al-matrix** command to display the Application Layer Matrix table. Use the **rmon show nl-matrix** command to display the Network Layer Matrix table.

## Parameters

|                                   |  |
|-----------------------------------|--|
| <b>index</b><br><index-number>    | A number between 1 and 65535 that uniquely identifies a row in the application layer matrix control table. |
| <b>port</b> <port>                | Specifies the port from which to collect data.   |
| <b>nl-max-entries</b><br><number> | Specifies the maximum number of network layer entries. The default is 1.                                   |
| <b>al-max-entries</b><br><number> | Specifies the maximum number of application layer entries. The default is 1.                               |
| <b>owner</b> <string>             | Specifies the owner of the event; for example, an IP address, machine name or person's name.               |



---

|                              |   |
|------------------------------|---|
| <b>status enable disable</b> | Enables or disables this matrix. The default is enable. |
|------------------------------|---|

---

## Restrictions

None.

## Example

To create an entry in the Application Layer Matrix control table:

```
xp(config)# rmon hl-matrix index 20 port et.1.3
```

# rmon host

## Purpose

Configures the RMON 1 Host group.

## Format

**rmon host index** <index-number> **port** <port> [**owner** <string>] [**status enable|disable**]

## Mode

Configure.

## Description

The RMON 1 Host group captures L2 information from hosts coming in on a particular port. The **rmon host** command sets various parameters of the Host group. If default tables were turned on for the standard group, an entry is created in the Host control table for each available port.

Use the **rmon show hosts** command to display the host data and logs.

## Parameters

|                                |  |
|--------------------------------|--|
| <b>index</b><br><index-number> | A number between 1 and 65535 that uniquely identifies a row in the Host table.               |
| <b>port</b> <port>             | Specifies the physical port from which to collect data.                                      |
| <b>owner</b> <string>          | Specifies the owner of the event; for example, an IP address, machine name or person's name. |
| <b>status enable disable</b>   | Enables or disables this host. The default is enable.  |

## Restrictions

None.

## Example

To create an entry in the Host control table:

```
xp(config)# rmon hosts index 20 port et.1.3
```

# rmon host-top-n

## Purpose

Configures the RMON 1 HostTopN group.

## Format

**rmon host-top-n index** <index-number> **host-index** <number> [**base** <statistics>]  
[**duration** <time>] [**size** <size>] [**owner** <string>] [**status enable|disable**]

## Mode

Configure.

## Description

The HostTopN group displays the top n number of hosts, sorted by a specified statistic. The **rmon host-top-n** command sets various parameters of the RMON 1 HostTopN control table. The HostTopN group depends upon the Host group and the host-index specified in the HostTopN control table must correspond to a pre-defined host index in the Host control table.

Use the **rmon show host-top-n** command to display the control table row.

Note that Host Top N report runs once. To run the reports again via the CLI, the control row must be disabled and then enabled. If the report has already been run, the Time Remaining field is set to zero. Otherwise, the Time Remaining field will be decremented until the report is run.

## Parameters

|                                |   |
|--------------------------------|---|
| <b>index</b><br><index-number> | A number between 1 and 65535 that uniquely identifies a row in the Host Top N table.        |
| <number>                       | A number between 1 and 65535 that is the index into the host table identified by hostIndex. |

|                                    |   |
|------------------------------------|---|
| <i>&lt;statistics&gt;</i>          | Specifies the type of statistic from which to collect data. Specify one of the following keywords:<br><br><b>in-packets</b> Gather top statistics according to In-Packets.<br><b>out-packets</b> Gather top statistics according to Out-Packets.<br><b>in-octets</b> Gather top statistics according to In-Octets.<br><b>out-octets</b> Gather top statistics according to Out-Octets.<br><b>out-errors</b> Gather top statistics according to Out-Errors.<br><br><b>Note:</b> The <b>out-errors</b> option is no longer valid—hardware restrictions prevent the host-top-n table from seeing out-errors.<br><br><b>out-broadcastPkts</b> Gather top statistics according to Out-BroadcastPkts.<br><b>out-multicastPkts</b> Gather top statistics according to Out-MulticastPkts. |
| <i>&lt;time&gt;</i>                | A number between 1 and 2147483647 that is the duration, in seconds, between reports. The default is 0.  |
| <i>&lt;size&gt;</i>                | A number between 1 and 2147483647 that is the maximum number of hosts to include in the table. The default is 10.   |
| <b>owner</b> <i>&lt;string&gt;</i> | Specifies the owner of the event; for example, an IP address, machine name or person's name.  |
| <b>status enable disable</b>       | Enables or disables this hostTopN. The default is enable.   |

## Restrictions

None.

## Example

To create an entry in the HostTopN control table:

|  |
|--|
| xp(config)# rmon host-top-n index 25 host-index 55 base in-packets duration 60 size 24 |
|--|

# rmon matrix

## Purpose

Configures the RMON 1 Matrix group.

## Format

**rmon matrix index** *<index-number>* [**port** *<port>*] [**owner** *<string>*] [**status enable|disable**]

## Mode

Configure.

## Description

The Matrix group captures L2 traffic on a particular port between two hosts (a source MAC and destination MAC address). The **rmon matrix** command sets various parameters of the RMON 1 Matrix control table. If default tables were turned on for the Standard group, an entry is created in the Matrix control table for each available port.

**Note:** By default, ports on the X-Pedition router operate in address-bridging mode. The port must be enabled in *flow-bridging* mode in order for layer 2 matrix information to be captured.

Use the **rmon show matrix** command to display the matrix group and logs.

## Parameters

|   |  |
|---|--|
| <b>index</b><br><i>&lt;index-number&gt;</i> | A number between 1 and 65535 that uniquely identifies a row in the Matrix table.             |
| <b>port</b> <i>&lt;port&gt;</i>             | Specifies the port from which to collect data.   |
| <b>owner</b> <i>&lt;string&gt;</i>          | Specifies the owner of the event; for example, an IP address, machine name or person's name. |
| <b>status enable disable</b>                | Enables or disables this matrix. The default is <b>enable</b> .                              |

## Restrictions

None.

## Example

To create an entry in the Matrix control table:

```
xp(config)# rmon matrix index 25 port et.1.3
```

# rmon nl-matrix-top-n

## Purpose

Gathers the top n Network Layer Matrix entries.

## Format

```
rmon nl-matrix-top-n index <index-number> matrix-index <number>
ratebase packets | octets duration <number> size <number> [owner <string>]
[status enable|disable]
```

## Mode

Configure.

## Description

The **rmon nl-matrix-top-n** command gathers the top n Network Layer Matrix entries. Before you do this, you should first configure the Application Layer/Network Layer Matrix table using the **rmon hl-matrix** command.

Use the **rmon show nl-matrix-top-n** command to display the top n Network Layer Matrix entries.

## Parameters

|  |   |
|--|---|
| <b>index</b><br><index-number>           | A number between 1 and 65535 that uniquely identifies a row in the network layer matrix table.            |
| <b>matrix-index</b><br><number>          | Specifies the index into the hl-matrix table. The default is 0.   |
| <b>ratebase</b><br><b>packets octets</b> | Specifies the sorting method:<br><br><b>packets</b> Sort by packets.<br><br><b>octets</b> Sort by octets. |
| <b>duration</b> <number>                 | Specifies the duration, in seconds, between reports. The default is 0.                                    |
| <b>size</b> <number>                     | Specifies the maximum number of matrix entries to include in the report. The default is 150.              |
| <b>owner</b> <string>                    | Specifies the owner of the event; for example, an IP address, machine name or person's name.              |
| <b>status enable disable</b>             | Enables or disables this matrix. The default is enable.   |

## Restrictions

None.

## Example

To gather the top n Network Layer Matrix entries:

```
xp(config)# rmon nl-matrix-top-n index 2 matrix-index 25 ratebase all-packets duration 60 size 100
```



# rmon protocol-distribution

## Purpose

Configures the RMON 2 Protocol Distribution group.

## Format

**rmon protocol-distribution index** *<index-number>* **port** *<port>* [**owner** *<string>*]  
[**status enable|disable**]

## Mode

Configure.

## Description

The Protocol Distribution group displays the packets and octets on a protocol and port basis. The **rmon protocol-distribution** command sets various parameters of the RMON 2 Protocol Distribution control table. If default tables were turned on for the Professional group, an entry is created in the Protocol Distribution control table for each available port.

Use the **rmon show protocol-distribution** command to display the protocol distribution.

## Parameters

|   |   |
|---|---|
| <b>index</b><br><i>&lt;index-number&gt;</i> | A number between 1 and 65535 that uniquely identifies a row in the Protocol Distribution table. |
| <b>port</b> <i>&lt;port&gt;</i>             | Specifies the port from which to collect data.  |
| <b>owner</b> <i>&lt;string&gt;</i>          | Specifies the owner of the event; for example, an IP address, machine name or person's name.    |
| <b>status enable disable</b>                | Enables or disables this matrix. The default is enable.   |

## Restrictions

None.

## Example

To create an entry in the Protocol Distribution control table:

```
xp(config)# rmon protocol-distribution index 25 port et.1.3
```

## rmon set

### Purpose

Configures the Lite, Standard, or Professional RMON groups.

### Format

**rmon set lite | standard | professional default-tables yes | no**

### Mode

Configure.

### Description

You can enable various levels of support (Lite, Standard, or Professional) for RMON groups on a specified set of ports.

Lite adds support for the following RMON 1 groups:

- Ethernet statistics (Etherstats)
- History
- Alarm
- Event

Standard adds support for the following RMON 1 groups:

- Host
- HostTopN
- Matrix
- Filter
- Packet Capture

**Note:** Packet capture using RMON uses considerable CPU cycles. For best results, enable packet capture when the CPU is not busy running other important tasks and CPU utilization is low.

Professional adds support for the following RMON 2 groups:

- Protocol Directory
- Protocol Distribution
- Address Map
- Network Layer Host
- Network Layer Matrix
- Application Layer Host
- Application Layer Matrix
- User History
- Probe Configuration

A group can consist of a control table and a data table. A control table specifies the statistics to be collected. Each row in the control table specifies the entities for which data is collected, for example, physical ports. The data tables contain the statistics that are collected based on the control table information.

## Parameters

|                                       |  |              |                       |                  |                |                      |  |
|---------------------------------------|--|--------------|-----------------------|------------------|----------------|----------------------|--|
| <b>lite   standard   professional</b> | Specifies the Lite, Standard, or Professional RMON groups.   |              |                       |                  |                |                      |  |
| <b>default-tables yes</b>             | <p>Creates control tables for the following Lite, Standard, or Professional RMON groups:</p> <table> <tr> <td>Lite groups:</td><td>Etherstats<br/>History</td></tr> <tr> <td>Standard groups:</td><td>Host<br/>Matrix</td></tr> <tr> <td>Professional groups:</td><td>Protocol Distribution<br/>Address Map<br/>Application Layer/Network Layer Host<br/>Application Layer/Network Layer Matrix</td></tr> </table> <p>A row in each control table is created for each port on the X-Pedition router, with the default owner “monitor.”</p> | Lite groups: | Etherstats<br>History | Standard groups: | Host<br>Matrix | Professional groups: | Protocol Distribution<br>Address Map<br>Application Layer/Network Layer Host<br>Application Layer/Network Layer Matrix |
| Lite groups:                          | Etherstats<br>History  |              |                       |                  |                |                      |  |
| Standard groups:                      | Host<br>Matrix   |              |                       |                  |                |                      |  |
| Professional groups:                  | Protocol Distribution<br>Address Map<br>Application Layer/Network Layer Host<br>Application Layer/Network Layer Matrix   |              |                       |                  |                |                      |  |
| <b>default-tables no</b>              | Removes all control table rows with the owner “monitor”. If you wish to save a particular control table row, you must change the owner to a value other than “monitor”.  |              |                       |                  |                |                      |  |

## Restrictions

None.

## Example

To configure the RMON Lite groups and create default control tables:

```
xp(config)# rmon set lite default-tables yes
```

# rmon set cli-filter

## Purpose

Defines filters that can be applied to certain RMON groups during a CLI session.

## Format

**rmon set cli-filter** <filter-id> <parameter>

## Mode

Configure.

## Description

You can define filters that CLI users can apply to certain RMON groups. The filters you define are visible to all users that have a Telnet or Console session on the X-Pedition router. Each user has the choice of whether or not to apply a particular filter using the **rmon apply cli-filters** command.

RMON CLI filters only affect the output of the following RMON groups:

- Host
- Matrix
- Network Layer Host
- Application Layer Host
- Network Layer Matrix
- Application Layer Matrix
- Protocol Distribution

The **rmon show cli-filters** command displays the RMON CLI filters that have been defined on the X-Pedition router.

## Parameters

---

|             |   |
|-------------|---|
| <filter-id> | A number between 1 and 65535 that uniquely identifies a CLI filter. |
|-------------|---|

---

|                  |   |
|------------------|---|
| <parameter>      | Specifies the parameter on which the filter is set:   |
| <b>src-mac</b>   | Source MAC Address  |
| <b>dst-mac</b>   | Destination MAC Address   |
| <b>inpkts</b>    | In Packets  |
| <b>inoctets</b>  | In Octets   |
| <b>outpkts</b>   | out packets   |
| <b>outoctets</b> | out Octets  |
| <b>multicast</b> | Multicast packets   |
| <b>broadcast</b> | Broadcast packets   |
| <b>errors</b>    | Errors  |
|                  | The following operands can also be used:  |
| <b>and</b>       | AND   |
| <b>or</b>        | Or  |
| <b>=</b>         | Equal to  |
| <b>&lt;</b>      | Less than   |
| <b>&lt;=</b>     | Less than or equal to   |
| <b>&gt;</b>      | Greater than  |
| <b>&gt;=</b>     | Greater than or equal to  |
| <b>!=</b>        | Not equal to  |
| <b>(</b>         | Left bracket  |
| <b>)</b>         | Right Bracket   |
|                  | <b>src-mac</b> and <b>dst-mac</b> can be specified once and the other parameters can be specified multiple times. |

---

## Restrictions

None.

## Example

To configure an RMON CLI filter on a source MAC address of 123456:123456 and on input packets greater than 1000 and error packets greater than 10 or out packets less than 10000, use the following command:

```
xp(config)# rmon set cli-filter 3 src-mac 123456:123456 and ((inpmts > 1000 and errors > 10) or  
(outpmts < 10000))
```

# rmon set memory

## Purpose

Increases the amount of memory allocated to RMON.

## Format

**rmon set memory** <number>

## Mode

Enable.

## Description

RMON allocates memory depending on the number of ports enabled for RMON, the groups that have been configured (Lite, Standard, or Professional) and whether or not default tables have been turned on or off. You can dynamically allocate additional memory to RMON, if needed.

Later, if this additional memory is no longer required, you can reduce the allocation; this change will not take effect until RMON is restarted. This is because memory cannot be freed while RMON is still using it. If the amount of memory specified is less than what RMON has currently allocated, a warning message is displayed and the action is ignored.

Use the **rmon show status** command to display the amount of memory currently allocated to RMON.

## Parameters

|              |   |
|--------------|---|
| <number>     | Specifies the total amount of memory, in Mbytes, to be allocated to RMON. The value can be between 2 and 96.    |
| <b>Note:</b> | The number specified is the total number of Mbytes of memory to be allocated; it is not an increment of memory. |

## Restrictions

None.



## Example

To show the amount of memory allocated to RMON:

```
xp# rmon show status
```

To increase the amount of memory allocated to RMON:

```
xp# rmon set memory 32
```

## rmon set ports

### Purpose

Enables RMON on one or more ports.

### Format

**rmon set ports** *<port list>* | **allports**

### Mode

Configure.

### Description

Since RMON uses many system resources, RMON can be enabled on a set of ports. Ports can be dynamically added and removed from the port list. For example, if default tables are turned on for the Lite group and port et.2.1 is then added to the port list, an entry for port et.2.1 is automatically created in the Etherstats and History control tables.

### Parameters

|                          |  |
|--------------------------|--|
| <i>&lt;port list&gt;</i> | Specifies the port(s) on which RMON is enabled.      |
| <b>allports</b>          | Enables RMON for all ports on the X-Pedition router. |

### Restrictions

None.

### Example

To enable RMON on all ports on the X-Pedition router:

```
xp(config)# rmon set ports allports
```

# rmon set protocol-directory

## Purpose

Specifies the protocol encapsulations that are managed with the Protocol Directory group.

## Format

```
rmon set protocol-directory <protocol> | all-protocols [address-map on|off|na] [host on|off|na]  
[matrix on|off|na]
```

## Mode

Configure.

## Description

The **rmon set protocol-directory** command defines the protocols that are managed with RMON on the X-Pedition router.

## Parameters

|   |   |
|---|---|
| <b>&lt;protocol&gt;  <br/>all-protocols</b> | Specifies the protocol encapsulations that are managed with the Protocol Directory group on the X-Pedition router. (See <a href="#">Appendix A</a> for a list of protocols supported on the X-Pedition router.) Specify <b>all-protocols</b> to manage all protocols that are supported on the X-Pedition router. |
| <b>address-map<br/>on off na</b>            | Configures support for the Address Map group for the specified protocol(s).   |
| <b>host on off na</b>                       | Configures support for the Host group for the specified protocol(s).  |
| <b>matrix on off na</b>                     | Configures support for the Matrix group for the specified protocol(s).  |

## Restrictions

The Protocol Directory group is part of the RMON Professional group. To use the **rmon set protocol-directory** command you must enable the RMON Professional group with the **rmon set professional** command.

## Example

To configure a protocol encapsulation for the Protocol Directory group:

```
xp(config)# rmon set protocol-directory all-protocols address-map on host on matrix on
```

# rmon show address-map-logs

## Purpose

Displays MAC address to network address bindings for each protocol.

## Format

**rmon show address-map-logs** *<port-list>* | **all-ports**

## Mode

Enable.

## Description

The **rmon show address-map-logs** command displays entries in the RMON 2 Address Map log table. Entries in this table are created automatically when default tables are turned on for the Professional group. You can show address bindings for specific ports or for all ports.

## Parameters

|                          |  |
|--------------------------|--|
| <i>&lt;port-list&gt;</i> | Specifies the port(s) for which you want to display MAC-network address information. |
| <b>all-ports</b>         | Shows information for all ports.   |

## Restrictions

This command is only available if you have configured the Professional group and Address Map control table entries exist for the specified port.

## Example

To display the address map log table for all ports:

| xp# <b>rmon show address-map-logs all-ports</b> |               |              |               |
|---|---------------|--------------|---------------|
| RMON II Address Map Control Table               |               |              |               |
| ❶   | ❷             | ❸            | ❹             |
| Port  | macAdd        | nlAdd        | Protocol      |
| ----  | -----         | -----        | -----         |
| et.5.1  | 00001D:CBA3FD | 192.100.81.1 | ether2.ip-v4  |
| et.5.1  | 00001D:CBA3FD | 192.100.81.1 | *ether2.ip-v4 |
| et.5.1  | 00001D:CBA3FD | 10.60.89.88  | ether2.ip-v4  |
| et.5.1  | 00001D:CBA3FD | 10.60.89.88  | *ether2.ip-v4 |
| et.5.5  | 00001D:CBA3FD | 192.100.81.3 | ether2.ip-v4  |
| et.5.5  | 00001D:CBA3FD | 192.100.81.3 | *ether2.ip-v4 |
| et.5.5  | 080020:835CAA | 10.60.89.88  | ether2.ip-v4  |
| et.5.5  | 080020:835CAA | 10.60.89.88  | *ether2.ip-v4 |
| et.5.1  | 0080C8:C172A6 | 192.100.81.3 | ether2.ip-v4  |
| et.5.1  | 0080C8:C172A6 | 192.100.81.3 | *ether2.ip-v4 |

### Legend:

1. The port on which the MAC address-network address binding was discovered.
2. The MAC address for the binding.
3. The network layer address for the binding.
4. The protocol, as specified in the RMON Protocol Directory for the X-Pedition router.

# **rmon show address-map-control**

## **Purpose**

Displays the address map control table.

## **Format**

**rmon show address-map-control**

## **Mode**

Enable.

## **Description**

The **rmon show address-map-control** command displays the collection of network layer addresses to physical addresses to interface mappings.

**Note:** This is not like the typical RMON controlTable and dataTable in which each entry creates its own datatable. Each entry in this table enables the discovery of addresses on a new interface and the placement of address mappings into the central addressMapTable.

Implementations are encouraged to add an entry per monitored interface upon initialization so that a default collection of address mappings is available.

## **Parameters**

None.

## **Restrictions**

None.

# rmon show al-host

## Purpose

Shows application layer traffic.

## Format

**rmon show al-host** <port-list> | **all-ports** [summary]

## Mode

Enable.

## Description

The **rmon show al-host** command shows entries in the RMON 2 Application Layer Host table for one or more ports. Entries in this table are created automatically when default tables are turned on for the Professional group.

If CLI filters have been applied, they will take effect when the Application Layer Host table is displayed. This command shows control rows and their corresponding logs only if there are logs. A control row with no data will not appear in the report.

The Application Layer host group is configured with the **rmon hl-host** command.

## Parameters

|                               |  |
|-------------------------------|--|
| <port-list>  <b>all-ports</b> | The port(s) for which you want to display application layer traffic information. Use <b>all-ports</b> to show traffic information for all the ports. |
| [summary]                     | Displays control row summary information only.   |

## Restrictions

This command is only available if you have configured the Professional group and control table entries exist for the specified port.



## Example

To show Application Layer Host tables on all ports:

|  |        |          |         |           |                          |
|--|--------|----------|---------|-----------|--------------------------|
| xp# <b>rmon show al-host all-ports</b>                             |        |          |         |           |                          |
| RMON II Application Layer Host Table                               |        |          |         |           |                          |
| Index: 500, Port: et.5.1, Inserts: 9, Deletes: 0, Owner: monitor ❶ |        |          |         |           |                          |
| ❷  | ❸      | ❹        | ❺       | ❻         | ❼                        |
| Address  | InPkts | InOctets | OutPkts | OutOctets | Protocol                 |
| -----  | -----  | -----    | -----   | -----     | -----                    |
| 10.60.89.88  | 1080   | 879418   | 2       | 164       | *ether2.ip-v4            |
| 10.60.89.88  | 1080   | 879418   | 2       | 164       | *ether2.ip-v4.tcp        |
| 10.60.89.88  | 1080   | 879418   | 2       | 164       | *ether2.ip-v4.tcp.telnet |
| 192.100.81.1   | 1      | 100      | 1       | 100       | *ether2.ip-v4            |
| 192.100.81.1   | 1      | 100      | 1       | 100       | *ether2.ip-v4.icmp       |
| 192.100.81.3   | 3      | 264      | 1081    | 879518    | *ether2.ip-v4            |
| 192.100.81.3   | 1      | 100      | 1       | 100       | *ether2.ip-v4.icmp       |
| 192.100.81.3   | 2      | 164      | 1080    | 879418    | *ether2.ip-v4.tcp        |
| 192.100.81.3   | 2      | 164      | 1080    | 879418    | *ether2.ip-v4.tcp.telnet |
| Index: 504, Port: et.5.5, Inserts: 6, Deletes: 0, Owner: monitor   |        |          |         |           |                          |
| Address  | InPkts | InOctets | OutPkts | OutOctets | Protocol                 |
| -----  | -----  | -----    | -----   | -----     | -----                    |
| 10.60.89.88  | 3      | 246      | 1141    | 92563     | *ether2.ip-v4            |
| 10.60.89.88  | 3      | 246      | 1141    | 92563     | *ether2.ip-v4.tcp        |
| 10.60.89.88  | 3      | 246      | 1141    | 92563     | *ether2.ip-v4.tcp.telnet |
| 192.100.81.3   | 1141   | 92563    | 3       | 246       | *ether2.ip-v4            |
| 192.100.81.3   | 1141   | 92563    | 3       | 246       | *ether2.ip-v4.tcp        |
| 192.100.81.3   | 1141   | 92563    | 3       | 246       | *ether2.ip-v4.tcp.telnet |

### Legend:

1. The control table entry for this port:

Index: uniquely identifies the entry in the control table.

Port: port name.

Inserts: number of Application Layer Host table entries for this port.

Deletes: number of Application Layer Host table entries deleted for this port.

Owner: default owner "monitor."

2. Network address discovered on the port.
3. Number of packets transmitted without errors to the network address for the protocol.
4. Number of octets transmitted without errors to the network address for the protocol.
5. Number of packets transmitted without errors from the network address for the protocol.
6. Number of octets transmitted without errors from the network address for the protocol.
7. The protocol, as specified in the RMON Protocol Directory for the X-Pedition router. Note that this shows the destination socket, as well as application/protocol information.

# rmon show al-matrix

## Purpose

Shows application layer traffic between source and destination addresses.

## Format

**rmon show al-matrix** *<port-list>***|all-ports** [**order-by srcdst|dstsrc**] [**summary**]

## Mode

Enable.

## Description

The **rmon show al-matrix** command shows entries in the RMON 2 Application Layer Matrix table for one or more ports. Entries in this table are created automatically when default tables are turned on for the Professional group.

If CLI filters have been applied, they will take effect when this table is displayed. The control rows and their corresponding logs are displayed only if there are logs. A control row with no data will not appear in the report.

## Parameters

|  |  |
|--|--|
| <i>&lt;port-list&gt;</i> <b> all-ports</b> | The port(s) for which you want to display application layer traffic information. Use <b>all-ports</b> to show traffic information for all the ports. |
| <b>srcdst</b>                              | Orders the logs by source address, then destination address (default).   |
| <b>dstsrc</b>                              | Orders the logs by destination address, then source address.   |
| <b>summary</b>                             | Displays control row summary information only.   |

## Restrictions

This command is only available if you have configured the Professional group and control table entries exist for the specified port.

## Example

To show the Application Layer Matrix table for all ports:.

|   |              |         |        |                          |
|---|--------------|---------|--------|--------------------------|
| xp# <b>rmon show al-matrix all-ports</b>                            |              |         |        |                          |
| RMON II Application Layer Host Table                                |              |         |        |                          |
| Index: 500, Port: et.5.1, Inserts: 10, Deletes: 0, Owner: monitor ❶ |              |         |        |                          |
| ❷   | ❸            | ❹       | ❺      | ❻                        |
| SrcAddr   | DstAddr      | Packets | Octets | Protocol                 |
| -----   | -----        | -----   | -----  | -----                    |
| 10.60.89.88   | 192.100.81.3 | 2       | 164    | *ether2.ip-v4            |
| 10.60.89.88   | 192.100.81.3 | 2       | 164    | *ether2.ip-v4.tcp        |
| 10.60.89.88   | 192.100.81.3 | 2       | 164    | *ether2.ip-v4.tcp.telnet |
| 192.100.81.1  | 192.100.81.3 | 1       | 100    | *ether2.ip-v4            |
| 192.100.81.1  | 192.100.81.3 | 1       | 100    | *ether2.ip-v4.icmp       |
| 192.100.81.3  | 10.60.89.88  | 1181    | 972211 | *ether2.ip-v4            |
| 192.100.81.3  | 10.60.89.88  | 1181    | 972211 | *ether2.ip-v4.tcp        |
| 192.100.81.3  | 10.60.89.88  | 1181    | 972211 | *ether2.ip-v4.tcp.telnet |
| 192.100.81.3  | 192.100.81.1 | 1       | 100    | *ether2.ip-v4            |
| 192.100.81.3  | 192.100.81.1 | 1       | 100    | *ether2.ip-v4.icmp       |
| Index: 504, Port: et.5.5, Inserts: 6, Deletes: 0, Owner: monitor    |              |         |        |                          |
| SrcAddr   | DstAddr      | Packets | Octets | Protocol                 |
| -----   | -----        | -----   | -----  | -----                    |
| 10.60.89.88   | 192.100.81.3 | 1242    | 100744 | *ether2.ip-v4            |
| 10.60.89.88   | 192.100.81.3 | 1242    | 100744 | *ether2.ip-v4.tcp        |
| 10.60.89.88   | 192.100.81.3 | 1242    | 100744 | *ether2.ip-v4.tcp.telnet |
| 192.100.81.3  | 10.60.89.88  | 3       | 246    | *ether2.ip-v4            |
| 192.100.81.3  | 10.60.89.88  | 3       | 246    | *ether2.ip-v4.tcp        |
| 192.100.81.3  | 10.60.89.88  | 3       | 246    | *ether2.ip-v4.tcp.telnet |

### Legend:

1. The control table entry for this port:

Index: uniquely identifies the entry in the control table.

Port: port name.

Inserts: number of application layer host table entries for this port.

Deletes: number of application layer host table entries deleted for this port.

Owner: default owner "monitor."

2. Source address.
3. Destination address.
4. Number of link layer packets transmitted from the source to the destination without errors for the protocol.
5. Number of octets transmitted from the source to the destination without errors for the protocol.
6. The protocol, as specified in the RMON Protocol Directory for the X-Pedition router.

## **rmon show al-matrix-top-n**

### **Purpose**

Reports the top *n* Application Layer Matrix entries, sorted by a specific metric.

### **Format**

**rmon show al-matrix-top-n**

### **Mode**

Enable.

### **Description**

The **rmon show al-matrix-top-n** command shows entries in the RMON 2 Application Layer Matrix Top N table.

### **Parameters**

None.

### **Restrictions**

This command is only available if you have enabled the Professional RMON group and entries exist in the Application Layer Matrix Top N table.

### **Example**

Consider the following command to gather the top *n* Application Layer Matrix entries:

```
xp(config)# rmon al-matrix-top-n index 1 matrix-index 500 ratebase all-packets duration 20 size 5
```

To show the top n entries in the Application Layer Matrix table, as specified by the previous command:

|                               |              |             |           |           |             |                          |         |         |
|-------------------------------|--------------|-------------|-----------|-----------|-------------|--------------------------|---------|---------|
| xp# rmon show al-matrix-top-n |              |             |           |           |             |                          |         |         |
| RMON II AI Matrix Table       |              |             |           |           |             |                          |         |         |
| ①                             | ②            | ③           | ④         | ⑤         | ⑥           | ⑦                        | ⑧       | ⑨       |
| Index                         | M-Index      | RateBase    | TimeRem   | Duration  | Size        | StartTime                | Reports | Owner   |
| 1                             | 500          | All-Packets | 14        | 20        | 5           | 00D 00H 50M 25S          | 1       | monitor |
| ⑩                             | ⑪            | ⑫           | ⑬         | ⑭         | ⑮           | ⑯                        |         |         |
| SrcAddr                       | DstAddr      | PktRate     | R-PktRate | OctetRate | R-OctetRate | Protocol                 |         |         |
| -----                         | -----        | -----       | -----     | -----     | -----       | -----                    |         |         |
| 192.100.81.3                  | 10.60.89.88  | 21          | 0         | 19836     | 0           | *ether2.ip-v4.tcp.telnet |         |         |
| 192.100.81.3                  | 10.60.89.88  | 21          | 0         | 19836     | 0           | *ether2.ip-v4.tcp        |         |         |
| 192.100.81.3                  | 10.60.89.88  | 21          | 0         | 19836     | 0           | *ether2.ip-v4            |         |         |
| 192.100.81.1                  | 192.100.81.3 | 0           | 0         | 0         | 0           | *ether2.ip-v4            |         |         |
| 192.100.81.3                  | 192.100.81.1 | 0           | 0         | 0         | 0           | *ether2.ip-v4            |         |         |

#### Legend:

1. Index number that identifies this entry in the Application Layer Matrix Top N control table.
2. The Application Layer Matrix table for which the top N report is shown.
3. The parameter on which the entries are sorted.
4. Number of seconds left in the report currently being collected.
5. Number of seconds that this report has collected during the last sampling interval.
6. Maximum number of matrix entries in this report.
7. The time when this report was last started.
8. The number of reports generated by this entry.
9. The entity that configured this entry.
10. Network address of the source host.
11. Network address of the destination host.
12. Number of packets from the source to the destination during the sampling interval.
13. Number of packets from the destination to the source during the sampling interval.
14. Number of octets from the source to the destination during the sampling interval.
15. Number of octets from the destination to the source during the sampling interval.
16. The protocol, as defined in the RMON Protocol Directory group on the X-Pedition router.

## **rmon show alarms**

### **Purpose**

Displays configured alarms.

### **Format**

**rmon show alarms**

### **Mode**

Enable.

### **Description**

The **rmon show alarms** command displays the RMON Alarm table.

### **Parameters**

None.

### **Restrictions**

This command is only available if you have configured the Lite group.

### **Example**

To show configured RMON alarms:

```
xp# rmon show alarm
```

# **rmon show channels**

## **Purpose**

Shows the contents of the Filter Channel table.

## **Format**

**rmon show channels**

## **Mode**

Enable.

## **Description**

The **rmon show channels** command displays the contents of the Filter Channel table.

## **Parameters**

None.

## **Restrictions**

This command is only available if you have configured the Standard group.

## **Example**

To show the contents of the Filter Channel table:

```
xp# rmon show channels
RMON 1 Channel Table
No channels defined
```

## rmon show cli-filters

### Purpose

Displays previously-configured RMON CLI filters.

### Format

**rmon show cli-filters**

### Mode

User and Enable.

### Description

The **rmon show cli-filters** command displays the RMON CLI filters that have been defined for use on the X-Pedition router. Use the **rmon apply cli-filters** command to apply a filter to your current Telnet or Console session.

### Parameters

None.

### Restrictions

None.

### Example

To show RMON CLI filters that are defined on the X-Pedition router:

```
xp> rmon show cli-filters
RMON CLI Filters

 ❶ ❷
Id  Filter
--  -----
 1  (inpks >= 0)
 2  (inpks >= 0 and outoctets >= 0)
 3  srcmac 222222222222 and (outoctets >= 0)
You have selected a filter: (inpks >= 0) ❸
```



**Legend:**

1. The filter ID. You use this value to apply a filter with the **rmon apply cli-filters** command.
2. The filter parameters that were specified with the **rmon set cli-filter** command.
3. This shows the parameters of the filter that is currently applied to your Telnet or Console session.

## **rmon show etherstats**

### **Purpose**

Displays Ethernet statistics for one or more ports.

### **Format**

**rmon show etherstats** *<port-list>* | **all-ports**

### **Mode**

Enable.

### **Description**

The **rmon show etherstats** command displays entries in the Ethernet table for one or more ports. Entries in this table are created automatically when default tables are turned on for the Lite group.

### **Parameters**

|                          |   |
|--------------------------|---|
| <i>&lt;port-list&gt;</i> | Specifies the port(s) for which you want Ethernet statistics displayed. |
| <b>all-ports</b>         | Shows Ethernet statistics on all ports.                                 |

### **Restrictions**

The RMON agent reports only traffic *received* on a port. This command is available only if you have configured the Lite group.

## Example

To display Ethernet statistics on a specified port:

```

xp# rmon show etherstats et.5.1
RMON I Ethernet Statistics Table
Index: 502, Port: et.5.1, Owner: monitor ❶
-----
RMON EtherStats          Total
-----
Octets                    83616016 ❷
Unicast Frames            86185 ❸
Broadcast Frames          0 ❹
Multicast Frames          0 ❺
Collisions                0 ❻
64 Byte Frames            292 ❼
65-127 Byte Frames        16625
128-255 Byte Frames       6145
256-511 Byte Frames       4520
512-1023 Byte Frames      7992
1024-1518 Byte Frames     50611

```

Legend:

1. The EtherStats control table entry for this port:  
 Index: uniquely identifies this entry.  
 Port: port et.5.1.  
 Owner: default owner "monitor."
2. Number of octets of data received on the network.
3. Number of good frames received that were directed to a Unicast address.
4. Number of good frames received that were directed to a broadcast address.
5. Number of good frames received that were directed to a multicast address.
6. Number of collisions on this Ethernet segment.
7. Number of good and bad frames received, for various frame size ranges.

## rmon show events

### Purpose

Displays configured events and logs of triggered events.

### Format

**rmon show events**

### Mode

Enable.

### Description

The **rmon show events** command displays configured events and the logs, if any, of triggered events.

### Parameters

None.

### Restrictions

This command is only available if you have configured the Lite group.

### Example

To show RMON events and logs:

```
xp# rmon show events
```

```
RMON I Event table
```

| ❶<br>Index          | ❷<br>Type | ❸<br>Community | ❹<br>Description | ❺<br>Owner |
|---------------------|-----------|----------------|------------------|------------|
| 1                   | log       | public         | Log Only         | monitor    |
| No event logs found |           |                |                  |            |
| Index               | Type      | Community      | Description      | Owner      |
| 2                   | both      | private        | Log & Trap       | monitor    |
| No event logs found |           |                |                  |            |

**Legend:**

1. Index number that identifies this entry in the Event table.
2. Type of event: log, trap, or both log and trap.
3. Community string used for this event.
4. User-defined description of this event.
5. Owner of this event entry.

## **rmon show filters**

### **Purpose**

Shows the contents of the Filters table.

### **Format**

**rmon show filters**

### **Mode**

Enable.

### **Description**

The **rmon show filters** command displays the contents of the Filter table.

### **Parameters**

None.

### **Restrictions**

This command is only available if you have configured the Standard group.

### **Example**

To show the contents of the Filter table:

```
xp# rmon show filters
RMON 1 Filter Table
  No filters defined
```

# rmon show history

## Purpose

Shows statistics over a period of time.

## Format

**rmon show history** *<port-list>* | **all-ports**

## Mode

Enable.

## Description

The **rmon show history** command displays statistical samples that are stored in the RMON History group. Entries in this table are created automatically when default tables are turned on for the Lite group.

## Parameters

|                          |   |
|--------------------------|---|
| <i>&lt;port-list&gt;</i> | Specifies the port(s) for which the history is to be displayed. |
| <b>all-ports</b>         | Shows history information on all the ports.                     |

## Restrictions

This command is only available if you have configured the Lite group.

## Example

To display history information for a specific port:

| xp# rmon show history et.5.1 |                 |                |         |         |         |      |       |       |       |       |   |  |
|------------------------------|-----------------|----------------|---------|---------|---------|------|-------|-------|-------|-------|---|--|
| RMON I History Table         |                 |                |         |         |         |      |       |       |       |       |   |  |
| 1                            | 2               | 3              | 4       | 5       |         |      |       |       |       |       |   |  |
| Index                        | Port            | Interval(secs) | Buckets | Owner   |         |      |       |       |       |       |   |  |
| 502                          | et.5.1          | 300            | 50/50   | monitor |         |      |       |       |       |       |   |  |
| 6                            | 7               |                |         | 8       | 9       | 10   | 11    | 12    | 13    |       |   |  |
| Index                        | SysUpTime       |                |         | Octets  | Packets | Best | Mcast | Colls | %Util | Other |   |  |
| 213                          | 00D 17H 45M 47S |                |         | 318114  |         | 336  | 0     | 0     | 0     | 0     | 0 |  |
| 214                          | 00D 17H 50M 47S |                |         | 323928  |         | 341  | 0     | 0     | 0     | 0     | 0 |  |
| 215                          | 00D 17H 55M 48S |                |         | 323586  |         | 335  | 0     | 0     | 0     | 0     | 0 |  |
| 216                          | 00D 18H 00M 49S |                |         | 317186  |         | 320  | 0     | 0     | 0     | 0     | 0 |  |
| 217                          | 00D 18H 05M 49S |                |         | 323470  |         | 333  | 0     | 0     | 0     | 0     | 0 |  |
|                              |                 |                |         | .       |         |      |       |       |       |       |   |  |
|                              |                 |                |         | .       |         |      |       |       |       |       |   |  |
|                              |                 |                |         | .       |         |      |       |       |       |       |   |  |
| 258                          | 00D 21H 31M 03S |                |         | 322264  |         | 312  | 0     | 0     | 0     | 0     | 0 |  |
| 259                          | 00D 21H 36M 03S |                |         | 327944  |         | 315  | 0     | 0     | 0     | 0     | 0 |  |
| 260                          | 00D 21H 41M 04S |                |         | 333138  |         | 309  | 0     | 0     | 0     | 0     | 0 |  |
| 261                          | 00D 21H 46M 06S |                |         | 327782  |         | 312  | 0     | 0     | 0     | 0     | 0 |  |
| 262                          | 00D 21H 51M 07S |                |         | 332268  |         | 294  | 0     | 0     | 0     | 0     | 0 |  |

### Legend:

1. Index number that identifies the entry for this port in the History control table.
2. Port name.
3. Interval (in seconds) for data samples for each data bucket.
4. The actual number of buckets/the requested number of buckets.
5. Owner of this entry “monitor” (default).
6. Index number for this data bucket.
7. Time at which the sample was measured.
8. Total number of octets received on the network.
9. Number of packets received during the sampling period.
10. Number of good packets received during the sampling interval that were directed to a broadcast address.
11. Number of good packets received during the sampling interval that were directed to a multicast.
12. The number of collisions on this Ethernet segment during the sampling interval (best estimate).
13. The percentage of the network being utilized (best estimate).



# **rmon show host-top-n**

## **Purpose**

Displays the top *n* hosts.

## **Format**

**rmon show host-top-n**

## **Mode**

Enable.

## **Description**

The **rmon show host-top-n** command displays a report of the top hosts for a specified statistic. Note that the Host Top N report runs once. To run the reports again via the CLI, the control row must be disabled and then enabled. If the report has already been run, the Time Remaining field is set to zero. Otherwise, the Time Remaining field will be decremented until the report is run.

## **Restrictions**

This command is only available if you have configured the Standard group and Host Top N control table entries exist.

## **Example**

Consider the following command to gather the top *n* Host entries:

```
xp(config)# rmon host-top-n index 1 host-index 500 base out-octets duration 20 size 5
```

To display the Host Top N report, as specified by the previous command:

|                          |           |            |          |          |          |                 |          |
|--------------------------|-----------|------------|----------|----------|----------|-----------------|----------|
| xp# rmon show host-top-n |           |            |          |          |          |                 |          |
| RMON I HostTopN Table    |           |            |          |          |          |                 |          |
| <b>1</b>                 | <b>2</b>  | <b>3</b>   | <b>4</b> | <b>5</b> | <b>6</b> | <b>7</b>        | <b>8</b> |
| Index                    | HostIndex | RateBase   | TimeRem  | Duration | Buckets  | StartTime       | Owner    |
| 1                        | 500       | Out-Octets | 0        | 20       | 5/5      | 00D 00H 39M 29S | monitor  |
| <b>9</b>                 | <b>10</b> |            |          |          |          |                 |          |
| Address                  | Rate      |            |          |          |          |                 |          |
| -----                    | ----      |            |          |          |          |                 |          |
| 0080C8:C172A6            | 19911     |            |          |          |          |                 |          |
| 00001D:CBA3FD            | 0         |            |          |          |          |                 |          |

**Legend:**

1. Index number that identifies this entry in the Host Top N control table.
2. Index number that identifies the Host control table entry.
3. The parameter used to order the list of top “n” entries.
4. Number of seconds left in the report currently being collected.
5. Number of seconds that this report has collected during the last (or current) sampling interval.
6. Maximum number of hosts requested for the Top N table/maximum number of hosts in the Top N table.
7. The time of the sampling.
8. The owner of this entry.
9. The host address.
10. The value of the statistic for the host address.

# rmon show hosts

## Purpose

Shows statistics about the hosts discovered on the network.

## Format

**rmon show hosts** <port-list> | **all-ports** [**summary**]

## Mode

Enable.

## Description

The **rmon show hosts** command displays entries in the Hosts table for one or more ports. Entries in this table are created automatically when default tables are turned on for the Standard group.

If CLI filters have been applied, they will take effect when the Host table is displayed. This command will display control rows and their corresponding logs only if there are logs. A control row that has no data is not displayed.

## Parameters

|                               |  |
|-------------------------------|--|
| <port-list>  <b>all-ports</b> | The port(s) for which host information is to be shown. Use <b>all-ports</b> to show host information on all the ports. |
| <b>summary</b>                | Shows a summary of all control table rows with the number of logs in each row.   |

## Restrictions

This command is only available if you have configured the Standard group and control table entries exist for the specified port.

## Example

To show host information for a specific port:

```

xp# rmon show hosts et.5.1
RMON I Host Table
Index: 502, Port: et.5.1, Owner: monitor ❶

```

| ❷<br>Address  | ❸<br>InPkts | ❹<br>InOctets | ❺<br>OutPkts | ❻<br>OutOctets | ❼<br>Bcst | ❽<br>Mcst |
|---------------|-------------|---------------|--------------|----------------|-----------|-----------|
| -----         | -----       | -----         | -----        | -----          | ----      | ----      |
| 00001D:CBA3FD | 88917       | 88436760      | 62132        | 5095029        | 0         | 0         |
| 0080C8:C172A6 | 62132 5     | 095029        | 88920        | 88437062       | 0         | 0         |

### Legend:

1. Host control table information for this port:

Index: number that identifies the entry for this port in the table.

Port: port name.

Owner: the default owner “monitor.”

2. MAC address of the discovered host.
3. Number of good packets transmitted to this address.
4. Number of good octets transmitted to this address.
5. Number of good packets transmitted from this address.
6. Number of good octets transmitted from this address.
7. Number of good packets transmitted by this address that were directed to a broadcast address.
8. Number of good packets transmitted by this address that were directed to a multicast address.

To show a summary of host information:

```

xp# rmon show all-ports summary
RMON I Host Table Summary

```

| ❶<br>Index | ❷<br>Data | ❸<br>Rows | ❹<br>Port | ❺<br>Status Mode | ❻<br>Owner |
|------------|-----------|-----------|-----------|------------------|------------|
| -----      | -----     | -----     | -----     | -----            | -----      |
| 500        | 1         | et.5.1    | Up        | Address          | monitor    |
| 501        | 1         | et.5.2    | Up        | Address          | monitor    |
| 502        | 0         | et.5.3    | Down      | Flow             | monitor    |
| 503        | 17        | et.5.4    | Up        | Flow             | monitor    |
| 504        | 0         | et.5.5    | Down      | Flow             | monitor    |
| 505        | 0         | et.5.6    | Down      | Flow             | monitor    |
| 506        | 0         | et.5.7    | Down      | Flow             | monitor    |
| 507        | 0         | et.5.8    | Down      | Flow             | monitor    |

**Legend:**

1. Index number that identifies this entry in the Host control table.
2. Number of data rows associated with this index number.
3. Port.
4. Current state of the port.
5. Source of the data for this entry.
6. Owner of this entry.

# rmon show matrix

## Purpose

Shows statistics for source-destination address pairs.

## Format

**rmon show matrix** <port-list>|**all-ports** [**summary**] [**order-by** srcdst|dstsrc]

## Mode

Enable.

## Description

The **rmon show matrix** command displays entries in the Matrix table. Entries in this table are automatically created when default tables are turned on for the Standard group.

If CLI filters have been applied, they will take effect when the Matrix table is displayed. This command will display control rows and their corresponding logs only if there are logs. A control row that has no data is not displayed.

## Parameters

|                                  |   |
|----------------------------------|---|
| <port-list>  <b>all-ports</b>    | The port(s) for which you want to display information. Use <b>all-ports</b> to show matrix information on all the ports.                    |
| <b>summary</b>   <b>order by</b> | Use <b>summary</b> to display the control rows only. Use <b>order-by</b> to display entries by source/destination or by destination/source. |
| <b>srcdst</b>   <b>dstsrc</b>    | Use <b>srcdst</b> to display the entries by source/destination. Use <b>dstsrc</b> to display entries by destination/source.                 |

## Restrictions

This command is only available if you have configured the Standard group.

## Example

To show statistics for source-destination address pairs:

|  |               |         |        |
|--|---------------|---------|--------|
| xp# <b>rmon show matrix all-ports</b>      |               |         |        |
| RMON I Matrix Table                        |               |         |        |
| Port: et.5.1, Index: 500, Owner: monitor ❶ |               |         |        |
| ❷  | ❸             | ❹       | ❺      |
| SrcAddr                                    | DstAddr       | Packets | Octets |
| -----                                      | -----         | -----   | -----  |
| 00001D:CBA3FD                              | 0080C8:C172A6 | 3       | 264    |
| 0080C8:C172A6                              | 00001D:CBA3FD | 4       | 346    |
| Port: et.5.5, Index: 504, Owner: monitor   |               |         |        |
| SrcAddr                                    | DstAddr       | Packets | Octets |
| -----                                      | -----         | -----   | -----  |
| 00001D:CBA3FD                              | 080020:835CAA | 3       | 246    |
| 080020:835CAA                              | 00001D:CBA3FD | 2       | 164    |

### Legend:

- The Matrix control table entry for this port:  
 Port: the name of the port.  
 Index: the index number for this port in the Matrix table.  
 Owner: default “monitor.”
- Source MAC address.
- Destination MAC address.
- Number of packets transmitted from the source to the destination address, including bad packets.
- Number of octets transmitted from the source to the destination address.

To show control row summary statistics:

| xp# <b>rmon show matrix all-ports summary</b> |           |        |        |         |         |
|---|-----------|--------|--------|---------|---------|
| RMON I Matrix Table Summary                   |           |        |        |         |         |
| Index   | Data Rows | Port   | Status | Mode    | Owner   |
| -----   | -----     | ---    | -----  | -----   | -----   |
| 500   | 0         | et.1.1 | Up     | Address | monitor |
| 501   | 0         | et.1.2 | Down   | Address | monitor |
| 502   | 0         | et.1.3 | Down   | Address | monitor |
| 503   | 0         | et.1.4 | Up     | Address | monitor |
| 504   | 0         | et.1.5 | Down   | Address | monitor |
| 505   | 0         | et.1.6 | Down   | Address | monitor |
| 506   | 0         | et.1.7 | Down   | Address | monitor |
| 507   | 0         | et.1.8 | Up     | Address | monitor |
| 508   | 0         | gi.4.1 | Up     | Address | monitor |
| 509   | 0         | gi.4.2 | Up     | Address | monitor |
| 510   | 0         | et.7.1 | Up     | Address | monitor |
| 511   | 0         | et.7.2 | Down   | Address | monitor |
| 512   | 0         | et.7.3 | Down   | Address | monitor |
| 513   | 0         | et.7.4 | Down   | Address | monitor |
| 514   | 0         | et.7.5 | Down   | Address | monitor |
| 515   | 0         | et.7.6 | Down   | Address | monitor |
| 516   | 0         | et.7.7 | Down   | Address | monitor |
| 517   | 0         | et.7.8 | Down   | Address | monitor |
| 25  | 0         | et.1.3 | Down   | Address | monitor |



# rmon show nl-host

## Purpose

Shows the amount of traffic to and from each network address.

## Format

**rmon show nl-host** *<port-list>*|**all-ports** [**summary**]

## Mode

Enable.

## Description

The **rmon show nl-host** command shows entries in the RMON 2 Network Layer Host table for one or more ports. Entries in this table are created automatically when default tables are turned on for the Professional group.

If CLI filters have been applied, they will take effect when the Network Layer host table is displayed. This command shows control rows and their corresponding logs only if there are logs. A control row with no data will not appear in the report.

## Parameters

|   |   |
|---|---|
| <i>&lt;port-list&gt;</i>   <b>all-ports</b> | The port(s) for which you want to display traffic information. Use the keyword <b>all-ports</b> to show information on all the ports. |
| <b>summary</b>                              | Displays control row summary information only.  |

## Restrictions

This command is only available if you have configured the Professional RMON group and control table entries exist for the specified port.

## Example

To display the network layer host table for all ports:

|  |        |          |         |           |               |
|--|--------|----------|---------|-----------|---------------|
| xp# <b>rmon show nl-host all-ports</b>                             |        |          |         |           |               |
| RMON II Network Layer Host Table                                   |        |          |         |           |               |
| Index: 500, Port: et.5.1, Inserts: 3, Deletes: 0, Owner: monitor ❶ |        |          |         |           |               |
| ❷  | ❸      | ❹        | ❺       | ❻         | ❼             |
| Address  | InPkts | InOctets | OutPkts | OutOctets | Protocol      |
| -----  | -----  | -----    | -----   | -----     | -----         |
| 10.60.89.88  | 1159   | 952300   | 2       | 164       | *ether2.ip-v4 |
| 192.100.81.1   | 1      | 100      | 1       | 100       | *ether2.ip-v4 |
| 192.100.81.3   | 3      | 264      | 1160    | 952400    | *ether2.ip-v4 |
| Index: 504, Port: et.5.5, Inserts: 2, Deletes: 0, Owner: monitor   |        |          |         |           |               |
| Address  | InPkts | InOctets | OutPkts | OutOctets | Protocol      |
| -----  | -----  | -----    | -----   | -----     | -----         |
| 10.60.89.88  | 3      | 246      | 1220    | 98962     | *ether2.ip-v4 |
| 192.100.81.3   | 1220   | 98962    | 3       | 246       | *ether2.ip-v4 |

### Legend:

1. The control table entry for this port:

Index: index number that identifies this entry in the hl host control table.

Port: name of port.

Inserts: number of inserts in the network layer host table for this entry.

Deletes: number of deletions in the network layer host table for this entry.

Owner: the entity that configured this entry.

2. The network address.
3. Number of packets received by this network address.
4. Number of octets received by this network address.
5. Number of packets sent by this network address.
6. Number of octets sent by this network address.
7. The protocol, as defined in the RMON Protocol Directory for the X-Pedition router. Note that this shows the network layer protocol encapsulations only. If you want to see application/protocol information, such as the destination socket, use the **rmon show al-host** command.

# rmon show nl-matrix

## Purpose

Shows information about the traffic between network address pairs.

## Format

**rmon show nl-matrix** *<port-list>***|all-ports** [**order-by srcdst****|dstsrc**] [**summary**]

## Mode

Enable.

## Description

The **rmon show nl-matrix** command shows entries in the Network Layer Matrix table for one or more ports. Entries in this table are created automatically when default tables are turned on for the Professional group.

If CLI filters have been applied, they will take effect when this table is displayed. The control rows and their corresponding logs are displayed only if there are logs. A control row with no data will not appear in the report.

## Parameters

|  |  |
|--|--|
| <i>&lt;port-list&gt;</i> <b> all-ports</b> | The port(s) for which you want to display network layer traffic information. Use the keyword <b>all-ports</b> to show information for all ports. |
| <b>order-by srcdst</b>                     | Orders the logs by source address, then destination address (default).   |
| <b>order-by dstsrc</b>                     | Orders the logs by destination address, then source address.   |
| <b>summary</b>                             | Displays control row summary information only.   |

## Restrictions

This command is only available if you have configured the Professional group and control table entries exist for the specified port.

## Example

To show the Network Layer Matrix table for all ports:

|  |              |         |         |               |
|--|--------------|---------|---------|---------------|
| xp# <b>rmon show nl-matrix all-ports</b>                           |              |         |         |               |
| RMON II Network Layer Matrix Table                                 |              |         |         |               |
| Index: 500, Port: et.5.1, Inserts: 4, Deletes: 0, Owner: monitor ❶ |              |         |         |               |
| ❷  | ❸            | ❹       | ❺       | ❻             |
| SrcAddr  | DstAddr      | Packets | Octets  | Protocol      |
| -----  | -----        | -----   | -----   | -----         |
| 10.60.89.88  | 192.100.81.3 | 2       | 164     | *ether2.ip-v4 |
| 192.100.81.1   | 192.100.81.3 | 1       | 100     | *ether2.ip-v4 |
| 192.100.81.3   | 10.60.89.88  | 1241    | 1025436 | *ether2.ip-v4 |
| 192.100.81.3   | 192.100.81.1 | 1       | 100     | *ether2.ip-v4 |
| Index: 504, Port: et.5.5, Inserts: 2, Deletes: 0, Owner: monitor   |              |         |         |               |
| SrcAddr  | DstAddr      | Packets | Octets  | Protocol      |
| -----  | -----        | -----   | -----   | -----         |
| 10.60.89.88  | 192.100.81.3 | 1302    | 105604  | *ether2.ip-v4 |
| 192.100.81.3   | 10.60.89.88  | 3       | 246     | *ether2.ip-v4 |

### Legend:

1. The control table entry for this port:

Index: index number that identifies this entry in the control table.

Port: name of port.

Inserts: number of inserts in the Network Layer Matrix table for this entry.

Deletes: number of deletions in the Network Layer Matrix table for this entry.

Owner: the entity that configured this entry.

2. Source network address.
3. Destination network address.
4. Number of packets transmitted without error from the source to the destination.
5. Number of octets transmitted without error from the source to the destination.
6. The protocol, as specified in the RMON Protocol Directory for the X-Pedition router.

# **rmon show nl-matrix-top-n**

## **Purpose**

Reports the top *n* Network Layer Matrix entries, sorted by a specific metric.

## **Format**

**rmon show nl-matrix-top-n**

## **Mode**

Enable.

## **Description**

The **rmon show nl-matrix-top-n** command shows entries in the RMON 2 Network Layer Matrix Top N table.

## **Parameters**

None.

## **Restrictions**

This command is only available if you have configured the Professional group and entries exist in the Network Layer Matrix Top N table.

## **Example**

Consider the following command to gather the top *n* Network Layer Matrix entries:

|   |
|---|
| <pre>xp(config)# rmon nl-matrix-top-n index 1 matrix-index 500 ratebase all-octets duration 20 size 5</pre> |
|---|

To show the top n entries in the Network Layer Matrix table, as specified by the previous command:

| xp# rmon show nl-matrix-top-n |              |          |           |           |             |                   |         |         |
|-------------------------------|--------------|----------|-----------|-----------|-------------|-------------------|---------|---------|
| RMON II NI Matrix Table       |              |          |           |           |             |                   |         |         |
| ①                             | ②            | ③        | ④         | ⑤         | ⑥           | ⑦                 | ⑧       | ⑨       |
| Index                         | M-Index      | RateBase | TimeRem   | Duration  | Size        | StartTime         | Reports | Owner   |
| 1                             | 500          | Octets   | 20        | 20        | 5           | 00D 00H 51M 37S 1 | 1       | monitor |
| ⑩                             | ⑪            | ⑫        | ⑬         | ⑭         | ⑮           | ⑯                 |         |         |
| SrcAddr                       | DstAddr      | PktRate  | R-PktRate | OctetRate | R-OctetRate | Protocol          |         |         |
| -----                         | -----        | -----    | -----     | -----     | -----       | -----             |         |         |
| 192.100.81.3                  | 10.60.89.88  | 23       | 0         | 19986     | 0           | *ether2.ip-v4     |         |         |
| 192.100.81.1                  | 192.100.81.3 | 0        | 0         | 0         | 0           | *ether2.ip-v4     |         |         |
| 192.100.81.3                  | 192.100.81.1 | 0        | 0         | 0         | 0           | *ether2.ip-v4     |         |         |
| 10.60.89.88                   | 192.100.81.3 | 0        | 23        | 0         | 19986       | *ether2.ip-v4     |         |         |

#### Legend:

1. Index number that identifies this entry in the network layer Matrix Top N control table.
2. The Network Layer Matrix table for which the top N report is shown.
3. The parameter on which the entries are sorted.
4. Number of seconds left in the report currently being collected.
5. Number of seconds that this report has collected during the last sampling interval.
6. Maximum number of matrix entries in this report.
7. The time when this report was last started.
8. The number of reports generated by this entry.
9. The entity that configured this entry.
10. Network address of the source host.
11. Network address of the destination host.
12. Number of packets from the source to the destination during the sampling interval.
13. Number of packets from the destination to the source during the sampling interval.
14. Number of octets from the source to the destination during the sampling interval.
15. Number of octets from the destination to the source during the sampling interval.
16. The protocol, as defined in the RMON Protocol Directory for the X-Pedition router.

# rmon show packet-capture

## Purpose

Shows packets captured after flowing through a channel.

## Format

**rmon show packet-capture control-table** [**captured-packets** <control-index>]

## Mode

Enable.

## Description

The **rmon show packet-capture** command shows the buffer table for captured packets. Before you use this command, first configure the Filter Channel group using the **rmon channel index** command. Then use the **rmon capture** command to configure the Packet Capture group which allows packets to be captured after they have flowed through a channel.

## Parameters

|  |   |
|--|---|
| <b>control-table</b>                       | Displays RMON packet capture filter information. Each packet captured belongs to one entry of the control-table.  |
| <b>captured-packets</b><br><control-index> | Displays all of the packets captured for RMON. If you supply the optional <i>control-index</i> , you will display only packets captured for the specified control index; otherwise, you will display all captured packets. To determine the <i>control-index</i> , use the command “ <b>rmon show packet-capture control-table.</b> ” |

## Restrictions

- This command is available only if you have enabled the Standard RMON groups.
- Packet capture using RMON uses considerable CPU cycles. For best results, enable packet capture when the CPU is not busy running other important tasks and CPU utilization is low.

## **rmon show probe-config**

### **Purpose**

Shows the configuration of the X-Pedition router for interaction with other RMON devices.

### **Format**

**rmon show probe-config** [basic] [net-config] [trap-dest]

### **Mode**

Enable.

### **Description**

The **rmon show probe-config** command shows entries in the RMON 2 Probe Configuration table.

### **Parameters**

|                   |  |
|-------------------|--|
| <b>basic</b>      | Shows basic probe configuration information. |
| <b>net-config</b> | Shows network configuration table.           |
| <b>trap-dest</b>  | Shows trap destination table.                |

### **Restrictions**

This command is only available if you have configured the Professional group.



# rmon show protocol-directory

## Purpose

Displays the protocols that the X-Pedition router can monitor with RMON.

## Format

**rmon show protocol-directory** *<protocol>* | **all-protocols**

## Mode

Enable.

## Description

The **rmon show protocol-directory** command displays the protocol encapsulations that are defined in the RMON 2 Protocol Directory group for the X-Pedition router.

## Parameters

|                         |   |
|-------------------------|---|
| <i>&lt;protocol&gt;</i> | The specific protocol encapsulation that is managed with the RMON 2 Protocol Directory group. (See <a href="#">Appendix A</a> for protocol encapsulations that are supported on the X-Pedition router.) |
| <b>all-protocols</b>    | Displays all protocol encapsulations that are managed with the Protocol Directory group.  |

## Restrictions

This command is only available if you have configured the Professional group.

## Example

To show all protocol encapsulations that are managed with the Protocol Directory group:

| xp# <b>rmon show protocol-directory all-protocols</b> |         |      |        |        |              |
|---|---------|------|--------|--------|--------------|
| RMON II Protocol Directory Table                      |         |      |        |        |              |
| Last Change: 00D 00H 00M 00S                          |         |      |        |        |              |
| Index   | AddrMap | Host | Matrix | Status | Protocol     |
| 1   | Off     | Off  | Off    | Active | ether2       |
| 2   | NA      | Off  | Off    | Active | idp          |
| 3   | NA      | Off  | Off    | Active | ip-v4        |
| 4   | NA      | Off  | Off    | Active | chaosnet     |
| 5   | NA      | Off  | Off    | Active | arp          |
| 6   | NA      | Off  | Off    | Active | rarp         |
| 7   | NA      | Off  | Off    | Active | vip          |
| 8   | NA      | Off  | Off    | Active | vloop        |
| 9   | NA      | Off  | Off    | Active | vloop2       |
| 10  | NA      | Off  | Off    | Active | vecho        |
| 11  | NA      | Off  | Off    | Active | vecho2       |
| 12  | NA      | Off  | Off    | Active | ipx          |
| 13  | NA      | Off  | Off    | Active | netbios-3com |
| 14  | NA      | Off  | Off    | Active | atalk        |
| 15  | NA      | Off  | Off    | Active | aarp         |
| ...   |         |      |        |        |              |

**NOTE:** The example above shows a partial listing only.

# rmon show protocol-distribution

## Purpose

Shows the octets and packets detected for different protocols on a network segment.

## Format

**rmon show protocol-distribution** *<port-list>* | **all-ports**

## Mode

Enable.

## Description

The **rmon show protocol-distribution** command displays the RMON 2 Protocol Distribution table. This table contains a list of protocols, defined in the RMON 2 Protocol Directory, that are discovered by the X-Pedition router. Entries in this table are created automatically when default tables are turned on for the Professional group. If you delete an entry in the Protocol Directory, then entries in this table associated with the deleted protocol are also deleted.

If CLI filters have been applied, they will take effect when the Protocol Distribution table is displayed.

## Parameters

|                          |   |
|--------------------------|---|
| <i>&lt;port-list&gt;</i> | The port(s) for which you want to show protocol distribution. |
| <b>all-ports</b>         | Shows protocol distribution information on all the ports.     |

## Restrictions

This command is only available if you have configured the Professional group.

## Example

To show the RMON 2 Protocol Distribution table:

```
xp(config)# rmon show protocol-distribution all-ports
RMON II Protocol Distribution Table

Index: 508, Port: gi.4.1, Owner: monitor
Pkts Octets Protocol
-----
3312 304550 ether2
3312 304550 ip-v4
2459 234564 icmp
853 69986 tcp
853 69986 telnet
```

# **rmon show status**

## **Purpose**

Displays RMON status, groups, enabled ports, and memory utilization.

## **Format**

**rmon show status**

## **Mode**

Enable.

## **Description**

The **rmon show status** command shows whether RMON is enabled, the RMON groups that are configured, the ports on which RMON is enabled, and the memory allocated and used by RMON.

## **Parameters**

None.

## Example

To show RMON status:

```

xp# rmon show status
RMON Status
-----
* RMON is ENABLED ❶
* RMON initialization successful.

+-----+
| RMON Group Status | ❷
+-----+
| Group | Status | Default |
+-----+
| Lite  | On  | Yes  |
+-----+
| Std   | On  | Yes  |
+-----+
| Pro   | On  | Yes  |
+-----+

RMON is enabled on: et.5.1, et.5.2, et.5.3, et.5.4, et.5.5, et.5.6, et.5.7, et.5.8 ❸

RMON Memory Utilization ❹
-----
      Total Bytes Available: 48530436

Total Bytes Allocated to RMON: 4000000
      Total Bytes Used: 2637872
      Total Bytes Free: 1362128

```

### Legend:

1. When the X-Pedition router is booted, RMON is off by default. RMON is enabled with the **rmon enable** command.
2. Shows which RMON group (Lite, Standard, or Professional) is configured and whether default control tables are turned on.
3. Shows the ports on which RMON is enabled.
4. Shows RMON memory utilization. You can adjust the amount of memory allocated to RMON with the **rmon set memory** command.

# **rmon show user-history**

## **Purpose**

Shows user-defined collection of historical information from MIB objects on the X-Pedition router.

## **Format**

**rmon** *<string>* **show user-history** [**all-indexes**]

## **Mode**

Enable.

## **Description**

The **rmon show user-history** command shows the User History table.

## **Parameters**

|                       |   |
|-----------------------|---|
| <i>&lt;string&gt;</i> | Specifies a particular rmon.                  |
| <b>all-indexes</b>    | This optional parameter displays all indexes. |

## **Restrictions**

This command is only available if you have configured the Professional group.

## **rmon user-history-apply**

### **Purpose**

Applies a specified group to the User History control table.

### **Format**

**rmon user-history-apply** *<groupname>* **to** *<user-history-index>* [**status enable|disable**]

### **Mode**

Configure.

### **Description**

The **rmon user-history-apply** command applies all objects in the group created with the **rmon user-history-objects** command to the row in the User History control table. If the number of objects specified in the control row is greater than those in the group, the remaining OIDs are set to 0.0. If the number of objects specified in the control row is less than those in the group, the remaining are discarded.

### **Parameters**

|                                   |  |
|-----------------------------------|--|
| <i>&lt;groupname&gt;</i>          | Is the name of a group of objects that has been created with the <b>rmon-user-history-objects</b> command. |
| <i>&lt;user-history-index&gt;</i> | Specifies the row in the User History control table.   |

### **Restrictions**

None.



# rmon user-history-control

## Purpose

Monitors a group of objects (OIDs) over a period of time.

## Format

**rmon user-history-control index** <index-number> **objects** <number> **samples** <number>  
**interval** <number> [**owner** <string>] [**status enable|disable**]

## Mode

Configure.

## Description

The **rmon user-history-control** command monitors the group of objects that are defined with the **rmon user-history-objects** command. This command creates an entry in the User History control table.

Use the **rmon show user-history** command to display the User History table.

## Parameters

|                              |  |
|------------------------------|--|
| <index-number>               | A number between 1 and 65535 that uniquely identifies a row in the user history control table. |
| <b>objects</b> <number>      | Specifies the number of MIB objects to be collected.   |
| <b>samples</b> <number>      | Specifies the number of discrete time intervals over which data is to be saved.                |
| <b>interval</b> <number>     | Specifies the interval, in seconds, between samples.   |
| <b>owner</b> <string>        | Specifies the owner of the event; for example, an IP address, machine name or person's name.   |
| <b>status enable disable</b> | Enables or disables this matrix. The default is <b>enable</b> .                                |

## Restrictions

None.

# rmon user-history-objects

## Purpose

Defines a group of objects (OIDs).

## Format

**rmon user-history-objects** *<groupname>* **variable** *<oid>* **type** **absolute-value|delta-value**  
**[status enable|disable]**

## Mode

Configure.

## Description

The **rmon user-history-objects** command defines the group of objects that can be monitored with the **rmon user-history-control** command. This command creates a group with a single OID as a member of the group. To add several objects to the group, you need to issue multiple **user-history-objects** commands. Each object appears as a separate row in the User History control table.

## Parameters

|   |   |
|---|---|
| <i>&lt;groupname&gt;</i>                      | Name of the group of objects.                                   |
| <b>variable</b> <i>&lt;oid&gt;</i>            | Specifies the object identifier to be monitored.                |
| <b>type</b> <b>absolute-value delta-value</b> | Specifies the method of sampling for the selected variable.     |
| <b>interval</b> <i>&lt;number&gt;</i>         | Specifies the interval, in seconds, between samples.            |
| <b>status</b> <b>enable disable</b>           | Enables or disables this matrix. The default is <b>enable</b> . |

## Restrictions

None.

# Chapter 64

## sam Commands

The **sam** commands allow users to configure and monitor the Security Attack Monitor (SAM).

### Command Summary

[Table 55](#) lists the **sam** commands. The sections following the table describe the command syntax.

**Table 55. sam Commands**

|   |
|---|
| <b>sam clear history   statistics</b>   |
| <b>sam enable</b>                       |
| <b>sam set activation-delay</b> <num>   |
| <b>sam set deactivation-delay</b> <num> |
| <b>sam set rate-limit</b> <num>         |
| <b>sam show history</b>                 |
| <b>sam show statistics</b>              |
| <b>sam show status</b>                  |

# sam clear

## Format

**sam clear history | statistics**

## Mode

Enable.

## Description

The **sam clear** command allows users to clear the current SAM history and statistics.

## Parameters

|                   |   |
|-------------------|---|
| <b>history</b>    | Clear SAM activation history, including the duration (i.e., start and end times) of the last 32 activations, the list of affected ports, and the list of port(s) that caused these activations. |
| <b>statistics</b> | Clear SAM statistics, including the number of times SAM was activated and the last time the statistics were cleared using the sam clear statistics command.                                     |

## Restrictions

None.

## Examples

To clear the SAM history, enter the following:

```
xp# sam clear history
```

Entering the **sam show history** command after clearing the SAM history displays the following:

```
xp# sam show history
There are no new Service Availability Manager activations since 2003-07-23 11:17:50
There are no current activations.
All previous activation records were cleared at 2003-07-23 11:17:50
```

To clear all SAM statistics, enter the following:

```
xp# sam clear statistics
```

# sam enable

## Format

**sam enable**

## Mode

Configure.

## Description

The **sam enable** command activates the X-Pedition Security Attack Monitor (SAM). With SAM enabled, the X-Pedition router will detect abnormally high network traffic that is typical of DoS attacks and aggressive NMS configurations, identify the ingress ports, re-prioritize attack traffic, then rate-limit the attack traffic received on the port range.

**Note:** SAM is disabled by default.

## Parameters

None.

## Restrictions

None.

## Example

To enable SAM on the X-Pedition router, enter the following:

```
xp (config)# sam enable
```

## sam set activation-delay

### Format

**sam set activation-delay** *<num>*

### Mode

Configure.

### Description

The **sam set activation-delay** command allows users to define how long the X-Pedition router will wait after detecting an attack before activating SAM.

### Parameters

|   |  |
|---|--|
| <b>activation-delay</b><br><i>&lt;num&gt;</i> | The amount of time (10 to 300 seconds) to wait before activating SAM.<br>By default, this delay is 20 seconds. |
|---|--|

### Restrictions

SAM is disabled by default. Therefore, this command will not take effect until the **sam enable** command is saved to the active configuration.

### Examples

To activate SAM 60 seconds after the router detects an attack, enter the following:

```
xp(config)# sam set activation-delay 60
```

# sam set deactivation-delay

## Format

**sam set deactivation-delay** <num>

## Mode

Configure.

## Description

The **sam set deactivation-delay** command allows users to set the length of time to wait after an attack before deactivating SAM. The deactivation delay prevents temporary interruptions in attack traffic from deactivating SAM prematurely. Before SAM will deactivate, attacks on each activated port range must subside for the specified deactivation delay

## Parameters

|                                    |  |
|------------------------------------|--|
| <b>deactivation-delay</b><br><num> | The amount of time (5 to 300 seconds) to wait before SAM deactivates.<br>By default, this delay is 20 seconds. |
|------------------------------------|--|

## Restrictions

SAM is disabled by default. Therefore, this command will not take effect until the **sam enable** command is saved to the active configuration.

## Examples

To deactivate SAM and return activated ports to normal status 35 seconds after an attack subsides, enter the following:

```
xp(config)# sam set deactivation-delay 35
```

## sam set rate-limit

### Format

**sam set rate-limit** <num>

### Mode

Configure.

### Description

The **sam set rate-limit** command sets the rate at which the CM will process and forward unlearned traffic from all activated ports. To disable rate limiting, enter a value of 0.

### Parameters

---

|                         |   |
|-------------------------|---|
| <b>rate-limit</b> <num> | The rate (in packets per second) at which the Control Module will process and forward unlearned traffic sent from all activated ports to the CM. Enter a value from 0 to 1000 (a value of 0 disables rate limiting). By default, this value is 100. |
|-------------------------|---|

---

### Restrictions

SAM is disabled by default. Therefore, this command will not take effect until the **sam enable** command is saved to the active configuration.

### Examples

To configure the router to process and send only 500 unlearned packets from all activated ports, enter the following:

```
xp(config)# sam set rate-limit 500
```



# **sam show history**

## **Format**

**sam show history**

## **Mode**

Enable.

## **Description**

The **sam show history** command allows users to display the SAM activation history. Each time a user enters this command, the router displays up to the last 32 instances that SAM was activated and deactivated. If SAM is currently active, the router includes the current activation in the output.

## **Parameters**

None.

## **Restrictions**

None.

## Example

The following is an example of the **sam show history** command output:

```
xp# sam show history

Security Attack Monitor history was last cleared on boot

----- Current Activations -----

Activation time           : 2004-01-12 16:14:48
Ports affected by this activation : et.5.1-8
Ports identified as attackers   : et.5.1
Ports currently being rate-limited : et.5.1

Activation time           : 2004-01-12 16:14:48
Ports affected by this activation : et.3.1-16
Ports identified as attackers   : et.3.(5,10)
Ports currently being rate-limited : et.3.5

----- Previous Activations -----

Deactivation time         : 2004-01-12 15:58:16
Activation time           : 2004-01-12 14:24:11
Ports affected by this activation : et.5.1-8
Ports identified as attackers   : et.5.1

Deactivation time         : 2004-01-12 15:18:19
Activation time           : 2004-01-12 14:24:11
Ports affected by this activation : gi.7.1-2
Ports identified as attackers   : gi.7.1

Deactivation time         : 2004-01-12 15:18:19
Activation time           : 2004-01-12 14:24:11
Ports affected by this activation : gi.6.1-2
Ports identified as attackers   : gi.6.2
```

# sam show statistics

## Format

**sam show statistics**

## Mode

Enable.

## Description

The **sam show statistics** command displays SAM's current status, the number of times SAM has activated, and the last time the statistics were cleared using the **sam clear statistics** command.

## Parameters

None.

## Restrictions

None.

## Example

The following shows an example of the SAM statistics output:

```
xp# sam show statistics
Security Attack Monitor      : Enabled
Security Attack Monitor      : Active
Number of new activation since last reset : 9
Number of new rate-limiting added since last reset : 14
Number of port ranges currently being suppressed : 2
Number of ports currently being rate-limited : 3
Statistics last cleared      : 2004-01-12 18:51:31
```

# sam show status

## Format

**sam show status**

## Mode

Enable.

## Description

The **sam show status** command will display SAM's current state on all modules installed in the router.

## Parameters

None.

## Restrictions

None.

## Example

The following shows a typical output for the **sam show status** command:

```
xp# sam show status

Security Attack Monitor      :   Enabled
Unlearned traffic parameters :
  Activation delay           :   20 seconds
  Deactivation delay         :   60 seconds
  Rate-limit for all rate-limited ports : 100 packets per second

Current state of the modules in the chassis:
Slot 3:
  Ports 1-16 :  suppressed, rate-limiting et.3.(5,10)
Slot 4:
  Ports 1-2  :  normal
Slot 5:
  Ports 1-8  :  suppressed, rate-limiting et.5.1
Slot 6:
  Ports 1-2  :  normal
Slot 7:
  Ports 1-2  :  normal
```

# Chapter 65

## save Command

The **save** command saves the configuration changes you have entered during the current CLI session. You can save the configuration commands in the scratchpad to the active configuration, thus activating changes. You then can save the active changes to the Startup configuration.

### Format

**save active|startup**

### Mode

Configure.

**Note:** If you are in Enable mode, you still can save the active configuration changes to the Startup configuration file by entering the **copy active to startup** command.

### Description

Saves configuration changes.

- If you use the **active** keyword, uncommitted changes in the scratchpad are *activated*. The X-Pedition router accumulates configuration commands in the scratchpad until you activate them, clear them, or reboot. The X-Pedition router runs these commands when you activate the changes.
- If you use the **startup** keyword, the X-Pedition router saves the *active* configuration to the Startup file. Any non-committed commands in the Scratchpad are ignored.

### Parameters

---

|                         |  |
|-------------------------|--|
| <b>active   startup</b> | Specifies the destination for the configuration commands you are saving. |
|-------------------------|--|

---

---

## Restrictions

None.

# Chapter 66

## search Command

### search

#### Format

**search** <search-string> **active-config** | **scratchpad**

#### Mode

Configure.

#### Description

The **search** command allows users to look for specific character strings within the Active configuration or scratchpad. By default, the **search** command looks in the Active configuration.

#### Parameters

|                      |  |
|----------------------|--|
| <search-string>      | Enter a character string for which to search. If the character string includes spaces, users must put the string in quotes (i.e., "vlan add"). |
| <b>active-config</b> | Enter this option to search the active configuration (running system).   |
| <b>scratchpad</b>    | Enter this option to search the scratchpad (non-committed changes).  |

#### Restrictions

None.

## Example

To search the active configuration for any use of the **vlan add** command, enter the following from the CLI:

```
xp(config)# search "vlan add" active-config
9 : vlan add ports gi.1.1 to vlan11
10 : vlan add ports gi.1.2 to vlan12
11 : vlan add ports gi.2.2 to vlan22
12 : vlan add ports gi.2.1 to vlan21
13 : vlan add ports gi.3.1 to vlan31
14 : vlan add ports gi.3.2 to vlan32
15 : vlan add ports gi.4.2 to vlan42
16 : vlan add ports gi.4.1 to vlan41
```

To search the active configuration for uses of the **smarttrunk** command, enter the following from the CLI:

```
xp(config)# search smarttrunk
1 : smarttrunk create st.1 protocol no-protocol
2 : smarttrunk add ports et.5.3-4 to st.1
```

To search the scratchpad for any uses of a port that begins with the "et" (ethernet) designation, enter the following from the CLI:

```
xp(config)# search et scratchpad
2*: smarttrunk add ports et.5.3-4 to st.1
!
4*: vlan add ports et.5.7-8,st.1 to yyy
!
5*: qos set ip xxx low any any any any et.5.1-2 any any any
!
6*: system set name SSR8-9
7*: system set idle-timeout serial 0 telnet 0
!
8*: arp add 10.0.0.69 mac-addr 00:0d:11:22:33:44 exit-port et.5.1
!
11*: comment line 6 "vlan add ports et.5.(1-3) to xxx"
xp(config)#
```



# Chapter 67

## show Command

### Purpose

The **show** command displays the configuration of your running system.

### Format

**show active | scratchpad | startup | failed**

### Mode

Configure.

### Description

The **show** command displays the configuration of your running system as well as any non-committed changes in the scratchpad. Each CLI command is preceded with a number. This number can be used with the **negate** command to negate one or more commands. If you see the character **E** (for Error) immediately following the command number, it means the command did not execute successfully due to an earlier error condition. To get rid of the command in error, you can either negate it or fix the original error condition.

There are three modes for the **show** command: **active**, **scratchpad**, and **startup**. Specifying **active** shows you the configuration that are currently active on the router. Specifying **scratchpad** shows you the configuration currently in the scratchpad but have yet to be applied as active. Specifying **startup** shows the configuration that will be applied to the next bootup. You must specify one of these three modes as a parameter for the **show** command.

---

When viewing the active configuration file, the CLI displays the configuration file command lines with the following possible annotations:

- Commands without errors are displayed without any annotation.
- Commands with errors are annotated with an “E”.
- If a particular command has been applied such that it can be expanded on additional interfaces/modules, then it is annotated with a “P”. For example, if you enable STP on all ports in the current system, but the X-Pedition router contains only one module, then that particular command will be extended to all modules when they have been added to the X-Pedition router.

A command like **stp enable et.\*.\*** would be displayed as follows:

P: stp enable et.\*.\*

indicating that it is only partially applied. If you add more modules to the X-Pedition router at a later date and then update the configuration file to encompass all of the available modules in the X-Pedition router, then the “P:” portion of the above command line would disappear when displaying this configuration file.

If a potentially partial command, which was originally configured to encompass all of the available modules on the X-Pedition router, becomes only partially activated (after a hotswap or some such chassis reconfiguration), then the status of that command line will automatically change to indicate a partial completion status, complete with “P:”.

**Note:** Commands with no annotation or annotated with a “P:” are not in error.

## Parameters

|                   |  |
|-------------------|--|
| <b>active</b>     | Specify this parameter to show the configuration that are currently active on the router.                          |
| <b>scratchpad</b> | Specify this parameter to show the configuration currently in the scratchpad but have yet to be applied as active. |
| <b>startup</b>    | Specify this parameter to show the configuration that will be applied to the next bootup.                          |
| <b>failed</b>     | This parameter shows all active configuration lines on the router that are in partial or total error.              |

## Restrictions

None.

---

## Examples

The following command shows the active configuration:

```
xp(config)# show active
Running system configuration:
!
! Last modified from Console on 2000-02-09 13:00:46
!
1E: atm create vcl port at.9.1.1.200
!
2E: interface create ip pos11 address-netmask 20.11.11.20/24 peer-address 20.11
.11.21 type point-to-point port so.13.1
3E: interface create ip atm1 address-netmask 12.1.1.1/24 port at.9.1.1.200
4 : interface add ip en0 address-netmask 134.141.179.147/27
!
5 : ip add route 134.141.173.0/24 gateway 134.141.179.129
6 : ip add route 134.141.176.0/24 gateway 134.141.179.129
7 : ip add route 134.141.172.0/24 gateway 134.141.179.129
!
8 : system set idle-timeout telnet 0
9 : system set idle-timeout serial 0
```

The following command shows the configuration currently in the scratchpad:

```
xp(config)# show scratchpad

***** Non-committed changes in Scratchpad *****
1*: atm define service service1 srv-cat cbr pcr 100000
!
2*: vlan create vlan1 ip id 5
!
3*: ip add route default host gateway 100.0.0.1
```

---

The following command shows the configuration saved for startup at next bootup:

```
xp(config)# show startup
!
! Startup configuration for the next system reboot
!
! Last modified from Console on 2001-12-28 16:51:19
!
version 3.1
atm create vcl port at.9.1.1.200
interface create ip pos11 address-netmask 20.11.11.20/24 peer-address 20.11.11.2
1 type point-to-point port so.13.1
interface create ip atm1 address-netmask 12.1.1.1/24 port at.9.1.1.200
interface add ip en0 address-netmask 134.141.179.147/27
ip add route 134.141.173.0/24 gateway 134.141.179.129
ip add route 134.141.176.0/24 gateway 134.141.179.129
ip add route 134.141.172.0/24 gateway 134.141.179.129
system set idle-timeout telnet 0
system set idle-timeout serial 0
pos set so.13.1 working protecting so.13.2
```

# Chapter 68

## smarttrunk Commands

SmartTRUNK ports are groups of ports that have been logically combined to increase throughput and provide link redundancy. The **smarttrunk** commands let you display and set parameters for SmartTRUNK ports. For additional information regarding SmartTRUNKs, see the *Enterasys X-Pedition User Reference Manual*.

### Command Summary

[Table 56](#) lists the **smarttrunk** commands. The sections following the table describe the command syntax.

**Table 56. smarttrunk Commands**

|  |
|--|
| <b>smarttrunk add ports</b> <port list> <b>to</b> <smarttrunk>   |
| <b>smarttrunk clear load-distribution</b> <smarttrunk list>   <b>all-smarttrunks</b>   |
| <b>smarttrunk create</b> <smarttrunk> <b>protocol</b> huntgroup  no-protocol  lacp [no-llap-ack]   |
| <b>smarttrunk lacp actor-parameters port</b> <port_list> <b>enable</b> [port-key <number>]<br>[port-priority <number>] [activity active  passive] [aggregation aggregatable  individual]<br>[timeout long  short]                                    |
| <b>smarttrunk lacp aggregator</b> <smarttrunk> <b>port-type</b> 10-100-Ethernet  Gigabit-Ethernet <br>10Gigabit-Ethernet  <b>actor-key</b> <number>  <b>default-10-100</b>   <b>default-gig</b>   <b>default-10gig</b><br>[system-priority <number>] |
| <b>smarttrunk set load-policy round-robin</b>  link-utilization on <smarttrunk-list> <br><b>all-smarttrunks</b>  |
| <b>smarttrunk show</b> <option>  |

# smarttrunk add ports

## Purpose

Adds physical ports to a SmartTRUNK.

## Format

**smarttrunk add ports** <port list> **to** <smarttrunk>

## Mode

Configure.

## Description

The **smarttrunk add ports** command allows you to add the ports specified in <port\_list> to a SmartTRUNK. Before adding the ports, you must create a SmartTRUNK with the **smarttrunk create** command and set all SmartTRUNK ports to full duplex. See [smarttrunk create on page 1153](#) for information on creating SmartTRUNKs.

**Note:** The DEC Hunt Group control protocol is limited to 256 ports. On the ER-16, you may configure SmartTRUNKs that use the DEC Hunt Group control protocol on slots 1-7 only.

## Parameters

|              |  |
|--------------|--|
| <port_list>  | The port(s) you will add to an existing SmartTRUNK. All the ports in the SmartTRUNK must be connected to the same destination. |
| <smarttrunk> | name of the existing SmartTRUNK to which you will add physical ports.  |

## Restrictions

Ports added to a SmartTRUNK must:

- Be set to full duplex
- Be members of the same VLAN
- Share identical properties (e.g., L2 aging, STP state)

**Note:** Do not use the **add ports** command to add ports to an LACP SmartTRUNK. When you use the **lACP actor-parameters** command to enable LACP, the X-Pedition router adds ports to the SmartTRUNK dynamically.

## Example

To add ports et.1.1, et.1.2, and et.1.3 to SmartTRUNK st.1:

```
xp(config)# smarttrunk add ports et.1.(1-3) to st.1
```

# smarttrunk clear load-distribution

## Purpose

Clears load distribution statistics for ports in a SmartTRUNK.

## Format

**smarttrunk clear load-distribution** <smarttrunk list> | **all-smarttrunks**

## Mode

Enable.

## Description

The **smarttrunk clear load-distribution** command allows you to reset load distribution statistics to zero. This command is used in conjunction with the **smarttrunk show distribution** command to gather statistics for the transmitted bytes per second flowing through the SmartTRUNK and each port in it.

## Parameters

|                        |   |
|------------------------|---|
| <smarttrunk list >     | The name of one or more existing SmartTRUNKs.             |
| <b>all-smarttrunks</b> | Clears load distribution information for all SmartTRUNKs. |

## Restrictions

None.

## Example

To clear load distribution information from SmartTRUNK st.1, enter the following:

```
xp# smarttrunk clear load-distribution st.1
```



# smarttrunk create

## Purpose

Create a SmartTRUNK and specify a control protocol for it.

## Format

**smarttrunk create** <smarttrunk> **protocol** huntgroup| **no-protocol**| lacp [**no-llap-ack**]

## Mode

Configure.

## Description

The **smarttrunk create** command allows you to create a SmartTRUNK logical port. Once you create a SmartTRUNK port, you can add physical ports to it with the **smarttrunk add ports** command.

SmartTRUNKs on the X-Pedition router are compatible with the DEC Hunt Groups control protocol. If you connect the SmartTRUNK to another X-Pedition router, Enterasys switch, or Digital GIGAswitch/Router, you can specify that the SmartTRUNK use this control protocol. SmartTRUNKing and Hunt Groups are composed of two protocols:

- Logical Link Aging Protocol (LLAP) – Assists in learning and aging
- Physical Link Affinity Protocol (PLAP) – Monitors and maintains the trunking states

SmartTRUNKs are also compatible with devices that do not support the Hunt Groups control protocol, such as those that support Cisco's EtherChannel technology. If you connect a SmartTRUNK to devices that do not support Hunt Groups, *no control protocol is used*. You must specify the **no-protocol** keyword in the **smarttrunk create** command.

## Parameters

|                                 |  |
|---------------------------------|--|
| <code>&lt;smarttrunk&gt;</code> | <p>The name of the SmartTRUNK to create, in the form <i>st.x</i> (e.g., <i>st.1</i>).</p> <ul style="list-style-type: none"> <li>The maximum number of SmartTRUNKs you may configure depends on the router you are using: <ul style="list-style-type: none"> <li>X-Pedition 2000 router allows up to 40</li> <li>X-Pedition 8000 router allows up to 64</li> <li>X-Pedition 8600 router allows up to 128</li> <li>ER-16 allows up to 256</li> </ul> </li> </ul> <p><b>Note:</b> When using firmware version E9.1.0.0 or later, the ER-16 supports SmartTRUNKs that use the lower index ranges of 1-240 only (i.e., <i>st.1</i>–<i>st.240</i>).</p> |
| <b>huntgroup</b>                | Specifies that the DEC Hunt Group control protocol be used. Use this keyword if you connect the SmartTRUNK to another X-Pedition router, Enterasys switch, or Digital GIGAswitch/Router.   |
| <b>no-protocol</b>              | Specifies that no control protocol be used. Use this keyword if the SmartTRUNK connects to a device that does not support the DEC Hunt Group control protocol.   |
| <b>lACP</b>                     | This option specifies that the 802.3 Link Aggregation Control Protocol be used. (Use this keyword if you are creating a SmartTRUNK for an aggregator.)   |
| <b>no-llap-ack</b>              | By default, the X-Pedition router sends out extra LLAP ack packets for backward compatibility with some Cabletron products. Select this option to stop these extra packets.  |

## Restrictions

When using firmware version E9.1.0.0 or later, the ER-16 supports SmartTRUNKs that use the lower index ranges of 1-240 only (i.e., *st.1*–*st.240*).

## Example

The following command creates a SmartTRUNK, *st.1* that uses the DEC Hunt Group control protocol.

```
xp(config)# smarttrunk create st.1 protocol huntgroup
```

# smarttrunk lacp actor-parameters

## Purpose

Enable Link Aggregation Control Protocol (LACP) and set actor parameters on a port to run link aggregation.

## Format

**smarttrunk lacp actor-parameters port** <port\_list> **enable** [**port-key** <number>]  
[**port-priority** <number>] [**activity** **active**| **passive**] [**aggregation** **aggregatable**| **individual**]  
[**timeout** **long**| **short**]

## Mode

Configure.

## Description

The **smarttrunk lacp actor-parameters** command allows you to enable LACP and set the actor parameters on a port to run link aggregation with the 802.3ad Link Aggregation Control Protocol (LACP).

### Specify Actor Parameters for LACP (Link Aggregation Control Protocol)

To set the actor parameters, do the following:

|  |  |
|--|--|
| Enable LACP on a port or series of ports.          | <b>smarttrunk lacp actor-parameters</b><br><b>port</b> <port_list> <b>enable</b>   |
| Set the administrative key for the port.           | <b>smarttrunk lacp actor-parameters port</b><br><port_list> <b>enable port-key</b> <number>  |
| Set the administrative priority for the port.      | <b>smarttrunk lacp actor-parameters</b><br><b>port</b> <port_list> <b>enable port-priority</b> <number>                              |
| Set the administrative LACP activity for the port. | <b>smarttrunk lacp actor-parameters</b><br><b>port</b> <port_list> <b>enable activity</b> <b>active</b>   <b>passive</b>             |
| Set the administrative aggregation for the port.   | <b>smarttrunk lacp actor-parameters</b><br><b>port</b> <port_list> <b>enable aggregation</b> <b>aggregatable</b>   <b>individual</b> |
| Set the administrative LACP Timeout for the port.  | <b>smarttrunk lacp actor-parameters</b><br><b>port</b> <port_list> <b>enable timeout</b> <b>long</b>   <b>short</b>                  |

## Parameters

|   |  |
|---|--|
| <b>port</b> <port-list>   | The port number for which to set the parameters.   |
| <b>enable</b>   | Enables LACP on the specified ports.   |
| <b>port-key</b> <number>  | Sets the admin key (1-65536) for the port (optional). The default port-key is <b>1</b> for 10-100 ports, <b>2</b> for gig ports, and <b>3</b> for 10gig ports. |
| <b>port-priority</b> <number>   | Sets the admin priority (1-65536) for the port (optional). The default priority is <b>1</b> .  |
| <b>activity</b> <b>active</b>   <b>passive</b>  | Sets the admin LACP activity (active or passive) for the port (optional). By default, the port is <b>active</b> .  |
| <b>aggregation</b> <b>aggregatable</b>   <b>individual</b>                                    | Sets the admin aggregation (aggregate or individual) for the port (optional). By default, the port setting is aggregate.                                       |
| <b>timeout</b> <b>long</b>   <b>short</b>   | Defines the admin LACP timeout (long or short) for the port (optional). By default, the timeout is <b>short</b> .  |
| <b>Note:</b> Any parameter for which you do not specify a value will use its default setting. |  |

## Restrictions

None.

# smarttrunk lacp aggregator

## Purpose

Set properties of the aggregator.

## Format

**smarttrunk lacp aggregator** <smarttrunk> **port-type** 10-100-Ethernet| Gigabit-Ethernet| 10Gigabit-Ethernet| **actor-key** <number>| **default-10-100**| **default-gig**| **default-10gig** [**system-priority** <number>]

## Mode

Configure.

## Description

The **smarttrunk lacp aggregator** command allows you to define aggregator properties.

## Parameters

|   |  |
|---|--|
| <b>aggregator</b><br><smarttrunk>   | Use this parameter to identify the SmartTRUNK you will configure.  |
| <b>port-type</b><br>10-100-Ethernet <br>Gigabit-Ethernet <br>10Gigabit-Ethernet                       | Defining the <b>port-type</b> parameter specifies whether the ports associated with the aggregator are 10/100 Ethernet, Gigabit Ethernet, or 10 Gigabit Ethernet ports.  |
| <b>actor-key</b> <number> <br><b>default-10-100</b>  <br><b>default-gig</b>  <br><b>default-10gig</b> | The <b>actor-key</b> parameter specifies the administrative key for the aggregator. To use a default value, enter one of the following: <b>default-10-100</b> , <b>default-gig</b> or <b>default-10gig</b> . If you define more than one LACP SmartTRUNK on the same router, the SmartTRUNKs cannot share the same key values. |
| <b>system-priority</b><br><number>  | Sets the priority (1-65536) of the system (optional). The default priority is <b>1</b> .   |

## Restrictions

Multiple LACP SmartTRUNKs cannot share the same default values—each SmartTRUNK must use a different default value.

# smarttrunk set load-policy

## Purpose

Specify traffic distribution among SmartTRUNK ports.

## Format

**smarttrunk set load-policy round-robin |link-utilization on <smarttrunk-list>| all-smarttrunks**

## Mode

Configure.

## Description

The **smarttrunk set load-policy** command lets you specify how a SmartTRUNK distributes traffic among its ports.

## Parameters

|                                 |   |
|---------------------------------|---|
| <b>round-robin</b>              | Round-robin (the default) assigns flows to ports on a sequential basis. The first flow goes to the first port in the SmartTRUNK, the second flow to the second port, and so on. This distributes traffic evenly across all ports. |
| <b>link-utilization</b>         | Sends packets to the least-used port in the SmartTRUNK.   |
| <b>&lt;smarttrunk-list &gt;</b> | Sends packets to one or more specific SmartTRUNKs.  |
| <b>all-smarttrunks</b>          | Apply the command to all SmartTRUNKs.   |

## Restrictions

None.

## Example

To specify that SmartTRUNK st.1 distribute flows sequentially among its component ports:

```
xp(config)# smarttrunk set load-policy on st.1 round-robin
```

# smarttrunk show

## Purpose

Displays information about SmartTRUNKs on the X-Pedition router.

## Format

**smarttrunk show trunks**

**smarttrunk show distribution| protocol-state| connections** <smarttrunk list>| **all-smarttrunks**

## Mode

Enable.

## Description

The **smarttrunk show** command displays statistics about SmartTRUNKs on the X-Pedition router.

## Parameters

|                        |   |
|------------------------|---|
| <b>connections</b>     | Shows information about the SmartTRUNK connection, including the MAC address of the remote switch, and the module number and port number of each remote port. Connection information is reported only if the Hunt Group protocol is enabled for the SmartTRUNK. |
| <b>protocol-state</b>  | Shows information about the control protocol on a SmartTRUNK.   |
| <b>distribution</b>    | Provides statistics on traffic distribution across the ports in a SmartTRUNK.   |
| <b>trunks</b>          | Shows information about all SmartTRUNKs, including active and inactive ports, and the control protocol used.  |
| <b>lACP-control</b>    | Shows the lACP parameters.  |
| <b>lACP-stats</b>      | Shows the lACP statistic counters.  |
| <b>show lags</b>       | Shows the lACP LAGs and their members.  |
| <smarttrunk list>      | Name of one or more specific SmartTRUNK for which you will display statistics.  |
| <b>all-smarttrunks</b> | Apply the command to all SmartTRUNKs.   |

## Restrictions

None.

## Examples

To display information about all SmartTRUNKs on the X-Pedition router:

```
xp# smarttrunk show trunks
```

Flags: D - Disabled I - Inactive

| SmartTRUNK | Active Ports | Inactive Ports | Primary | Port  | Protocol | Load-Policy | Flags |
|------------|--------------|----------------|---------|-------|----------|-------------|-------|
| -----      | -----        | -----          | -----   | ----- | -----    | -----       | ----- |
| st.1       | et.3.(7-8)   | None           | None    | RR    |          |             |       |

To show how traffic is distributed across the ports on all SmartTRUNKs:

```
xp# smarttrunk show distribution all-smarttrunks
```

| SmartTRUNK | Member | %TX Util. | %RX Util. | Link Status | Grp Status |
|------------|--------|-----------|-----------|-------------|------------|
| -----      | -----  | -----     | -----     | -----       | -----      |
| st.1       | et.2.4 | 0.00      | 0.00      | Forwarding  | Up         |
| st.1       | et.2.5 | 0.00      | 0.00      | Forwarding  | Up         |
| st.1       | et.2.6 | 0.00      | 0.00      | Forwarding  | Up         |

To show information about the control protocol for SmartTRUNK st.1:

```
xp# smarttrunk show protocol-state st.1
```

| SmartTRUNK | Protocol  | State | Port             | Port State             |
|------------|-----------|-------|------------------|------------------------|
| -----      | -----     | ----- | -----            | -----                  |
| st.1       | HuntGroup | Down  | et.3.1<br>et.3.2 | Negotiate<br>Negotiate |

To show connection information for all SmartTRUNKs:

```
xp# smarttrunk show connections all-smarttrunks
```

| SmartTRUNK | Local Port | Remote Switch      | Remote Module | Remote Port | State |
|------------|------------|--------------------|---------------|-------------|-------|
| -----      | -----      | -----              | -----         | -----       | ----- |
| st.1       | et.2.1     | Enterasys A9:6E:57 | 3             | 1           | Up    |
| st.1       | et.2.2     | Enterasys A9:6E:57 | 3             | 2           | Up    |
| st.1       | et.2.3     | Enterasys A9:6E:57 | 3             | 3           | Up    |
| st.1       | gi.3.1     | Enterasys A9:6E:57 | 4             | 5           | Up    |
| st.2       | et.2.4     | --                 | --            | --          | Up    |
| st.2       | et.2.5     | --                 | --            | --          | Up    |
| st.2       | et.2.6     | --                 | --            | --          | Up    |

**Note:** In the example above, SmartTRUNK st.2 has no control protocol enabled, so no connection information is reported.



# Chapter 69

## snmp Commands

The **snmp** commands let you set and show SNMP parameters including SNMP community names and IP host targets for SNMP traps.

**Note:** In order to run NetFlow, you must enable SNMP.

### Command Summary

[Table 57](#) lists the **snmp** commands. The sections following the table describe the command syntax.

**Table 57. snmp Commands**

|   |
|---|
| <b>snmp disable trap authentication</b>   <b>link-up-down</b>   <b>frame-relay</b>   <b>ospf</b>   <b>spanning-tree</b>   <b>bgp</b>   <b>vrrp</b>   <b>environmentals</b>  |
| <b>snmp disable port-trap</b> <port list>   |
| <b>snmp set chassis-id</b> <chassis-name>   |
| <b>snmp set community</b> <community> <b>name</b> <community-name> <b>security-name</b> <security-name> <b>engine-id</b> <engine-id-string> <b>tag</b> <tag-string>   |
| <b>snmp set community-to-group</b> <security-name> <b>to</b> <group-name> [ <b>v1</b>   <b>v2c</b> ]  |
| <b>snmp set filter</b> <filter-name> <b>subtree</b> <OID> <b>mask</b> <mask-string> [ <b>category</b> <b>bgp</b>   <b>dot1dbridge</b>   <b>ds3</b>   <b>frame-relay-dte</b>   <b>interfaces</b>   <b>ipx</b>   <b>ospf</b>   <b>rmon</b>   <b>snmp</b>   <b>xp-enterprise</b>   <b>vrrp</b> ] [ <b>type</b> <b>included</b>   <b>excluded</b> ] |
| <b>snmp set group</b> <group-name> [ <b>v1</b>   <b>v2c</b>   <b>v3</b> [ <b>auth</b>   <b>noauth</b>   <b>priv</b> ]] <b>read</b> <readview> <b>write</b> <writeview> <b>notify</b> <notifyview>   |
| <b>snmp set if-alias</b> <interface-name> <b>alias</b> <alias-name>   |
| <b>snmp set mib name</b> <mib-name> <b>status</b> <b>enable</b>   <b>disable</b>  |

Table 57. snmp Commands

|   |
|---|
| <b>snmp set notify</b> <notify-name> <b>tag</b> <tag-string> [ <b>type</b> trap   inform]   |
| <b>snmp set retro-mib-ifspeed</b>   |
| <b>snmp set target</b> [<target-name>   <ip-address>] <b>ip-address</b> <ip-address><br><b>param</b> <param-name> <b>owner</b> <owner-name> [ <b>v1</b>   <b>v2c</b>   <b>v3</b> [ <b>auth</b>   <b>noauth</b>   <b>priv</b> ]]<br>[ <b>community</b> <community-name>   <b>security</b> <security-name>] <b>port</b> <udp-port><br><b>timeout</b> <timeout-value> <b>retries</b> <count> [ <b>type</b> traps   informs]<br><b>notifications</b> <notification-list> <b>tags</b> <tag-list> <b>mask</b> <mask-string> <b>mms</b> <mms-value><br>[ <b>status</b> enable   disable] |
| <b>snmp set target-params</b> <param-name> [ <b>v1</b>   <b>v2c</b>   <b>v3</b> [ <b>auth</b>   <b>noauth</b>   <b>priv</b> ]]<br><b>security-name</b> <security-name> <b>filter</b> <filter-name>  |
| <b>snmp set trap-source</b> <IPAddr>  |
| <b>snmp set user</b> <username> [ <b>engine-id</b> <id-string>   <b>local</b> ] [ <b>auth</b> md5  sha1] [ <b>priv</b> des]   |
| <b>snmp set user-to-group</b> <username> <b>to</b> <groupname>  |
| <b>snmp set view</b> <view-name> <b>subtree</b> <OID> <b>mask</b> <mask-string> [ <b>type</b> include  exclude]   |
| <b>snmp show</b> all  access  chassis-id  tftp  trap  community  statistics  mibs <br>{engine-id <IP_address>  <port>}  statistics  {user <user-name> [engine-id <id-string>  local] <br>all}  {group <group-name>  all}  {view <view-name>  all}  {target-params <params-name> <br>all}  {notify <notify-name>  all}  {filter <filter-name>  all}  |
| <b>snmp stop</b>  |
| <b>snmp test trap type</b> ps-failure  ps-recover  vrrpNewMaster  coldStart  linkDown  linkUp   |

# snmp disable trap

## Purpose

Disable specific SNMP trap types.

## Format

**snmp disable trap authentication| link-up-down| frame-relay| ospf| spanning-tree| bgp| vrrp| environmental**s

## Mode

Configure.

## Description

The **snmp disable trap** command controls the types of traps the X-Pedition router emits based trap type.

## Parameters

|                       |   |
|-----------------------|---|
| <b>authentication</b> | Disables authentication traps, which the X-Pedition router sends when it receives an invalid SNMP community string. |
| <b>link-up-down</b>   | Disables link-state change traps, which the X-Pedition router sends when a port's operational state changes.        |
| <b>frame-relay</b>    | DLCI up/down trap.  |
| <b>ospf</b>           | Sixteen different OSPF traps.   |
| <b>spanning-tree</b>  | NewRoot and topologyChange traps.   |
| <b>bgp</b>            | BGPEstablished and bgpBackwardTransistion traps   |
| <b>vrrp</b>           | NewMaster and authFailure traps.  |
| <b>environmentals</b> | Temperature, fan, and power supply traps  |

## Restrictions

None.

## snmp disable port-trap

### Purpose

Disable specific SNMP trap types for a specific port.

### Format

**snmp disable port-trap** *<port list>*

### Mode

Configure.

### Description

The **snmp disable port-trap** command controls the types of traps the X-Pedition router emits based trap type on specific ports. You can disable the following trap types on a per-port basis:

- Link-state change – use the **link-up-down** keyword to prevent the X-Pedition router from sending a trap each time a port changes operational state.

### Parameters

---

|                          |   |
|--------------------------|---|
| <i>&lt;port list&gt;</i> | Specifies the port(s) on which you wish to disable traps. |
|--------------------------|---|

---

### Restrictions

None.

## **snmp set chassis-id**

### **Purpose**

Set the X-Pedition chassis ID using SNMP.

### **Format**

**snmp set chassis-id** *<chassis-name>*

### **Mode**

Configure.

### **Description**

The **snmp set chassis-id** command lets you set a string to give the X-Pedition router an SNMP identity.

### **Parameters**

---

|                             |   |
|-----------------------------|---|
| <i>&lt;chassis-name&gt;</i> | Is a string describing the X-Pedition router. |
|-----------------------------|---|

---

### **Restrictions**

None.

# snmp set community

## Purpose

Set an SNMP community string and specify the access privileges for that string.

## Format

```
snmp set community <community> name <community-name> security-name <security-name>  
engine-id <engine-id-string> tag <tag-string>
```

## Mode

Configure.

## Description

The **snmp set community** command sets a community string for SNMP access to the X-Pedition router. SNMP management stations that want to access the router must supply a community string that is set on the switch. This command also sets the level of access to the router to read-only or read-write. Communities that are read-only allow SNMP *GETs* but not SNMP *SETs*. Communities that have read-write access allow both SNMP *GETs* and SNMP *SETs*.

## Parameters

|   |  |
|---|--|
| <b>community</b><br><community>         | Character string for the community string.   |
| <b>name</b><br><community-name>         | Enter a community name for this community entry. If not specified, it is the same as <community>.  |
| <b>security-name</b><br><security-name> | The security name used to map to an access group, which specifies the access rights. This is the security name used in the <b>snmp set community-to-group</b> command. If not specified, it is the same as the <name> value or <community> if name is not specified.               |
| <b>engine-id</b><br><engine-id-string>  | Identifies the SNMP entity for which this community is used. If not present, the local engine ID is used.  |
| <b>tag</b> <tag-string>                 | A tag value for this community entry. If specified, it limits community authentication to messages received from NMS entities whose transport address matches <b>snmp set target</b> commands with matching tag in the tag list. See <a href="#">snmp set target</a> on page 1180. |

## Restrictions

None.

## Example

To set the SNMP community string to “public,” which has read-only access:

```
xp(config)# snmp set community public privilege read
```

# snmp set community-to-group

## Purpose

Assigns an SNMP community to an SNMP group.

## Format

**snmp set community-to-group** <security-name> **to** <group-name> [**v1**| **v2c** ]

## Mode

Configure.

## Description

The **snmp set community-to-group** command allows you to assign an SNMP community to an SNMP group. Related commands include **snmp show**, **snmp set group**, and **snmp set community**.

## Parameters

|  |   |
|--|---|
| <b>community-to-group</b><br><security-name> | The security name of the community to assign.<br>See <a href="#">snmp set community on page 1166</a> .  |
| <b>to</b> <group-name>                       | Specify the name of the group to which you will assign the community.<br>The group name is specified with the <b>snmp set group</b> command.<br>See <a href="#">snmp set group on page 1171</a> . |
| <b>v1</b>   <b>v2c</b>                       | Specifies the security model for this community-to-group assignment.  |



# snmp set filter

## Purpose

Configures notification filters to include or exclude certain notifications.

## Format

**snmp set filter** *<filter-name>* **subtree** *<OID>* **mask** *<mask-string>* [**category** **bgp**| **dot1dbridge**| **ds3**| **frame-relay-dte**| **interfaces**| **ipx**| **ospf**| **rmon**| **snmp**| **xp-enterprise**| **vrp**] [**type** **included**| **excluded**]

## Mode

Configure.

## Description

The **snmp set filter** command configures notification filters to include or exclude certain notifications.

Also see [snmp show on page 1190](#) and [snmp set target-params on page 1183](#).

## Parameters

|  |  |   |
|--|--|---|
| <b>filter</b> <i>&lt;filter-name&gt;</i> | The name of the notification filter.   |   |
| <b>subtree</b> <i>&lt;OID&gt;</i>        | A string containing the OID value of the subtree.  |   |
| <b>mask</b> <i>&lt;mask-string&gt;</i>   | A bit string, represented by a hexadecimal representation of 1 to 16 characters, used to specify a mask that modifies which parts of the specified subtree are selected. |   |
| <b>category</b>                          | May be used instead of the subtree and mask options to select notifications by feature name. Enter one of the following keywords:  |   |
|  | <b>bgp</b>   | Border Gateway Protocol notifications                   |
|  | <b>dot1dbridge</b>   | Dot1d bridging notifications                            |
|  | <b>ds3</b>   | DS3/E3 WAN Interface notifications                      |
|  | <b>frame-relay-dte</b>   | Frame Relay DTE notifications                           |
|  | <b>interfaces</b>  | Generic interface notifications                         |
|  | <b>ipx</b>   | Novell IPX notifications                                |
|  | <b>ospf</b>  | Open Shortest Path First routing protocol notifications |
|  | <b>rmon</b>  | RMON alarm notifications                                |
|  | <b>snmp</b>  | SNMP Authentication notifications                       |
|  | <b>xp-enterprise</b>   | X-Pedition router-specific enterprise notifications     |
|  | <b>vrp</b>   | Virtual Router Redundancy Protocol notifications        |

| <b>type</b>     | Specifies whether or not the selected subtree is included in the filter.  |
|-----------------|---|
| <b>included</b> | The selected subtree is included in the filter (i.e., notifications that are part of the subtree will be filtered out). |
| <b>excluded</b> | The selected subtree is excluded from the filter (i.e., only notifications that are part of the subtree will be sent).  |

## Restrictions

None.

# snmp set group

## Purpose

To configure a new SNMP group or table that maps SNMP users to SNMP views.

## Format

```
snmp set group <group-name> [v1 | v2c | v3 [auth | noauth | priv]] read <readview>  
write <writeview> notify <notifyview>
```

## Mode

Configure.

## Description

The **snmp set group** command allows you to configure a new SNMP group or table that maps SNMP users to SNMP views. When configuring a group, you may specify only one security model per command. To configure a second set of views for the same group using a second security model, add another **snmp set group** command.

When a community string is configured internally, two groups with the name of the defined community string are automatically generated, one for the v1 security model and the other for the v2c security model. Similarly, deleting a community string will delete a v1 group with the name of the defined community string and a v2c group with the name of the community string.

Also see [snmp show on page 1190](#) and [snmp set user on page 1186](#).

## Parameters

|                           |  |
|---------------------------|--|
| <b>group</b> <group-name> | The name of the group  |
| <b>v1</b>                 | Members of this group authenticated using the SNMPv1 security model will use the read, write, and notify views specified.                        |
| <b>v2c</b>                | Members of this group authenticated using the SNMPv2c security model will use the read, write, and notify views specified.                       |
| <b>v3</b>                 | Members of this group authenticated using the SNMPv3 security model (USM) will use the read, write, and notify views specified.                  |
| <b>auth</b>               | Members of this group authenticated using one of the secure authentication security levels will use the read, write, and notify views specified. |

|                            |   |
|----------------------------|---|
| <b>noauth</b>              | Members of this group authenticated using the plaintext username authentication security level will use the read, write, and notify views specified.  |
| <b>priv</b>                | Members of this group authenticated using both secure authentication and privacy will use the read, write, and notify views specified.  |
| <b>read</b> <readview>     | This option allows you to specify a read view. Enter the name (a string up to 64 characters) of the view that enables you only to view the contents of the agent. By default, this value is the null OID  |
| <b>write</b> <writeview>   | This option allows you to specify a write view. Enter the name (a string up to 64 characters) of the view that enables you to enter data and configure the contents of the agent. By default, this value is the null OID. Write access must be configured explicitly. |
| <b>notify</b> <notifyview> | This option allows you to specify a notify view. Enter the name (a string up to 64 characters) of the view that enables you to specify a notify, inform, or trap. By default, this value is the null OID. Notify access must be configured explicitly.                |

## Restrictions

None.

# snmp set if-alias

## Purpose

Used to assign additional identification information to any interface handled by the ifXTable (i.e., physical ports, IP interfaces, IPX interfaces, VLANs, and SmartTRUNKs).

## Format

**snmp set if-alias** *<interface-name>* **alias** *<alias-name>*

## Mode

Configure.

## Description

Used primarily for administrative purposes, the ifAlias SNMP object allows you to assign additional identification information to any interface handled by the ifXTable (i.e., physical ports, IP interfaces, IPX interfaces, VLANs, and SmartTRUNKs). The X-Pedition router allows one alias assignment per interface and limits each alias to a maximum length of 64 characters. You may use a remote SNMP manager to view, add, change, or delete an alias.

To assign an alias, enter the following from configuration mode:

```
router(config)# snmp set if-alias <interface-name> alias <alias-name>
```

**Note:** You cannot remove an interface until you remove any alias assigned to the interface.

## Parameters

|                               |   |
|-------------------------------|---|
| <i>&lt;interface-name&gt;</i> | The name of an existing interface (i.e., physical port, IP interface, IPX interface, VLAN, or SmartTRUNK).  |
|                               | <b>Note:</b> Enterasys recommends that you use alphabetic characters when defining interface names—purely numeric interfaces will be interpreted as IP addresses. The X-Pedition router will display interface names up to 32 characters in length. |
| <i>&lt;alias-name&gt;</i>     | The name (up to 64 characters) of the alias you will assign to the interface.   |

## Restrictions

None.

## Examples

The following example demonstrates how to assign the alias “spare-port” to the physical port et.4.8.

```
router(config)# snmp set if-alias et.4.8 alias spare-port
```

The example below illustrates how to assign the alias “NEWALIAS” to the newly created “NEWIF” IP interface.

```
router(config)# interface create ip NEWIF address-netmask 10.0.0.1/8 port et.1.1  
router(config)# snmp set if-alias NEWIF alias NEWALIAS
```

# snmp set mib

## Purpose

Enables or disables a given MIB module in the SNMP agent.

## Format

**snmp set mib name** *<mib-name>* **status enable|disable**

## Mode

Configure.

## Description

The **snmp set mib** command allows you to enable or disable a particular MIB module in the SNMP agent.

## Parameters

---

|                            |   |  |
|----------------------------|---|--|
| <i>&lt;mib-name&gt;</i>    | Character string for the MIB module you wish to enable or disable. The following MIB modules are supported by the SNMP agent: |  |
| <b>LAG-MIB</b>             | IEEE 802.3ad LACP   |  |
| <b>SNMPv2-MIB</b>          | System and snmp group objects   |  |
| <b>EtherLike-MIB</b>       | IEEE 802.3 detailed ethernet statistics   |  |
| <b>IF-MIB</b>              | Interfaces group: ifTable, ifXTable, ifStackTable   |  |
| <b>IP-MIB</b>              | IP group containing global IP statistics  |  |
| <b>IP-FORWARD-MIB</b>      | IP CIDR Route Table   |  |
| <b>UDP-MIB</b>             | UDP statistics group  |  |
| <b>TCP-MIB</b>             | TCP Statistics group  |  |
| <b>BGP4-MIB</b>            | Border Gateway Protocol Version 4 mib   |  |
| <b>OSPF-MIB</b>            | OSPF Version 2 mib  |  |
| <b>RIPv2-MIB</b>           | RIP Version 2 mib   |  |
| <b>BRIDGE-MIB</b>          | Transparent layer 2 bridging protocol mib   |  |
| <b>FRAME-RELAY-DTE-MIB</b> | Frame Relay mib   |  |
| <b>PPP-LCP-MIB</b>         | Point to Point Link Control Protocol mib  |  |

|                               |  |
|-------------------------------|--|
| <b>PPP-IP-NCP-MIB</b>         | Point to Point IP Network Control Protocol           |
| <b>PPP-BRIDGE-NCP-MIB</b>     | Point to Point Bridge Control Protocol               |
| <b>DS1-MIB</b>                | Transmission statistics for DS1 serial line protocol |
| <b>DS3-MIB</b>                | Transmission statistics for DS3 serial line protocol |
| <b>SONET-MIB</b>              | Transmission statistics for SONET                    |
| <b>ATM-MIB</b>                | Transmission statistics for ATM                      |
| <b>RADIUS-AUTH-CLIENT-MIB</b> | Radius client protocol statistics                    |
| <b>RMON-MIB</b>               | Remote Monitoring for Layer 2 traffic                |
| <b>RMON2-MIB</b>              | Remote Monitoring for Layer 3/4 traffic              |
| <b>VRRP-MIB</b>               | Virtual Router Redundancy Protocol                   |
| <b>DVMRP-MIB</b>              | Distance Vector Multicast Routing Protocol           |
| <b>MAU-MIB</b>                | IEE 802.3 Medium Attachment Units (MIB)              |
| <b>APPLETALK-MIB</b>          | AppleTalk MIB II                                     |
| <b>FDDI-MIB</b>               | FDDI MIB   |
| <b>DEC-ELAN-EXT-MIB</b>       | DEC FDDI Extensions MIB                              |
| <b>NOVELL-RIPSAP-MB</b>       | Novell RIPSAP MIB                                    |
| <b>NOVELL-IPX-MIB</b>         | Novell IPX MIB                                       |
| <b>CDP-MIB</b>                | Cabletron Discovery Protocol                         |
| <b>POLICY-MIB</b>             | Policy Configuration MIB                             |
| <b>CONFIG-MIB</b>             | Configuration control mib                            |
| <b>HARDWARE-MIB</b>           | Chassis, environmental and inventory statistics      |
| <b>SERVICE-STATUS-MIB</b>     | Operational protocol statistics                      |
| <b>CAPACITY-MIB</b>           | Device capacity usage statistics                     |
| <b>CTRON-MIB2-MIB</b>         | Cabletron extension to MIB-II                        |
| <b>CTRON-CONTAINER-MIB</b>    | Cabletron container MIB                              |
| <b>CTRON-CHASSIS-MIB</b>      | Cabletron chassis MIB (6SSRM-02 only)                |
| <b>CT-DOWNLOAD-MIB</b>        | Cabletron download MIB                               |
| <b>OSPF-TRAP-MIB</b>          | MIB module to describe traps for OSPF Version 2      |
| <b>IGMP-STD-MIB</b>           | Internet Group Management Protocol MIB               |
| <b>IP-MROUTE-STD-MIB</b>      | IPv4 Multicast Routing MIB                           |
| <b>PIM-MIB</b>                | Protocol Independent Multicast MIB                   |

---



|                |  |  |
|----------------|--|--|
| <b>status</b>  | Specifies whether to enable or disable the MIB module: |  |
| <b>enable</b>  | Enables the MIB module                                 |  |
| <b>disable</b> | Disables the MIB module                                |  |

---

## Restrictions

None.

## Example

To enable the RMON2-MIB in the SNMP agent:

```
xp(config)# snmp set mib rmon2-mib status enable
```

# snmp set notify

## Purpose

The **snmp set notify** command allows you to associate a specific notification type with one or more targets.

## Format

**snmp set notify** <notify-name> **tag** <tag-string> [**type trap | inform**]

## Mode

Configure.

## Description

SNMP notifications can be sent as traps or informs. Traps are unreliable because the receiver does not send acknowledgments when it receives traps. The sender cannot determine if the traps were received. However, an SNMP entity that receives an inform request acknowledges the message with an SNMP response PDU. If the sender never receives the response, the inform request can be sent again. Thus, informs are more likely to reach their intended destination.

However, informs consume more resources in the agent and in the network. Unlike a trap, which is discarded as soon as it is sent, an inform request must be held in memory until a response is received or the request times out. Also, traps are sent only once, while an inform may be retried several times. The retries increase traffic and contribute to a higher overhead on the network.

Also see [snmp show on page 1190](#) and [snmp set target on page 1180](#).

## Parameters

|                             |   |               |
|-----------------------------|---|---------------|
| <b>notify</b> <notify-name> | The name of the notification.   |               |
| <b>tag</b> <tag-string>     | A string containing the tag value for this notification. Identifies the targets used when sending the notification. |               |
| <b>[type trap   inform]</b> | Specifies the type of notification.   |               |
|                             | <b>Trap</b>   | Send traps.   |
|                             | <b>Inform</b>   | Send informs. |

## Restrictions

None.

# **snmp set retro-mib-ifspeed**

## **Purpose**

Causes the ifSpeed for IP Interface rows to return speed of the first operational port. The default reported value is zero. This allows the ifSpeed to behave as it would in earlier versions of the MIB.

## **Format**

**snmp set retro-mib-ifspeed**

## **Mode**

Configure.

## **Description**

The **snmp set retro-mib-ifspeed** command causes the ifSpeed for IP Interface rows to return the speed of the first operational port.

## **Parameters**

None.

## **Restrictions**

None.

# snmp set target

## Purpose

Configures the recipient of an SNMP trap operation.

## Format

```
snmp set target [<target-name> | <ip-address>] ip-address <ip-address>  
param <param-name> owner <owner-name> [v1 | v2c | v3 [auth | noauth | priv]]  
[community <community-name> | security <security-name>] port <udp-port>  
timeout <timeout-value> retries <count> [type traps | informs] notifications <notification-list>  
tags <tag-list> mask <mask-string> mms <mms-value> [status enable | disable]
```

## Mode

Configure.

## Description

The **snmp set target** command configures the recipient of an SNMP trap operation (i.e., the IP address of the target server(s) to which you want the X-Pedition router to send SNMP traps). You may configure multiple targets with the same IP address and different security strings, but traps will not be sent to a target if the security string specified on the target is not configured. Trap targets are **enabled** by default but you can use the status argument to disable or re-enable a target. Also see [snmp show on page 1190](#), [snmp set target-params on page 1183](#), and [snmp set notify on page 1178](#).

### Notes:

- If you do not enter an snmp set target command, no notifications are sent. In order to configure the X-Pedition router to send SNMP notifications, you must enter at least one snmp set target command.
- In order to enable multiple targets, you must issue a separate snmp set target command for each target.
- If target-name is not explicitly specified, then the agent will generate a unique name that will be automatically assigned to the target.
- If no security model is specified, either explicitly or through an associated target-parameters entry, SNMPv1 will be used. If no community string is specified, explicitly or through an associated target-parameters entry, “public” will be used.
- If the param option is specified, then the security level and community string are not used. Similarly, if the type option is specified, then the notification list is not used.

## Parameters

|   |   |  |
|---|---|--|
| <b>target</b> [<target-name>  <ip-address>]                                       | String containing the target name.  |  |
| <b>ip-address</b><br><IP-address>   | The IP Address of the target system. By default, <b>192.168.1.1</b> .   |  |
|   | <b>Note:</b>  | The target IP address should be locally attached to the X-Pedition router.   |
| <b>param</b><br><param-name>  | String containing the name of the associated target parameters. This can be used to link this target with an snmp set target-params command as a convenient way of grouping multiple snmp set target commands with the same set of parameters used for creating trap or inform messages. The security model, security level, and community are defined by the snmp set target-params command. By default, <i>param-name</i> is the same as <i>target-name</i> . |  |
| <b>owner</b><br><owner-name>  | The name (a string value) of the creator/owner of the target. By default, the owner-string value is “ <b>monitor</b> .”   |  |
| <b>[v1  v2c  v3 [auth  noauth  priv]]</b>   | <b>v1</b>   | Specifies that the SNMPv1 security model should be used when communicating with this target.                             |
|   | <b>v2c</b>  | Specifies that the SNMPv2c security model should be used when communicating with this target.                            |
|   | <b>v3</b>   | Specifies that the SNMPv3 security model (USM) should be used when communicating with this target.                       |
|   | <b>auth</b>   | One of the secure authentication protocols will be used when v3 is specified.  |
|   | <b>noauth</b>   | Plaintext username authentication will be used when v3 is specified.   |
|   | <b>priv</b>   | Encryption will be used, in addition to one of the secure authentication protocols, when communicating with this target. |
| <b>[community</b><br><community-name><br><b>security-name</b><br><security-name>] | The security name to use to authenticate with the target. This can be an SNMP community string or an SNMP user name.  |  |
| <b>port</b> <udp-port>  | The destination UDP port on the target to which to send the trap or informs. The default udp port is <b>162</b> .   |  |
| <b>timeout</b><br><time-value>  | The inform response timeout value (in hundredths of seconds). By default, <i>time-value</i> = <b>1500</b> .   |  |
| <b>retries</b> <count>  | The number of retries when there is no response to an inform. The default value is <b>3</b> .   |  |

|   |   |   |
|---|---|---|
| <b>[type traps  informs]</b>                | The type of notification to send. (not used when <i>notifications</i> is specified).  |   |
|   | <b>Traps</b>  | Send traps.                             |
|   | <b>Informs</b>  | Send informs.                           |
| <b>notifications</b><br><notification-list> | A list of notify tag-string values used to associate a notify entry or a group of notify entries with this target (do not use with the <i>type</i> option). By default, this value is <b>defaultTrap</b> .  |   |
| <b>tags</b> <tag-list>                      | The list of tags associated with notifications or communities which reference this target. When specifying multiple tags, use quotes around the tag list and separate each tag name with a space. Use this parameter in place of the “notifications” option.  |   |
| <b>mask</b> <mask-string>                   | Mask to be used when this target is selected by an SNMPv1 or SNMPv2c community tag. Specify using hexadecimal representation. Contains one bit for each bit in the ip-address and port values (4 bytes of ip-address : 2 bytes for port value).<br><br>Example: 0xff:ff:ff:00:ff:ff<br><br>For each bit set to one, the target address/port must match the from transport address/port on an incoming message. For each bit set to zero, no match is required. This parameter allows one target to specify multiple transport addresses. If a mask is not specified, a value of all ones is used. |   |
| <b>mms</b> <mms-value>                      | The maximum size PDU that can be received from or sent to this target. Enter a value equal to or greater than 484. If not specified, 2048 is used.  |   |
| <b>status enable   disable</b>              | Target status.  |   |
|   | <b>disabled</b>   | Target currently not available for use. |
|   | <b>enabled</b>  | Target enabled.                         |

## Restrictions

None.

# snmp set target-params

## Purpose

The **snmp set target-params** command allows you to configure PDU generation parameters for use by the **snmp set target** command.

## Format

```
snmp set target-params <param-name> [v1 | v2c | v3 [auth | noauth | priv]]  
security-name <security-name> filter <filter-name>
```

## Mode

Configure.

## Description

Use the **snmp set target-params** configuration command to group multiple targets with the same trap/inform message generation parameters to one configuration statement. The **snmp set target** command need not specify the parameters in the **snmp set target-params** configuration command. Instead, specify the desired parameters using the param option to reference an **snmp set target-params** configuration command. Also see [snmp show on page 1190](#), [snmp set target on page 1180](#), and [snmp set filter on page 1169](#).

## Parameters

|                                      |  |
|--------------------------------------|--|
| <b>target-params</b><br><param-name> | The name of the target parameters.   |
| <b>v1</b>                            | Specifies that targets associated with this target-params entry will use the SNMPv1 security model.  |
| <b>v2c</b>                           | Specifies that targets associated with this target-params entry will use the SNMPv2c security model.   |
| <b>v3</b>                            | Specifies that targets associated with this target-params entry will use the SNMPv3 security model (USM).<br><br><b>auth</b> For SNMPv3, specifies that one of the secure authentication protocols is to be used.<br><br><b>noauth</b> For SNMPv3, specifies that plaintext username authentication is to be used.<br><br><b>priv</b> For SNMPv3, specifies that encryption is to be used in addition to one of the secure authentication protocols. |

|   |  |
|---|--|
| <b>security-name</b><br><security-name> | The security name to use to authenticate with the target. This can be an SNMP community string or an SNMP user name. |
| <b>filter</b> <filter-name>             | The name of the notification filter to apply when sending notifications to associated targets.                       |

## Restrictions

None.



# snmp set trap-source

## Purpose

Sets the source interface IP address reported in traps sent by the SNMP Agent.

## Format

**snmp set trap-source** <IPaddr>

## Mode

Configure.

## Description

The **snmp set trap-source** command configures the IP address reported in traps sent by the SNMP Agent.

## Parameters

---

|          |                 |
|----------|-----------------|
| <IPaddr> | The IP address. |
|----------|-----------------|

---

## Restrictions

None.

# snmp set user

## Purpose

To configure a new SNMP user.

## Format

**snmp set user** <username> [**engine-id** <id-string> | **local**] [**auth md5| sha1**] [**priv des**]

## Mode

Configure.

## Description

The **snmp set user** command allows you to configure a new SNMP user. When creating a user, use the engine-id option to localize the user for use with a specific SNMP engine and to specify any additional authentication or encryption options to be used with that SNMP engine. Once the user has been created, use the **snmp set user-to-group** command to assign the user to a group.

Related commands include [snmp show on page 1190](#), [snmp set user-to-group on page 1188](#), and [snmp set group on page 1171](#).

**Note:** When you use the **comment out** command to disable an **snmp set user** command, the X-Pedition router will delete the passwords for that user. If you attempt to reactivate the command through the **comment in** command, the **snmp set user** command will fail and you will need to re-enter the command and create a new account for the user. To disable users and prevent them from accessing the X-Pedition router through SNMP, **comment out** the user's corresponding **snmp set user-to-group** command. This will prevent you from having to recreate user accounts.

## Parameters

|                              |  |
|------------------------------|--|
| <b>user</b> <username>       | The name of the user.  |
| <b>engine-id</b> <id-string> | Identifies a remote SNMP Engine-ID.                                    |
| <b>local</b>                 | Specifies the local agent's SNMP Engine-ID.                            |
| <b>auth</b>                  | Configures the user to use one of the secure authentication protocols. |
| <b>md5</b>                   | Specifies use of the HMAC-MD5-96 secure authentication protocol.       |
| <b>sha1</b>                  | Specifies use of the HMAC-SHA-96 secure authentication protocol.       |

---

|             |   |
|-------------|---|
| <b>priv</b> | Configures the user to use encryption for privacy, in addition to one of the secure authentication protocols. |
| <b>des</b>  | Specifies use of the CBC-DES encryption algorithm.<br>This is the default value.                              |

---

## Restrictions

None.

# snmp set user-to-group

## Purpose

Assigns an SNMP user to an SNMP group.

## Format

**snmp set user-to-group** <username> **to** <groupname>

## Mode

Configure.

## Description

The **snmp set user-to-group** command allows you to assign an SNMP user to an SNMP group. Related Commands include [snmp show on page 1190](#), [snmp set user on page 1186](#), and [snmp set group on page 1171](#).

## Parameters

|                                    |  |
|------------------------------------|--|
| <b>user-to-group</b><br><username> | The name of the user.                                    |
| <b>to</b> <groupname>              | The name of the group to which you will assign the user. |

## Restrictions

None.

# snmp set view

## Purpose

Configure a new view.

## Format

**snmp set view** <view-name> **subtree** <OID> **mask** <mask-string> [**type include**| **exclude**]

## Mode

Configure.

## Description

The **snmp set view** command allows you to configure a view that may be referenced by a group. Also see [snmp show](#) on page 1190 and [snmp set group](#) on page 1171.

## Parameters

|                                      |  |
|--------------------------------------|--|
| <b>snmp set view</b><br><view-name>  | The name of the view.  |
| <b>subtree</b> <OID>                 | A string specifying the OID of the subtree.  |
| <b>mask</b> <mask-string>            | Specifies a mask that modifies which parts of the specified subtree are selected. A bit string containing the mask is a hexadecimal representation of 1 to 16 characters.                            |
| <b>type include</b>   <b>exclude</b> | Specifies whether or not the selected subtree is included in the view.<br><br><b>Include</b> Include the selected subtree in the view.<br><b>Exclude</b> Exclude the selected subtree from the view. |

## Restrictions

None.

# snmp show

## Purpose

Shows SNMP information.

## Format

```
snmp show all| access| chassis-id| tftp| trap| community| statistics| mibs|  
{engine-id <IP_address>| <port>}| statistics| {user <user-name> [engine-id <id-string>| local]|  
all}| {group <group-name>| all}| {view <view-name>| all}| {target-params <params-name>| all}|  
{notify <notify-name>| all}| {filter <filter-name>| all}| {target-addr <target-name>}
```

## Mode

Enable.

## Description

The **snmp show** command allows you to display the following SNMP information:

- Five most recent clients to access the X-Pedition router
- SNMP name
- Tftp SNMP status
- Trap target related configuration
- Community strings
- SNMP statistics
- MIB registry
- Local SNMP engine and all remote engines configured on the device
- Agent statistics
- Name of user whose SNMP information is displayed
- Engine ID
- Name of group for which SNMP information is displayed
- VACM views
- Trap and inform target parameters
- Notification entries
- Notification filters
- SNMP target information

## Parameters

|   |   |  |
|---|---|--|
| <b>all</b>  | Displays all SNMP information (equivalent to specifying all the other keywords).  |  |
| <b>access</b>   | Displays the last five SNMP clients to access the X-Pedition router.  |  |
| <b>chassis-id</b>   | Displays the X-Pedition SNMP name.  |  |
| <b>tftp</b>   | Show tftp SNMP status.  |  |
| <b>trap</b>   | Displays the IP address of the trap target server.  |  |
| <b>community</b>  | Displays the X-Pedition community string.   |  |
| <b>statistics</b>   | Displays SNMP statistics.   |  |
| <b>mibs</b>   | Displays the SNMP MIB registry.   |  |
| <b>{engine-id</b><br><b>&lt;IP_address&gt; </b><br><b>&lt;port&gt;}</b>           | For information about similar commands, see <a href="#">snmp set user on page 1186</a> and <a href="#">snmp set target on page 1180</a> .   |  |
|   | <b>&lt;IP_address&gt;</b>   | Specify an IP Address if you would like to display the remote engine-id of an SNMP entity at a particular IP address. If the SNMP agent already knows the engine-id of the entity at that address, it will display in the table. If the SNMP agent does not know the engine-id, it will attempt to discover the engine-id by sending a discovery packet to the IP address. If the router receives a valid reply to a discover request, it will add the engine-id to an internal table and the following errorlog message will appear:<br><br>%SNMP-I-ENGINE_DSCRVD, SNMP has just discovered an engine-id for: 10.136.136.210 Engine-ID = 0x80:00:07:e5:80:09:86:da:7f:92:1b:58:3d |
|   | <b>&lt;port&gt;</b>   | By default, the X-Pedition router monitors engine-ids on UDP trap port 162. Use the port option if the SNMP entity is configured to listen to traps on a different UDP port. This will cause the router to search for the IP Address / Port pair in the internal table or to place the specified port in the discovery packet.   |
| <b>statistics</b>   | View statistics for the SNMP agent.   |  |
| <b>user</b> <user-name><br><b>[engine-id</b><br><b>&lt;id-string&gt;   local]</b> | <user-name>   | The name of the user whose SNMP information you will display. Use the keyword <b>all</b> to view information about all users.  |
|   | <id-string>   | The host on which the user is defined. Also see <a href="#">snmp set user on page 1186</a> .   |
| <b>group</b> <group-name>   | The name of the group for which you will view the SNMP information. Use the <b>all</b> keyword to view information about all groups. Also see <a href="#">snmp set group on page 1171</a> . |  |

|                                    |  |
|------------------------------------|--|
| <b>view</b> <view-name>            | Display information about a specific SNMP VACM view. Use the <b>all</b> keyword to view information about all views. Also see <a href="#">snmp set view on page 1189</a> .   |
| <b>target-params</b> <params-name> | Display information about a specific set of SNMP trap and inform target parameters. Use the <b>all</b> keyword to view information about all target parameters. Also see <a href="#">snmp set target-params on page 1183</a> . |
| <b>notify</b> <notify-name>        | Display information about a specific SNMP notification entry. Use the <b>all</b> keyword to view information about all notification entries. Also see <a href="#">snmp set notify on page 1178</a> .                           |
| <b>filter</b> <filter-name>        | Display information about SNMP notification filters. Use the <b>all</b> keyword to view information about all notification filters. Also see <a href="#">snmp set filter on page 1169</a> .                                    |
| <b>target-addr</b> <target-name>   | Displays information about a specific set of SNMP targets. Use the <b>all</b> keyword to display information about all targets.  |

## Restrictions

None.

## Examples

The following examples depict sample output of each **show** command option.

### Example 1

The following **snmp show access** command displays a log of SNMP access to the X-Pedition router. The host that accessed the X-Pedition router and the X-Pedition system time when the access occurred are listed.

```
xp(config)# snmp show access
SNMP Last 5 Clients:
  10.15.1.2      Wed Feb 7 18:42:59 2001
  10.15.1.2      Wed Feb 7 18:42:55 2001
  10.15.1.2      Wed Feb 7 18:42:56 2001
  10.15.1.2      Wed Feb 7 18:42:57 2001
  10.15.1.2      Wed Feb 7 18:42:58 2001
```



**Example 2**

To display the SNMP identity of the X-Pedition router:

```
xp(config)# snmp show chassis-id
```

```
SNMP Chassis Identity:
s/n 123456
```

**Example 3**

To display the IP address of the trap target server:

```
xp(config)# snmp show trap
```

```
Trap Table:
```

| Index | Trap | Target    | Addr | Community String | Status   |
|-------|------|-----------|------|------------------|----------|
| 1.    |      | 10.15.1.2 |      | public           | enabled  |
| 2.    |      | 1.2.3.4   |      | public123        | disabled |
| 3.    |      | 5.6.7.8   |      | public20         | disabled |

**Example 4**

The following example shows 0x80:00:15:F8:03:00:00:1D:5F:00:1E as the local Engine-ID and 0x12:34:56:78:9A:BC:DE:F0:00:00:00:00 as the remote Engine-ID, 171.69.37.61 as the IP address of the remote engine, or copy of SNMP, and 162 as the port on the remote device to which the local device connects.

```
router# snmp show engine-id
```

```
Local SNMP engineID: 0x80:00:15:f8:03:00:00:1D:5F:00:1E
Remote Engine ID      IP-addr      Port
0x12:34:56:78:9A:BC:DE:F0:00:00:00:00  171.69.37.61  162
```

**Field Descriptions**

|                             |   |
|-----------------------------|---|
| <b>Local SNMP engine ID</b> | A string that identifies the copy of SNMP on the local device.  |
| <b>Remote Engine ID</b>     | A string that identifies the copy of SNMP on the remote device. |
| <b>IP-addr</b>              | The IP address of the remote device.                            |
| <b>Port</b>                 | The port number on the remote device.                           |

**Example 5**

To display the statistics for the SNMP agent, use the **snmp show statistics** command.

```
router# snmp show statistics

SNMP Statistics:
  7 packets received
  7 in get objects processed
  0 in get requests
  0 in get responses
  7 get-next requests
  0 in set requests
  0 in total objects set
  0 bad SNMP versions
  0 bad community names
  0 ASN.1 parse errors
  0 PDUs too big
  0 no such names
  0 bad values
  0 in read onlys
  0 in general errors
  0 silent Drops
  0 packets sent
  0 out get requests
  0 get-next responses
  0 out set requests
  0 response PDUs too big
  0 no such name errors
  0 bad values
  0 general errors
  0 version 1 traps sent
  0 traps in queue
  0 traps dropped due to queue overflow

SNMPv3 Engine Stats:
  20 engine boots
  01:24:11 engine time

SNMPv3 Message Processing Stats:
  0 unknown security models
  0 invalid messages
  0 unknown PDU handlers
  0 unavailable contexts
  0 unknown contexts

User Security Model stats:
  0 unsupported security levels
  0 not in time window
  0 unknown users names
  0 unknown engine ids
  0 wrong digests
  0 decryption errors
```

### Field Descriptions

|                                    |   |
|------------------------------------|---|
| <b>Engine boots</b>                | The number of times the SNMP engine has re-initialized since initial configuration.                         |
| <b>Engine time</b>                 | The time since engine boots was last incremented.   |
| <b>Unknown security models</b>     | The number of packets dropped because they referenced a security model which is not known or not supported. |
| <b>Invalid messages</b>            | The number of packets dropped because there were invalid or inconsistent components in the packet.          |
| <b>Unknown PDU handlers</b>        | The number of packets dropped because no application existed to process the PDU.                            |
| <b>Unavailable contexts</b>        | The number of packets dropped because the context in the message was unavailable.                           |
| <b>Unknown contexts</b>            | The number of packets dropped because the context in the message was unknown.                               |
| <b>Unsupported security levels</b> | The number of packets dropped because they requested a security level that was unknown or unavailable.      |
| <b>Not in time window</b>          | The number of packets dropped because they appeared outside of the authoritative SNMP engine's time window. |
| <b>Unknown users names</b>         | The number of packets dropped because they referenced a unknown user.                                       |
| <b>Unknown engine ids</b>          | The number of packets dropped because they referenced an snmpEngineID that was not known.                   |
| <b>Wrong digests</b>               | The number of packets dropped because they did not contain the expected digest value.                       |
| <b>Decryption errors</b>           | The number of packets dropped because they could not be decrypted.  |

**Example 6**

To display information on SNMP users in the USM user table, use the **snmp show user** command. The following example shows the username as “authuser,” the Engine-ID as 0x00:00:00:09:02:00:00:00:0C:02:58:08, the authentication protocol as sha1, no privacy protocol, and the storage-type as nonVolatile:

```
router# snmp show user authuser

user name:  authuser
engine id:  0x00:00:00:09:02:00:00:00:0C:02:58:08
auth type:  sha1
priv type:  none
storage-type: nonVolatile
```

**Field Descriptions**

|                     |   |
|---------------------|---|
| <b>User name</b>    | A string identifying the name of the SNMP user.   |
| <b>Engine id</b>    | A string identifying the name of the copy of SNMP on the device.  |
| <b>Auth type</b>    | The authentication protocol the user is configured to use, either MD5, SHA1, or none.   |
| <b>Priv type</b>    | The privacy protocol the user is configured to use, either DES or none.   |
| <b>Storage-type</b> | Indicates whether the settings have been set in volatile or temporary memory on the device, or in non-volatile or persistent memory where settings will remain after the device has been turned off and on again. |

**Example 7**

The **snmp show group** example below shows the group name as public, the security model as v1, the security level as noauth the read view name as v1default, no write view, the notify view name as v1notify, and the storage type as volatile:

```
router# snmp show group public

groupname:  public          security model: v3 noAuth
readview:   v1default
writeview:
notifyview: v1notify
storage-type: volatile
```

### Field Descriptions

|                       |   |
|-----------------------|---|
| <b>Groupname</b>      | The name of the SNMP group, or collection of users who have a common access policy.   |
| <b>Security model</b> | The security model used by the group, either v1, v2c, or v3.  |
| <b>Readview</b>       | A string identifying the read view of the group.  |
| <b>Writeview</b>      | A string identifying the write view of the group.   |
| <b>Notifyview</b>     | A string identifying the notify view of the group.  |
| <b>Storage-type</b>   | Indicates whether the settings have been set in volatile or temporary memory on the device, or in non-volatile or persistent memory where settings will remain after the device has been turned off and on again. |

### Example 8

The **snmp show view** example below shows the view name as internet, the subtree as 1.3.6.1, no mask, and the storage type as permanent:

```
router# snmp show view internet
```

```
viewname:      internet
subtree:       1.3.6.1
mask:
type:          include
storage-type:  permanent
```

### Field Descriptions

|                     |  |
|---------------------|--|
| <b>Viewname</b>     | The name of the view.  |
| <b>Subtree</b>      | The string indentifying the subtree oid.   |
| <b>Mask</b>         | A string identifying the mask associated with the subtree.   |
| <b>Type</b>         | The type of view: <i>included</i> or <i>excluded</i> .   |
| <b>Storage-type</b> | Indicates whether the settings have been set in volatile or temporary memory on the device, or in non-volatile or persistent memory where settings will remain after the device has been turned off and on again. You may modify but not remove permanent entries. |

**Example 9**

The **snmp show target-params** example below shows the target parameters name as publicTargets, the security level as v1, the security name as public, and the storage type as nonVolatile:

```
router# snmp show target-params publicTargets
```

```
params name:  publicTargets
security level:  v1
security name:  public
storage-type:  nonVolatile
```

**Field Descriptions**

|                       |   |
|-----------------------|---|
| <b>Params name</b>    | The name of the target parameters.  |
| <b>Security level</b> | The security model and security level specified by the target parameters.   |
| <b>Security name</b>  | The security name specified by the target parameters. Depending on the security model this will either be a community string or a username.   |
| <b>Storage-type</b>   | Indicates whether the settings have been set in volatile or temporary memory on the device, or in non-volatile or persistent memory where settings will remain after the device has been turned off and on again. |

**Example 10**

The **snmp show notify** example below shows the notification entry name as defaultTrap, the notify tag as defaultTrap, the notify type as trap, and the storage type as permanent:

```
router# snmp show notify defaultTrap
```

```
notify name:  defaultTrap
notify tag:    defaultTrap
notify type:  trap
storage-type:  permanent
```

**Field Descriptions**

|                    |  |
|--------------------|--|
| <b>Notify name</b> | The name of the notification entry.  |
| <b>Notify tag</b>  | The tag used to associate targets with the notification entry.   |
| <b>Notify type</b> | The types of notifications, either traps or informs, to be sent to targets associated with the notification entry. |

|                     |   |
|---------------------|---|
| <b>Storage-type</b> | Indicates whether the settings have been set in volatile or temporary memory on the device, or in non-volatile or persistent memory where settings will remain after the device has been turned off and on again. |
|---------------------|---|

### Example 11

The **snmp show filter** example below shows the notification filter name as noBGP, the subtree as 1.3.6.1.2.1.15, no mask, the filter type as included, and the storage type as volatile:

```
router# snmp show filter noBGP

filter name:      noBGP
subtree:          1.3.6.1.2.1.15
mask:
filter type:      included
storage-type:     volatile
```

### Field Descriptions

|                     |  |
|---------------------|--|
| <b>Filter name</b>  | The name of the notification filter.   |
| <b>Subtree</b>      | The OID subtree that is included in, or excluded from, the filter.   |
| <b>Mask</b>         | The mask used to modify which parts of the subtree are selected.   |
| <b>Filter type</b>  | Shows whether the filter includes or excludes the selected subtree. If the subtree is included in the filter, notifications that are part of the subtree will be filtered out. If the subtree is excluded from the filter, only notifications that are part of the subtree will be sent. |
| <b>Storage-type</b> | Indicates whether the settings have been set in volatile or temporary memory on the device, or in non-volatile or persistent memory where settings will remain after the device has been turned off and on again.  |

**Example 12**

The following example displays information about the SNMP target *target1*.

```
xp# snmp show target-addr target1
```

```
addr name:          target1
ip addr:            134.141.136.193/0162
timeout:           1500
retry count:        3
tag-list:           mytag defaultTrap
params:            target1
tmask:             0xff:ff:ff:ff:00:00
max msg size:       2048
storage-type:       volatile
```

**Field Descriptions**

|              |  |
|--------------|--|
| addr name    | The name of the target.  |
| ip addr      | The IP address and UDP port number of the target.  |
| timeout      | The timeout value used when retrying informs.  |
| retry count  | The number of times to retry an inform.  |
| tag-list     | A list of tags associated with notify or community command tags.   |
| params       | The associated target-params command.  |
| tmask        | A mask used to determine which bits of the IP address/port are<br> used when matching a community tag.   |
| max msg size | The maximum allowed message size for this target.  |
| storage-type | Indicates whether the settings have be set in volatile or<br> temporary memory on the device, or in non-volatile or persistent<br> memory where settings will remain after the device has been<br> reset or turned off and on again. |



## **snmp stop**

### **Purpose**

Stop SNMP access to the device.

### **Format**

**snmp stop**

### **Mode**

Configure.

### **Description**

The **snmp stop** command stops SNMP access to the X-Pedition router. The X-Pedition router will still finish all active requests but will then disregard future requests. When you issue this command, UDP port 161 is closed.

### **Parameters**

None.

### **Restrictions**

None.

## snmp test trap

### Purpose

Tests SNMPv1 notifications to currently configured managers.

### Format

**snmp test trap type** **ps-failure**| **ps-recover**| **vrrpNewMaster**| **coldStart**| **linkDown** |**linkUp**

### Mode

Enable.

### Description

The **snmp test trap** command allows you to test the SNMPv1 notifications to the managers currently configured.

### Parameters

|                      |  |
|----------------------|--|
| <b>ps-failure</b>    | Tests the power supply failure trap notification.    |
| <b>ps-recover</b>    | Tests the power supply recover trap notification.    |
| <b>vrrpNewMaster</b> | Tests the Virtual Router Redundancy New Master Trap. |
| <b>coldStart</b>     | Send coldStart trap to manager.                      |
| <b>linkDown</b>      | Send link down for ifIndex 1 to manager.             |
| <b>linkUp</b>        | Send link up for ifIndex 1 to manager.               |

### Restrictions

None.

# Chapter 70

## sonet Commands

The **sonet** commands configure and display various parameters for Synchronous Optical Network (SONET) encapsulation. These commands allow you to accommodate Packet-over-SONET (POS) and ATM (asynchronous transfer mode) transmission using the X-Pedition router.

Packet-over-SONET technology provides the ability to transmit IP packets and ATM cells over a SONET backbone by encapsulating them into a SONET frame. In reference to the OSI Layer model, the SONET layer rests right beneath the IP layer or the ATM layer. Based on the transmission mechanism of SONET frames, the result is larger traffic bandwidth and faster line speed (OC-3), accommodating QoS guarantees and the ability to deliver voice/video data over an internetwork.

SONET frames carry a large amount of data stored as overhead. This overhead information provide the information for OAM&P (operation, administration, management, and provisioning) capabilities, such as performance monitoring, automatic protection switching, and path tracing.

The Enterasys SONET technology features Automatic Protection Switching, performance monitoring capabilities, as well as commercial circuit identification.

## Command Summary

[Table 58](#) lists the **sonet** commands. The sections following the table describe the command syntax.

### Notes:

- The X-Pedition router does *not* support PVST over POS. However, the router *will* support STP over POS.
- A hardware limitation allows FDDI and SONET modules to increment only the *ifInUcastPkts* and *ifOutUcastPkts* ifMib counters. Non-unicast packet counters (i.e., *ifInNUcastPkts* and *ifOutNUcastPkts*) do not increment and will remain 0.

On gigabit and 10-Gigabit modules, all OCMAC counters increment correctly.

Table 58. sonet Commands

|   |
|---|
| <b>sonet set</b> <SONET ports> <b>C2</b> <num>  |
| <b>sonet set</b> <SONET ports> <b>circuit-id</b> <string>   |
| <b>sonet set</b> <SONET ports> <b>fcs-16-bit</b>  |
| <b>sonet set</b> <SONET ports> <b>framing sonet</b>   <b>sdh</b>  |
| <b>sonet set</b> <SONET ports> <b>J0</b> <num>  |
| <b>sonet set</b> <SONET ports> <b>loopback none</b>   <b>line-facility</b>   <b>serial-terminal</b>   <b>parallel</b> |
| <b>sonet set</b> <SONET ports> <b>path-trace</b> <string>   |
| <b>sonet set</b> <SONET ports> <b>payload-scramble on</b>   <b>off</b>  |
| <b>sonet set</b> <SONET ports> <b>protected-by</b> <SONET port>   |
| <b>sonet set</b> <SONET ports> <b>protection 1+1</b>  |
| <b>sonet set</b> <SONET ports> <b>protection-switch lockoutprot</b>   <b>forced</b>   <b>manual</b>                   |
| <b>sonet set</b> <SONET ports> <b>revertive off</b>   <b>on</b>   |
| <b>sonet set</b> <SONET ports> <b>S1S0</b> <num>  |
| <b>sonet set</b> <SONET ports> <b>sd-ber</b> <num>  |
| <b>sonet set</b> <SONET ports> <b>sf-ber</b> <num>  |
| <b>sonet set</b> <SONET ports> <b>sts-stream-scramble on</b>   <b>off</b>   |
| <b>sonet set</b> <SONET ports> <b>WTR-timer</b> <num>   |
| <b>sonet show aps</b> <SONET ports>   |
| <b>sonet show loopback</b> <SONET ports>  |
| <b>sonet show medium</b> <SONET ports>  |
| <b>sonet show pathtrace</b> <SONET ports>   |

# sonet set C2

## Purpose

Sets a value for the C2 flag.

## Format

**sonet set** <SONET ports> **C2** <num>

## Mode

Configure.

## Description

The **sonet set C2** command allows you to specify a value for the C2 flag. SONET frames carry overhead for path, section and line for easier multiplexing and better OAM&P (operation, administration, management, and provisioning) capabilities.

The SONET frame overhead information is stored in separate bytes, or flags.

There are nine bytes allocated for section overhead labeled A1, A2, B1, D1, D2, D3, E1, F1, J0/Z0.

There are 18 bytes allocated for line overhead labeled H1, H2, H3, B2, K1, K2, D4, D5, D6, D7, D8, D9, D10, D11, D12, S1/Z1, M0/M1, and E2.

There are nine bytes allocated for path overhead labeled J1, B3, C2, H4, G1, P2, Z3, Z4, and Z5.

The **sonet set C2** command sets the C2 flag. The C2 flag is the path signal label byte used to indicate the contents of the synchronous payload envelope.

## Parameters

|               |   |
|---------------|---|
| <SONET ports> | Specifies the SONET port name(s).   |
| <num>         | Specifies the value of the C2 flag. Specify any number between 0 and 255. |

## Restrictions

None.

## **Example**

To set the C2 flag to 16 on port so.2.1:

```
xp(config)# sonet set so.2.1 C2 16
```

# sonet set circuit-id

## Purpose

Sets a circuit identifier.

## Format

**sonet set** <SONET ports> **circuit-id** <string>

## Mode

Configure.

## Description

The **sonet set circuit-id** command allows you to set a circuit identifier on a specified SONET port. This command is for administrative purposes, used to identify this line and associate it with a certain customer circuit. Primarily used for service level management.

## Parameters

|               |  |
|---------------|--|
| <SONET ports> | Specifies the SONET port name(s).  |
| <string>      | Specifies the circuit identifier. The maximum length must be 64 bytes or less. |

## Restrictions

None.

## Example

To identify the circuit line on port so.2.1 to as 'customer1':

```
xp(config)# sonet set so.2.1 circuit-id customer1
```

## sonet set fcs-16-bit

### Purpose

Sets the frame check sequence to 16 bits.

### Format

**sonet set** <SONET ports> **fcs-16-bit**

### Mode

Configure.

### Description

The **sonet set fcs-16-bit** command allows you to set the frame check sequence (FCS) field length of the SONET frame to 16 bits. By default, this field length is set to 32 bits (4 octets). Using this command, you can set the frame check sequence field length to 16 bits (2 octets) instead.

The FCS field is used as an error check mechanism during frame transmission. An FCS value is calculated before transmission based on destination address, source address, and other data inside the frame. The FCS field inside the SONET frame carries this value. After the frame arrives to the destination, the FCS value is calculated again and compared with the value in the FCS field. This is done to ensure that there was no errors during transmission.

### Parameters

---

|               |                                   |
|---------------|-----------------------------------|
| <SONET ports> | Specifies the SONET port name(s). |
|---------------|-----------------------------------|

---

### Restrictions

None.

### Example

To set the frame check sequence on port so.2.1 to 16 bits:

```
xp(config)# sonet set so.2.1 fcs-16-bit
```



## sonet set framing

### Purpose

Sets optical framing for SONET or SDH.

### Format

**sonet set** <SONET ports> **framing sonet|sdh**

### Mode

Configure.

### Description

The **sonet set framing** command allows you to specify the SONET frame type for mapping the data. The two options are SONET (Synchronous Optical Network) which is an ANSI standard, or SDH (Synchronous Digital Hierarchy) which is an ITU standard.

There are minor differences between the two standards. One such difference is that SONET has a basic transmission rate of OC-1 (51.84 Mbps), whereas SDH has a basic transmission rate of OC-3 (155.52 Mbps).

### Parameters

|               |   |
|---------------|---|
| <SONET ports> | Specifies the SONET port name(s).           |
| <b>sonet</b>  | Sets the optical framing standard to SONET. |
| <b>sdh</b>    | Sets the optical framing standard to SDH.   |

### Restrictions

None.

### Example

To set optical framing on port so.2.1 to SONET:

```
xp(config)# sonet set so.2.1 framing sonet
```

## sonet set J0

### Purpose

Sets a value for the J0 flag.

### Format

**sonet set** <SONET ports> **J0**<num>

### Mode

Configure.

### Description

The **sonet set J0** command allows you to specify a value for the J0 flag. SONET frames carry overhead for path, section and line for easier multiplexing and better OAM&P (operation, administration, management, and provisioning) capabilities.

The SONET frame overhead information is stored in separate bytes, or flags.

There are nine bytes allocated for section overhead labeled A1, A2, B1, D1, D2, D3, E1, F1, J0/Z0.

There are 18 bytes allocated for line overhead labeled H1, H2, H3, B2, K1, K2, D4, D5, D6, D7, D8, D9, D10, D11, D12, S1/Z1, M0/M1, and E2.

There are nine bytes allocated for path overhead labeled J1, B3, C2, H4, G1, P2, Z3, Z4, and Z5.

The **sonet set J0** command sets the J0 flag. The J0 flag is the section trace byte.

### Parameters

|               |   |
|---------------|---|
| <SONET ports> | Specifies the SONET port name(s).   |
| <num>         | Specifies the value of the J0 flag. Specify any number between 0 and 255. |

### Restrictions

None.

## Example

To set the J0 flag to 16 on port so.2.1:

```
xp(config)# sonet set so.2.1 J0 16
```

# sonet set loopback

## Purpose

Exercises loopback functionality.

## Format

**sonet set** <SONET ports> **loopback none**| **line-facility**| **serial-terminal**| **parallel**

## Mode

Configure.

## Description

The **sonet set loopback** command allows you to exercise loopback functionality on a specified SONET port. Loopback is used to verify connectivity between two devices.

## Parameters

|                        |   |
|------------------------|---|
| <SONET ports>          | Specifies the SONET port name(s).   |
| <b>none</b>            | Disables loopback functionality. Loopback is disabled by default.                       |
| <b>line-facility</b>   | Line or facility loopback connects high speed receive data to high speed transmit data. |
| <b>serial-terminal</b> | Serial or terminal loopback connects high speed transmit to high speed receive data.    |
| <b>parallel</b>        | Parallel loopback connects byte wide transmit to receive processor.                     |

## Restrictions

None.

## Example

To connect high speed receive data to high speed transmit on port so.2.1:

```
xp(config)# sonet set so.2.1 loopback line-facility
```

## sonet set path-trace

### Purpose

Sets a path trace message.

### Format

**sonet set** *<SONET ports>* **path-trace** *<string>*

### Mode

Configure.

### Description

The **sonet set path-trace** command allows you to set a message in a buffer to be sent as a path-trace message.

The path trace message is part of the path overhead of the transport overhead in every SONET frame. This path trace byte is a 64 byte (or less) message string that is used by the destination and source to notify each other that they are connected within a path.

### Parameters

|                            |  |
|----------------------------|--|
| <i>&lt;SONET ports&gt;</i> | Specifies the SONET port name(s).  |
| <i>&lt;string&gt;</i>      | Specifies a character string. The maximum length must be 64 bytes or less. |

### Restrictions

None.

### Example

To send the path trace message 'tracer' on port so.2.1:

```
xp(config)# sonet set so.2.1 path-trace tracer
```

# sonet set payload-scramble

## Purpose

Enables scrambling and descrambling of the STS (synchronous transfer signal) payload.

## Format

**sonet set** <SONET ports> **payload-scramble on| off**

## Mode

Configure.

## Description

The **sonet set payload-scramble** command allows you to enable scrambling or descrambling of the payload encapsulated in the STS frame. Scrambling the STS payload is important in optimizing the transmission density of the data stream. Since all SONET transmission use the same source clock for timing, scrambling the payload using a random number generator converts the data stream to a more random sequence. This ensures optimal transmission density of the data stream.

## Parameters

|               |  |
|---------------|--|
| <SONET ports> | Specifies the SONET port name(s).                        |
| <b>on</b>     | Enables scrambling and descrambling of the STS payload.  |
| <b>off</b>    | Disables scrambling and descrambling of the STS payload. |

## Restrictions

None.

## Example

To enable scrambling on port so.2.1:

```
xp(config)# sonet set so.2.1 payload-scramble on
```

# sonet set protected-by

## Purpose

Configures an APS protecting port.

## Format

**sonet set** <SONET ports> **protected-by** <SONET port>

## Mode

Configure.

## Description

The **sonet set protecting** command allows you to specify a protecting port for Automatic Protection Switching (APS). APS is used to provide redundancy for transmission between two SONET devices. This ensures that if a link goes down, traffic can be automatically switched to a secondary backup link and the connection remains operational.

With APS, there is a **working** (primary) port and a **protecting** (backup) port. APS automatically switches all traffic over from the **working** to the **protecting** port in case of signal degradation or failure in receive on the working port.

This command is used in conjunction with the **sonet set protection** command.

## Parameters

|                                     |  |
|-------------------------------------|--|
| <SONET ports>                       | Specifies the SONET port name(s).  |
| <b>protected-by</b><br><SONET port> | Specifies the APS protecting port. This must be a single port. Only valid for Packet-over-SONET ports. |

## Restrictions

None.

## Example

To set so.1.1 as the APS protecting port for so.2.1:

```
xp(config)# sonet set so.2.1 protection 1+1 protected by so.1.1
```

# sonet set protection

## Purpose

Configures an APS working port.

## Format

**sonet set** <SONET ports> **protection 1+1**

## Mode

Configure.

## Description

The **sonet set protection 1+1** command configures a working port for Automatic Protection Switching (APS). The working port is protected by the protecting port. APS provides redundancy for transmission between two SONET devices. This ensures that if a link goes down, traffic can be automatically switched to a secondary backup link and the connection remains operational.

With APS, there is a **working** (primary) port and a **protecting** (backup) port. APS automatically switches all traffic over from the **working** to the **protecting** port in case of signal degradation or failure in receive on the working port.

This command is used in conjunction with the sonet set **protected-by** option.

Negate this command to disable APS on the SONET port.

## Parameters

|               |   |
|---------------|---|
| <SONET ports> | Specifies the SONET port name(s).   |
| <b>1+1</b>    | Specifies the 1+1 APS scheme, where one working port is matched with one protecting port. |

## Restrictions

None.



## Example

To configure so.2.1 as an APS working port protected by so.1.1:

```
xp(config)# sonet set so.2.1 protection 1+1 protected-by so.1.1
```

# sonet set protection-switch

## Purpose

Configures protection switching parameters.

## Format

**sonet set** <SONET ports> **protection-switch** **lockoutprot** | **forced** | **manual**

## Mode

Configure.

## Description

The **sonet set protection-switch** command allows you to configure SONET Automatic Protection Switching (APS) on a SONET port. With APS, there is a **working** (primary) port and a **protecting** (backup) port. APS automatically switches all traffic over from the **working** to the **protecting** port in case of signal degradation or failure in receive on the working port.

Use this command to configure the APS switching characteristics for a SONET port.

## Parameters

|                    |  |
|--------------------|--|
| <SONET ports>      | Specifies the SONET port name(s).  |
| <b>lockoutprot</b> | Prevents APS switching from a <b>working</b> port to a <b>protecting</b> port in the case of signal failure or signal degrade. This command is configured only on the protecting port.                                       |
| <b>forced</b>      | Allows protection switching to occur. Switches service from this port to the other port, even when there are errors on the other port.   |
| <b>manual</b>      | Allows you to manually switch service from a port to the other APS port. This is provided that there are no errors on the protecting port. This command can be configured on either the working port or the protecting port. |

## Restrictions

None.

## Example

To configure APS switching for the working port so.2.1:

```
xp(config)# sonet set so.2.1 protection-switch forced
```

## sonet set revertive

### Purpose

Sets SONET protection switching to revertive or nonrevertive mode.

### Format

**sonet set** <SONET ports> **revertive off|on**

### Mode

Configure.

### Description

The **sonet set revertive** command allows you to select whether traffic will be switched back to the working port from the protecting port after the signal degrade or failure condition has been corrected. Once the condition has been corrected, APS waits for a specified time period (WTR-timer) before switching back to the working port.

With APS, there is a **working** (primary) port and a **protecting** (backup) port. APS automatically switches all traffic over from the **working** to the **protecting** port in case of signal degradation or failure in receive on the working port.

### Parameters

|               |  |
|---------------|--|
| <SONET ports> | Specifies the SONET port name(s).  |
| <b>off</b>    | Prevents automatic switch back to the <b>working</b> port from the <b>protecting</b> port after the signal degrade or failure condition has been corrected.  |
| <b>on</b>     | Allows traffic to switch back from the <b>protecting</b> port to the <b>working</b> port after the signal degrade or failure condition has been corrected and after the Wait-to-Restore timer has expired. |

### Restrictions

None.

## Example

To set APS switching to revertive mode for the protecting port so.2.1:

```
xp(config)# sonet set so.2.1 revertive on
```

## sonet set S1S0

### Purpose

Sets a value for the S1/S0 flag.

### Format

**sonet set** <SONET ports> **S1S0** <num>

### Mode

Configure.

### Description

The **sonet set S1S0** command allows you to specify a value for the S1/S0 flag. SONET frames carry overhead for path, section and line for easier multiplexing and better OAM&P (operation, administration, management, and provisioning) capabilities.

The SONET frame overhead information is stored in separate bytes, or flags.

There are nine bytes allocated for section overhead labeled A1, A2, B1, D1, D2, D3, E1, F1, J0/Z0.

There are 18 bytes allocated for line overhead labeled H1, H2, H3, B2, K1, K2, D4, D5, D6, D7, D8, D9, D10, D11, D12, S1/Z1, M0/M1, and E2.

There are nine bytes allocated for path overhead labeled J1, B3, C2, H4, G1, P2, Z3, Z4, and Z5.

The **sonet set S1S0** command sets the S1/S0 flag. The S1/S0 flag is the line synchronization status byte used to indicate synchronization state of the line terminating devices.

### Parameters

|               |  |
|---------------|--|
| <SONET ports> | Specifies the SONET port name(s).  |
| <num>         | Specifies the value of the S1/S0 flag. Specify any number between 0 and 3. |

### Restrictions

None.

## Example

To set the S1/S0 flag to 1 on port so.2.1:

```
xp(config)# sonet set so.2.1 S1S0 1
```

## sonet set sd-ber

### Purpose

Sets the Bit Error Rate (BER) signal degrade threshold level.

### Format

**sonet set** <SONET ports> **sd-ber** <num>

### Mode

Configure.

### Description

The **sonet set sd-ber** command allows you to specify a signal degrade threshold level. There are two threshold levels based on the Bit Error Rate: signal degrade and signal failure. These two threshold levels act as a two stage alarm system, where the signal degrade threshold is always met first before the signal failure threshold.

Once the BER reaches the signal degrade threshold level, then a signal degrade alarm occurs and the receive is considered to be in signal degrade condition. Based upon the APS configuration, all traffic is switched from the working port to the protecting port.

### Parameters

|               |   |
|---------------|---|
| <SONET ports> | Specifies the SONET port name(s).   |
| <num>         | Specifies the Bit Error Rate signal degrade threshold level in $10^{-n}$ . Specify any number for n between 5 to 9. The default is 6, indicating a threshold level of $10^{-6}$ . This means that a signal degrade alarm occurs if the Bit Error Rate rises past the 1/1000000 level. |

### Restrictions

None.

### Example

To set the BER signal degrade threshold level to  $10^{-6}$  or 1/1000000:

```
xp(config)# sonet set so.2.1 sd-ber 6
```



## sonet set sf-ber

### Purpose

Sets the Bit Error Rate (BER) signal failure threshold level.

### Format

**sonet set** <SONET ports> **sf-ber** <num>

### Mode

Configure.

### Description

The **sonet set sf-ber** command allows you to specify a signal failure threshold level. There are two threshold levels based on the Bit Error Rate: signal degrade and signal failure. These two threshold levels act as a two-stage alarm system, whereby the signal degrade threshold is always met first before the signal failure threshold.

Once the BER reaches the signal failure threshold level, then a signal failure alarm occurs and the receive is considered to be in signal failure condition. Based upon the APS configurations, all traffic is switched from the working port to the protecting port.

### Parameters

|               |  |
|---------------|--|
| <SONET ports> | Specifies the SONET port name(s).  |
| <num>         | Specifies the Bit Error Rate signal failure threshold level in $10^{-n}$ . Specify any number for n between 3 to 5. The default is 3, indicating a threshold level of $10^{-3}$ . This means that a signal failure alarm occurs if the Bit Error Rate rises past the 1/1000 level. |

### Restrictions

None.

### Example

To set the BER signal failure threshold level to  $10^{-3}$  or 1/1000:

```
xp(config)# sonet set so.2.1 sf-ber 3
```

# sonet set sts-stream-scramble

## Purpose

Enables scrambling or descrambling of the STS (synchronous transfer signal) stream.

## Format

**sonet set** *<SONET ports>* **sts-stream-scramble on| off**

## Mode

Configure.

## Description

The **sonet set sts-stream-scramble** command allows you to enable scrambling and descrambling of the STS stream. Scrambling the STS stream is important in optimizing the transmission density of the data stream. Since all STS transmission use the same source clock for timing. Scrambling the payload using a random number generator converts the data stream to a more random sequence. This ensures optimal transmission density of the data stream.

## Parameters

|                            |   |
|----------------------------|---|
| <i>&lt;SONET ports&gt;</i> | Specifies the SONET port name(s).                       |
| <b>on</b>                  | Enables scrambling and descrambling of the STS stream.  |
| <b>off</b>                 | Disables scrambling and descrambling of the STS stream. |

## Restrictions

None.

## Example

To enable scrambling on port so.2.1:

```
xp(config)# sonet set so.2.1 sts-stream-scramble on
```

# sonet set WTR-timer

## Purpose

Sets the Wait-to-Restore timer.

## Format

**sonet set** <SONET ports> **WTR-timer** <num>

## Mode

Configure.

## Description

The **sonet set WTR-timer** command allows you to set the Wait-to-Restore timer. The WTR-timer specifies a time period that must expire before traffic is switched back to the working port from the protecting port. Once the signal degrade or failure condition has been corrected, APS waits until the WTR-timer expires before switching back to the working port.

## Parameters

|               |   |
|---------------|---|
| <SONET ports> | Specifies the SONET port name(s).   |
| <num>         | Specifies the WTR timer (in minutes). Specify any number between 5 and 12 minutes. The <b>default</b> is 5 minutes. |

## Restrictions

None.

## Example

To set the WTR-timer to 6 minutes on port so.2.1:

```
xp(config)# sonet set so.2.1 WTR-timer 6
```

## sonet show aps

### Purpose

Displays APS status.

### Format

**sonet show aps** <SONET ports>

### Mode

Enable.

### Description

The **sonet show aps** command allows you to display APS (automatic protection switching) status. This command allows you to display such APS parameters as protection level, working or protecting port, directionality, and switch status.

### Parameters

---

|               |                                   |
|---------------|-----------------------------------|
| <SONET ports> | Specifies the SONET port name(s). |
|---------------|-----------------------------------|

---

### Restrictions

None.

### Example

To display the APS status for port so.2.1:

|                                  |
|----------------------------------|
| xp# <b>sonet show aps so.2.1</b> |
|----------------------------------|

# sonet show loopback

## Purpose

Displays loopback status.

## Format

**sonet show loopback** <SONET ports>

## Mode

Enable.

## Description

The **sonet show loopback** command allows you to display loopback status for a specified SONET port. Loopback is used to verify connectivity between two devices.

## Parameters

---

|               |                                   |
|---------------|-----------------------------------|
| <SONET ports> | Specifies the SONET port name(s). |
|---------------|-----------------------------------|

---

## Restrictions

None.

## Example

To display the loopback status for port so.2.1:

|                                       |
|---------------------------------------|
| xp# <b>sonet show loopback so.2.1</b> |
|---------------------------------------|

## sonet show medium

### Purpose

Displays SONET optical line values.

### Format

**sonet show medium** *<SONET ports>*

### Mode

Enable.

### Description

The **sonet show medium** command allows you to display the various SONET optical line values associated with a SONET port. This command will allow you to display values such as framing status, line type, and administrator-specified circuit identifier.

### Parameters

---

|                            |                                   |
|----------------------------|-----------------------------------|
| <i>&lt;SONET ports&gt;</i> | Specifies the SONET port name(s). |
|----------------------------|-----------------------------------|

---

### Restrictions

None.

### Example

To display optical line values for port so.2.1:

|                                     |
|-------------------------------------|
| xp# <b>sonet show medium so.2.1</b> |
|-------------------------------------|

# sonet show pathtrace

## Purpose

Displays received path trace messages.

## Format

**sonet show pathtrace** *<SONET ports>*

## Mode

Enable.

## Description

The **sonet show pathtrace** command allows you to display path trace messages received on a specified SONET port.

## Parameters

---

|                            |                                   |
|----------------------------|-----------------------------------|
| <i>&lt;SONET ports&gt;</i> | Specifies the SONET port name(s). |
|----------------------------|-----------------------------------|

---

## Restrictions

None.

## Example

To display the path trace messages for port so.2.1:

|  |
|--|
| xp# <b>sonet show pathtrace so.2.1</b> |
|--|





# Chapter 71

## ssh Commands

Secure Shell (SSH) is a “secure” replacement for Telnet. SSH provides the same remote access to the X-Pedition router that Telnet provides, but does so securely by encrypting all session data—including passwords.

**Note:** When you enable the SSH server, the X-Pedition router automatically disables Telnet access.

### Command Summary

Table 59 lists the secure shell (ssh) commands. The sections following the table describe the command syntax.

**Table 59. ssh Commands**

|  |
|--|
| <b>ssh</b> <host> [ <b>encryption-preference</b> <encryption-algorithm-list>]<br>[ <b>escape</b> <escape-character>  <b>none</b> ] [ <b>login-as</b> <username>]<br>[ <b>mac-preference</b> <mac-algorithm-list>] [ <b>no-compression</b> ] [ <b>port</b> <tcp-port>]<br>[ <b>protocol-version-preference</b> <version-list>] [ <b>ssh1-encryption</b> 3des  blowfish]                                     |
| <b>ssh-client clear-known-hosts</b>  |
| <b>ssh-client delete-host-key</b> <hostname> [dsa  rsa  rsa1]  |
| <b>ssh-client import-host-keys</b> <filename>  |
| <b>ssh-client set</b> [ <b>encryption-preference</b> <cipher1> [<cipher2>] ...] <br>[ <b>escape</b> <escape-character>  <b>none</b> ] [ <b>mac-preference</b> <mac1> [<mac2>] ...]  [ <b>no-</b><br><b>compression</b> ] [ <b>port</b> <tcp-port>]  [ <b>protocol-version-preference</b> [ssh1] [ssh2]] <br>[ssh1-encryption 3des blowfish]  [ <b>strict-host-key-checking</b> ] [ <b>username</b> <name>] |
| <b>ssh-client set software-version-string</b> <version-string>   |
| <b>ssh-server enable</b>   |

**Table 59. ssh Commands (Continued)**

|  |
|--|
| <b>ssh-server generate-host-key</b> <type> <b>bits</b> <bits>                    |
| <b>ssh-server set auth-grace-timeout</b> <timeout>                               |
| <b>ssh-server set encryption</b> <cipher1> <cipher2> ...                         |
| <b>ssh-server set listen-port</b> <port>   |
| <b>ssh-server set mac</b> <mac1> <mac2> ...                                      |
| <b>ssh-server set max-sessions</b> <limit>                                       |
| <b>ssh-server set protocol-version</b> <version>                                 |
| <b>ssh-server set server-key-lifetime</b> <time>                                 |
| <b>ssh-server set software-version-string</b> <version-string>                   |
| <b>ssh-server show public-host-key</b> <type> <b>fingerprint-format</b> <format> |

# ssh

## Format

```
ssh <host> [encryption-preference <encryption-algorithm-list>]
[escape <escape-character>| none] [login-as <username>]
[mac-preference <mac-algorithm-list>] [no-compression] [port <tcp-port>]
[protocol-version-preference <version-list>] [ssh1-encryption 3des| blowfish]
```

## Mode

Enable.

## Description

The **ssh** command invokes the Secure Shell client. Any options specified on the command-line will override any defaults and configuration settings saved in the active configuration. No configuration is required in order to use the **ssh** command.

**Note:** SSH client requires firmware version E9.1.0.0 or later.

## Parameters

| <i>&lt;host&gt;</i>  | The host name or IP address of the remote SSH server with which to connect.  |        |             |            |          |     |            |         |         |          |              |          |             |
|--|--|--------|-------------|------------|----------|-----|------------|---------|---------|----------|--------------|----------|-------------|
| <b>encryption-preference</b><br><i>&lt;encryption-algorithm-list&gt;</i> | Specify a comma-separated list of SSH-2 encryption algorithms or <i>ciphers</i> to attempt, in order of preference. By default, the algorithms attempted are (in order of preference) AES, Triple-DES, Blowfish, CAST-128, and ARCFOUR. Valid ciphers and their corresponding names are shown as follows: <div> <table> <tr> <th>Cipher</th><th>Cipher Name</th></tr> <tr> <td>Triple-DES</td><td>3des-cbc</td></tr> <tr> <td>AES</td><td>aes128-cbc</td></tr> <tr> <td>ARCFOUR</td><td>arcfour</td></tr> <tr> <td>Blowfish</td><td>blowfish-cbc</td></tr> <tr> <td>CAST-128</td><td>cast128-cbc</td></tr> </table> <p><b>Note:</b> Cipher names are case sensitive and, when formulating the comma-separated list, there should be <b>no</b> spaces.</p> </div> | Cipher | Cipher Name | Triple-DES | 3des-cbc | AES | aes128-cbc | ARCFOUR | arcfour | Blowfish | blowfish-cbc | CAST-128 | cast128-cbc |
| Cipher   | Cipher Name  |        |             |            |          |     |            |         |         |          |              |          |             |
| Triple-DES   | 3des-cbc   |        |             |            |          |     |            |         |         |          |              |          |             |
| AES  | aes128-cbc   |        |             |            |          |     |            |         |         |          |              |          |             |
| ARCFOUR  | arcfour  |        |             |            |          |     |            |         |         |          |              |          |             |
| Blowfish   | blowfish-cbc   |        |             |            |          |     |            |         |         |          |              |          |             |
| CAST-128   | cast128-cbc  |        |             |            |          |     |            |         |         |          |              |          |             |
| <b>escape</b><br><i>&lt;escape-character&gt;</i><br><b>none</b>          | Specify a single character to use as the escape-sequence initiator. Use the circumflex character (^) as a prefix to designate a control character. Select the <b>none</b> option if you do not want the router to recognize escape sequences.  |        |             |            |          |     |            |         |         |          |              |          |             |

| <b>login-as</b> <username>                              | Specify the name to use for authentication on the remote host. The username cannot exceed 32 characters in length.   |                  |                       |          |          |             |             |                |                |           |           |              |              |
|---|--|------------------|-----------------------|----------|----------|-------------|-------------|----------------|----------------|-----------|-----------|--------------|--------------|
| <b>mac-preference</b><br><mac-algorithm-list>           | Specify a comma-separated list of SSH-2 Message Authentication Code algorithms or MACs to attempt, in order of preference. By default, the algorithms attempted are (in order of preference) HMAC-MD5, HMAC-SHA1, HMAC-RIPEMD160, HMAC-SHA1-96, and HMAC-MD5-96. Valid MACs and their corresponding names are shown as follows: <div style="margin-left: 40px;"> <table> <tr> <th>MAC</th><th>MAC Name</th></tr> <tr> <td>HMAC-MD5</td><td>hmac-md5</td></tr> <tr> <td>HMAC-MD5-96</td><td>hmac-md5-96</td></tr> <tr> <td>HMAC-RIPEMD160</td><td>hmac-ripemd160</td></tr> <tr> <td>HMAC-SHA1</td><td>hmac-sha1</td></tr> <tr> <td>HMAC-SHA1-96</td><td>hmac-sha1-96</td></tr> </table> </div> <p><b>Note:</b> MAC names are case sensitive and, when formulating the comma-separated list, there should be <b>no</b> spaces.</p> | MAC              | MAC Name              | HMAC-MD5 | hmac-md5 | HMAC-MD5-96 | hmac-md5-96 | HMAC-RIPEMD160 | hmac-ripemd160 | HMAC-SHA1 | hmac-sha1 | HMAC-SHA1-96 | hmac-sha1-96 |
| MAC   | MAC Name   |                  |                       |          |          |             |             |                |                |           |           |              |              |
| HMAC-MD5  | hmac-md5   |                  |                       |          |          |             |             |                |                |           |           |              |              |
| HMAC-MD5-96   | hmac-md5-96  |                  |                       |          |          |             |             |                |                |           |           |              |              |
| HMAC-RIPEMD160  | hmac-ripemd160   |                  |                       |          |          |             |             |                |                |           |           |              |              |
| HMAC-SHA1   | hmac-sha1  |                  |                       |          |          |             |             |                |                |           |           |              |              |
| HMAC-SHA1-96  | hmac-sha1-96   |                  |                       |          |          |             |             |                |                |           |           |              |              |
| <b>no-compression</b>                                   | Specifying this option will disable compression of session data which, by default, is compressed. When compression is enabled, the router compresses data prior to its encryption. Generally speaking, leaving compression <i>enabled</i> will result in better performance—it is far more taxing on system resources to encrypt data than to compress it.   |                  |                       |          |          |             |             |                |                |           |           |              |              |
| <b>port</b> <tcp-port>                                  | Specify an alternate TCP port (from 1 to 65,535 inclusive) to connect to on the remote host. Typically, SSH servers listen for incoming SSH connection requests on TCP port 22.  |                  |                       |          |          |             |             |                |                |           |           |              |              |
| <b>protocol-version-preference</b><br><version-list>    | Specify a comma-separated list of which protocol versions to allow, in order of preference. By default, the allowed protocol versions are (in order of preference) SSH-2 and SSH-1. Valid protocol versions and their corresponding names are shown as follows: <div style="margin-left: 40px;"> <table> <tr> <th>Protocol Version</th><th>Protocol Version Name</th></tr> <tr> <td>SSH-1</td><td>ssh1</td></tr> <tr> <td>SSH-2</td><td>ssh2</td></tr> </table> </div> <p><b>Note:</b> Protocol version names are case-sensitive and, when formulating the comma-separated list, there should be <b>no</b> spaces.</p>   | Protocol Version | Protocol Version Name | SSH-1    | ssh1     | SSH-2       | ssh2        |                |                |           |           |              |              |
| Protocol Version  | Protocol Version Name  |                  |                       |          |          |             |             |                |                |           |           |              |              |
| SSH-1   | ssh1   |                  |                       |          |          |             |             |                |                |           |           |              |              |
| SSH-2   | ssh2   |                  |                       |          |          |             |             |                |                |           |           |              |              |
| <b>ssh1-encryption</b><br><b>3des</b>   <b>blowfish</b> | Specify a cipher to use for an SSH-1 session. Enter <b>3des</b> to use the Triple-DES cipher and <b>blowfish</b> to use the Blowfish cipher.   |                  |                       |          |          |             |             |                |                |           |           |              |              |

## Restrictions

- If a PCMCIA flash card is not present in the router, some SSH client security features will be disabled. Enterasys Networks recommends that you use PCMCIA flash cards in all routers that will run the SSH client.
- SSH client requires firmware version E9.1.0.0 or later.

# ssh-client clear-known-hosts

## Format

**ssh-client clear-known-hosts**

## Mode

Enable.

## Description

The Known Hosts database stores host keys belonging to all known SSH servers and is used to verify the identity of a server each time an SSH connection is made. If unauthorized alterations are made to the Known Hosts database or if database tampering is otherwise detected, the router will not allow any new outbound SSH sessions. In such an event, entering the **ssh-client clear-known-hosts** command from the CLI will reset the Known Hosts database, allowing the router to rebuild data and restore access to new SSH sessions.

**Note:** For added security, only users with configuration-level privileges or knowledge of the configuration mode password (if enabled) may execute this command.

## Parameters

None.

## Restrictions

- This command requires that a PCMCIA flash card be present in the router.
- Only users with configuration-level privileges or knowledge of the configuration mode password (if enabled) may execute this command.
- SSH client requires firmware version E9.1.0.0 or later.

# ssh-client delete-host-key

## Format

**ssh-client delete-host-key** <hostname> [**dsa**|**rsa**|**rsa1**]

## Mode

Enable.

## Description

In the event that a particular host key is compromised or becomes outdated, you can delete the key with the **ssh-client delete-host-key** command. When you specify the optional key-type, the router will remove only keys of that type from the host—otherwise, all keys that belong to the specified host will be deleted.

**Note:** For added security, only users with configuration-level privileges or knowledge of the configuration mode password (if enabled) may execute this command.

## Parameters

|   |  |
|---|--|
| <hostname>                                | The name or IP address of the host whose key(s) you want to delete. To delete keys of a specific type from the host, enter one of the following: |
| [ <b>dsa</b>   <b>rsa</b>   <b>rsa1</b> ] |  |
| <b>dsa</b>                                | Delete only DSA keys.  |
| <b>rsa</b>                                | Delete only RSA keys.  |
| <b>rsa1</b>                               | Delete only RSA1 keys.   |

## Restrictions

- This command requires that a PCMCIA flash card be present in the system chassis.
- Only users with configuration-level privileges or knowledge of the configuration mode password (if enabled) may execute this command.
- SSH client requires firmware version E9.1.0.0 or later.

# ssh-client import-host-keys

## Format

**ssh-client import-host-keys** <filename>

## Mode

Enable.

## Description

The **ssh-client import-host-keys** command is useful for initially populating the Known Hosts database on a number of X-Pedition routers. The X-Pedition router allows you to create a text file that contains a list of the hosts you wish to add to the Known Hosts databases, then upload the file to each router you wish to configure. Executing this command on each router will import the host keys from the uploaded file and will create an identical Known Hosts database list on each router.

The text-file used to import keys must adhere to the following:

- Each host key must occupy a single line.
- No line should exceed 8,192 characters in length.
- Each line should be formatted as follows: *[hostname,]ip-address public-host-key*

**Note:** Although *hostname* is optional, it should be followed by a comma if used and there should be no spaces in or between *hostname* and *ip-address*. *Public-host-key* should be the ASCII representation of the DSA, RSA, or RSA1 public host key. The ASCII representation of these keys is obtained by entering the **ssh-server show public-host-key** command from the CLI. The fingerprint should not be included—only the part of the key displayed after “**Key:**”.

## Parameters

|            |  |
|------------|--|
| <filename> | The name of the file on the local system that contains the population list for the Known Hosts database. |
|------------|--|

## Restrictions

- This command requires that a PCMCIA flash card be present in the system chassis.
- For added security, only users with configuration-level privileges or knowledge of the configuration mode password (if enabled) may execute this command.
- SSH client requires firmware version E9.1.0.0 or later.

## Example

The following example demonstrates how to import host keys from the text file “**host\_keys**” located on a remote TFTP server::

```
xp# copy tftp://192.168.1.1/host_keys to host_keys
xp# ssh-client import-host-keys bootflash:host_keys
```



# ssh-client set

## Format

```
ssh-client set [encryption-preference <cipher1> [<cipher2>] ...] [escape <escape-character>|
none] [mac-preference <mac1> [<mac2>] ...] [no-compression] [port <tcp-port>] [protocol-
version-preference [ssh1] [ssh2]] [ssh1-encryption 3des|blowfish] [strict-host-key-checking]
[username <name>]
```

## Mode

Configure.

## Description

Customizes default values for SSH client sessions. Configured values will be used by all sessions unless explicitly overridden by an alternate value on the SSH command-line.

## Parameters

|  |   |               |
|--|---|---------------|
| <b>encryption-preference</b><br><cipher1><br>[<cipher2>] | Sets the default SSH-2 encryption algorithms (i.e., <i>ciphers</i> ) and priority for all future SSH-2 client sessions. The SSH client will attempt only the specified ciphers and in the order they are listed below. Available options for the ciphers appear as follows: |               |
|  | <b>Option</b>   | <b>Cipher</b> |
|  | 3des-cbc  | Triple-DES    |
|  | aes128-cbc  | AES           |
|  | arcfour   | ARCFOUR       |
|  | blowfish-cbc  | Blowfish      |
|  | cast128-cbc   | CAST-128      |
| <b>escape</b> <escape-character>  <b>none</b>            | Specify a single character to use as the escape-sequence initiator. Use the circumflex character (^) as a prefix to designate a control character. Select the <b>none</b> option if you do not want the router to recognize escape sequences.                               |               |

| <b>mac-preference</b><br><mac1> [<mac2>]                | <p>Sets the default SSH-2 Message Authentication Code or <i>MAC</i> algorithms and priority for all future SSH-2 client sessions. The SSH client will attempt only the specified MACs in the order listed below. Available options for the MACs appear as follows:</p> <table> <tr> <th>Option</th><th>MAC</th></tr> <tr> <td>hmac-md5</td><td>HMAC-MD5</td></tr> <tr> <td>hmac-md5-96</td><td>HMAC-MD5-96</td></tr> <tr> <td>hmac-ripemd160</td><td>HMAC-RIPEMD160</td></tr> <tr> <td>hmac-sha1</td><td>HMAC-SHA1</td></tr> <tr> <td>hmac-sha1-96</td><td>HMAC-SHA1-96</td></tr> </table>   | Option           | MAC                   | hmac-md5 | HMAC-MD5 | hmac-md5-96 | HMAC-MD5-96 | hmac-ripemd160 | HMAC-RIPEMD160 | hmac-sha1 | HMAC-SHA1 | hmac-sha1-96 | HMAC-SHA1-96 |
|---|--|------------------|-----------------------|----------|----------|-------------|-------------|----------------|----------------|-----------|-----------|--------------|--------------|
| Option  | MAC  |                  |                       |          |          |             |             |                |                |           |           |              |              |
| hmac-md5  | HMAC-MD5   |                  |                       |          |          |             |             |                |                |           |           |              |              |
| hmac-md5-96   | HMAC-MD5-96  |                  |                       |          |          |             |             |                |                |           |           |              |              |
| hmac-ripemd160  | HMAC-RIPEMD160   |                  |                       |          |          |             |             |                |                |           |           |              |              |
| hmac-sha1   | HMAC-SHA1  |                  |                       |          |          |             |             |                |                |           |           |              |              |
| hmac-sha1-96  | HMAC-SHA1-96   |                  |                       |          |          |             |             |                |                |           |           |              |              |
| <b>no-compression</b>                                   | <p>Specifying this option will disable compression of session data for all future SSH sessions which, by default, is compressed. When compression is enabled, the router compresses data prior to its encryption. Generally speaking, leaving compression <i>enabled</i> will result in better performance—it is far more taxing on system resources to encrypt data than to compress it.</p>  |                  |                       |          |          |             |             |                |                |           |           |              |              |
| <b>port</b> <tcp-port>                                  | <p>Specify an alternate TCP port (from 1 to 65,535 inclusive) to connect to on the remote host for all future SSH sessions. Typically, SSH servers listen for incoming SSH connection requests on TCP port 22.</p>   |                  |                       |          |          |             |             |                |                |           |           |              |              |
| <b>protocol-version-preference</b> [ssh1]<br>[ssh2]     | <p>Sets the default protocol versions and priority for all future SSH sessions. Only the specified version(s) will be attempted, and in the order listed as follows:</p> <table> <tr> <th>Protocol Version</th><th>Protocol Version Name</th></tr> <tr> <td>SSH-1</td><td>ssh1</td></tr> <tr> <td>SSH-2</td><td>ssh2</td></tr> </table> <p><b>Note:</b> Protocol version names are case-sensitive and, when formulating the comma-separated list, there should be <b>no</b> spaces.</p>  | Protocol Version | Protocol Version Name | SSH-1    | ssh1     | SSH-2       | ssh2        |                |                |           |           |              |              |
| Protocol Version  | Protocol Version Name  |                  |                       |          |          |             |             |                |                |           |           |              |              |
| SSH-1   | ssh1   |                  |                       |          |          |             |             |                |                |           |           |              |              |
| SSH-2   | ssh2   |                  |                       |          |          |             |             |                |                |           |           |              |              |
| <b>ssh1-encryption</b><br><b>3des</b>   <b>blowfish</b> | <p>Specify a cipher to use for all future SSH-1 client sessions. Enter <b>3des</b> to use the Triple-DES cipher and <b>blowfish</b> to use the Blowfish cipher.</p>  |                  |                       |          |          |             |             |                |                |           |           |              |              |
| <b>strict-host-key-checking</b>                         | <p>Under normal circumstances, when an ordinary user connects an SSH session to an unknown host, the user receives a warning that the host is unknown. If the user elects to continue, the new host key is added automatically to the Known Hosts database.</p> <p>The <b>ssh-client set strict-host-key-checking</b> configuration command changes the default behavior by preventing users from automatically adding new host keys to the Known Hosts database. With this option enabled, users may add new keys to the Known Hosts database via the <b>ssh-client import-host-keys</b> command only. This provides a higher level of security by allowing only users with configuration-level privileges to add new keys to the Known Hosts database.</p> <p><b>Note:</b> This parameter requires that a PCMCIA flash card be present in the system chassis—otherwise, the router will not permit any outbound SSH client sessions.</p> |                  |                       |          |          |             |             |                |                |           |           |              |              |

---

|                        |  |
|------------------------|--|
| <b>username</b> <name> | The default username to use for all future SSH client sessions. At the start of a client session, the router sends this username to the remote host for authentication. The user name should not exceed 32 characters in length. |
|------------------------|--|

---

## Restrictions

- The **strict-host-key-checking** option requires that a PCMCIA flash card be present in the system chassis—otherwise, the router will not permit any outbound SSH client sessions.
- SSH client requires firmware version E9.1.0.0 or later.

# ssh-client set software-version-string

## Format

**ssh-client set software-version-string** <version-string>

## Mode

Configure.

## Description

This command allows users to change the built-in software version string sent to SSH servers—useful in cases where incompatibilities exist between the X-Pedition SSH client and a third-party server.

## Parameters

|  |   |
|--|---|
| <b>software-version-string</b><br><version-string> | Enter the version string (up to 63 characters in length). By default, this string is XPSSH. |
|--|---|

## Restrictions

SSH client requires firmware version E9.1.0.0 or later.

## Example

The following example uses a the software version string, “OpenSSH\_2.9.9p2.”

```
xp (config)# ssh-server set software-version-string OpenSSH_2.9.9p2
```

# **ssh-server enable**

## **Purpose**

Start the secure shell server.

## **Format**

**ssh-server enable**

## **Mode**

Configure.

## **Description**

Launches the secure shell server. In order for the server to start, at least one host key must exist and the key must be compatible with the configured protocol-version.

## **Parameters**

None.

## **Restrictions**

When you enable the SSH server, the X-Pedition router automatically disables Telnet access.

## **Example**

To start the secure shell server, enter the following:

|                          |
|--------------------------|
| <b>ssh-server enable</b> |
|--------------------------|

# ssh-server generate-host-key

## Purpose

Generate host key pairs.

## Format

ssh-server generate-host-key <type> bits <bits>

## Mode

Enable.

## Description

Generates asymmetric host key pairs. The host key is used to uniquely and securely identify the SSH server to the SSH client. In other words, the host key makes it possible for the SSH client to guarantee that it is connected to the intended host, not an imposter.

## Parameters

|             |   |
|-------------|---|
| <type>      | There are three key types of host key pairs— <i>rsa1</i> , <i>rsa</i> , and <i>dsa</i> .  |
| <b>rsa1</b> | An RSA1 key must be generated in order to interoperate with SSH-1 clients. RSA1 keys use the RSA public-key encryption algorithm.   |
| <b>rsa</b>  | An RSA key can be used to interoperate with SSH-2 clients. RSA keys use the RSA public key encryption algorithm.  |
| <b>dsa</b>  | A DSA key can be used to interoperate with SSH-2 clients. DSA keys use the DSA public key encryption algorithm.   |
| <b>all</b>  | Generates one key of each key type.   |
| <bits>      | Specifies the bit length (512–4096) of the keys to generate. In general, 1,024 bits (the default) is considered very secure. Lengths greater than 1,024 bits are not considered to provide much additional security and will slow down cryptographic operations. For example, keys that are 1,024 bits or less in size take only a few minutes to generate. In contrast, keys larger than 1,024 bits may take several hours to generate (e.g., 4,096 bit keys may require several hours). |

## Restrictions

None.

## Example

To generate a 1,024-bit DSA host key pair, enter the following:

```
ssh-server generate-host-key dsa bits 1024
```

## ssh-server set auth-grace-timeout

### Purpose

Sets the authentication time limit for connecting clients.

### Format

**ssh-server set auth-grace-timeout** *<timeout>*

### Mode

Configure.

### Description

Sets the time limit used to authenticate and connect clients. Clients that take longer than this to connect and successfully authenticate will be disconnected.

### Parameters

|                        |  |
|------------------------|--|
| <i>&lt;timeout&gt;</i> | Number of seconds (10-120) given to clients to successfully authenticate.<br>By default, this value is 60. |
|------------------------|--|

### Restrictions

None.

### Example

To set a 90-second authentication time limit, enter the following:

```
xp(config)# ssh-server set auth-grace-timeout 90
```



# ssh-server set encryption

## Purpose

Enable various encryption algorithms that will “scramble” and protect data.

## Format

**ssh-server set encryption** <cipher1> <cipher2> ...

## Mode

Configure.

## Description

Specifies which encryption algorithms the X-Pedition router will support. Encryption algorithms provide privacy of session data by “scrambling” the contents of the message so that only the intended recipient will be able to “unscramble” the data.

## Parameters

|                     |   |
|---------------------|---|
| <b>cipher(n)</b>    | The name of the cipher encryption algorithm to support. To select multiple ciphers, enter the name of each cipher or enter the keyword <b>all</b> (the default) to support all encryption algorithms.   |
| <b>aes128-cbc</b>   | 128-bit AES encryption operates in cipher-block-chaining mode. AES is relatively fast, but has not as yet seen as much real-world use as some of the other options. AES was formerly known as Rijndael.   |
| <b>3des-cbc</b>     | Triple-DES encryption utilizes three separate 56-bit keys operating in cipher-block-chaining mode. This encryption is considered by many to be the most secure widely-available bulk cipher because of its lengthy record of real-world use. Very slow compared to the other available algorithms. Key generation, in particular, is very slow and may result in a noticeable delay when generating new session keys. |
| <b>blowfish-cbc</b> | 128-bit Blowfish encryption operates in cipher-block-chaining mode. Blowfish has received much scrutiny, but has so far proved secure. Its speed is comparable to that of AES encryption.   |
| <b>cast128-cbc</b>  | CAST-128 encryption (128-bit) operates in cipher-block-chaining mode. Slightly slower than Blowfish, CAST-128 is perhaps more widely implemented due to its standardization in RFC-2144.  |
| <b>arcfour</b>      | 128-bit ARCFOUR encryption is a “stream” cipher. ARCFOUR is the only non-cipher-block-chaining cipher widely used with SSH implementations. Although it has received little scrutiny, ARCFOUR is considered secure by many. ACRFOUR is the fastest of the available options.  |

## Restrictions

None.

## Example

To set Triple-DES, 128-bit Blowfish, and 128-bit ARCFOUR encryption, enter the following:

```
xp(config)# ssh-server set encryption 3des-cbc blowfish-cbc arcfour
```

# ssh-server set listen-port

## Purpose

Set the TCP port on which secure shell server will listen.

## Format

**ssh-server set listen-port** *<port>*

## Mode

Configure.

## Description

Secure shell servers normally listen on TCP port 22. This command allows you to change the TCP port.

## Parameters

---

|                     |   |
|---------------------|---|
| <i>&lt;port&gt;</i> | The TCP port number on which to listen. By default, the TCP port is 22. |
|---------------------|---|

---

## Restrictions

None.

## Example

To assign secure shell server to listen on TCP port ten, enter the following:

```
xp(config)# ssh-server set listen-port 10
```

# ssh-server set mac

## Purpose

Enable support for MAC algorithms under SSH-2 to provide additional authentication for session data.

## Format

```
ssh-server set mac <mac1> <mac2> ...
```

## Mode

Configure.

## Description

Specifies which Message Authentication Code (MAC) algorithms the X-Pedition router will support. MAC algorithms provide authenticity for session data by digitally “signing” each message. The digital signature prevents a third party from altering or falsifying any session data. Applies to SSH-2 only.

## Parameters

|                       |  |
|-----------------------|--|
| <b>mac(n)</b>         | The name of the MAC to enable. To specify multiple MACs, enter the name of each MAC or specify the keyword <b>all</b> (the default) to select all MACs. When a client connects, the first MAC listed that is supported by both the client and the server will be used for the session. |
| <b>hmac-sha1</b>      | The HMAC-SHA1 MAC algorithm based on the SHA-1 message digest algorithm.   |
| <b>hmac-md5</b>       | The HMAC-MD5 MAC algorithm based on the MD5 message digest algorithm.  |
| <b>hmac-ripemd160</b> | The HMAC-RIPEMD160 MAC algorithm based on the RIPEMD-160 message digest algorithm.   |
| <b>hmac-sha1-96</b>   | The HMAC-SHA1-96 MAC algorithm based on the SHA-1 message digest algorithm.  |
| <b>hmac-md5-96</b>    | The HMAC-MD5-96 MAC algorithm based on the MD5 message digest algorithm.   |

## Restrictions

None.

## Example

To support the HMAC-SHA1, HMAC-MD5, and HMAC-MD5-96 MAC algorithms under SSH-2, enter the following:

```
xp(config)# ssh-server set mac hmac-sha1 hmac-md5 hmac-md5-96
```

## ssh-server set max-sessions

### Purpose

Set the maximum allowed number of simultaneous secure-shell sessions.

### Format

**ssh-server set max-sessions** *<limit>*

### Mode

Configure.

### Description

This command allows you to limit the number of secure shell sessions that can be active simultaneously. Limiting this to fewer than four sessions can be useful in preventing multiple users from modifying the configuration at the same time. This command is also useful for limiting the amount of CPU and memory resources consumed by active SSH sessions, since the cryptographic operations performed by active sessions can be somewhat resource intensive.

### Parameters

|                      |  |
|----------------------|--|
| <i>&lt;limit&gt;</i> | The maximum number (1-4) of secure-shell sessions that can be active simultaneously. The default is 4. |
|----------------------|--|

### Restrictions

None.

### Example

To allow three simultaneous secure shell sessions, enter the following:

```
xp(config)# ssh-server set max-sessions 3
```

# ssh-server set protocol-version

## Purpose

Select which Secure Shell protocol version(s) to support.

## Format

**ssh-server set protocol-version** <version>

## Mode

Configure.

## Description

Specifies which SSH protocol version(s) to support. Secure shell protocol versions include SSH-1 and SSH-2—SSH-2 is considered to be more secure than SSH-1. By default, the X-Pedition router enables both SSH protocols.

## Parameters

|             |   |
|-------------|---|
| <version>   | Specifies which Secure Shell protocol version(s) connecting clients will be allowed to use.                               |
| <b>ssh1</b> | Clients will be allowed to connect using the SSH-1 protocol only.   |
| <b>ssh2</b> | Clients will be allowed to connect using the SSH-2 protocol only.   |
| <b>both</b> | Clients will be allowed to connect using either SSH-1 or SSH-2 protocols. The X-Pedition router uses this as the default. |

## Restrictions

None.

## Example

To enable support for both versions of the secure shell protocol, enter the following from configuration mode:

```
xp(config)# ssh-server set protocol-version both
```

# ssh-server set server-key-lifetime

## Purpose

Set the regeneration period for the server key.

## Format

**ssh-server set server-key-lifetime** <time>

## Mode

Configure.

## Description

SSH-1 uses the server key to provide “perfect forward secrecy” for SSH-1 sessions. The **ssh-server set server-key-lifetime** command determines how often the server key regenerates. More frequent regeneration may provide slightly increased security, but comes at the cost of increased CPU utilization. The server key always generates a 768-bit RSA1 key and is not used for SSH-2. For additional information regarding perfect forward security refer to the *Enterasys X-Pedition User Reference Manual*.

## Parameters

|        |  |
|--------|--|
| <time> | The number of minutes (5–480) that will transpire before the server key regenerates. By default, this value is 60 minutes. |
|--------|--|

## Restrictions

None.

## Example

To set a delay time of 2 hours (120 minutes) before regenerating the server key, enter the following from configuration mode:

```
xp(config)# ssh-server set server-key-lifetime 120
```



# ssh-server set software-version-string

## Format

**ssh-sever set software-version-string** *<version-string>*

## Mode

Configure.

## Description

This command allows users to change the built-in software version string sent to SSH clients—useful in cases where incompatibilities exist between the X-Pedition SSH server and a third-party client.

## Parameters

|   |   |
|---|---|
| <b>software-version-string</b><br><i>&lt;version-string&gt;</i> | Enter the version string (up to 63 characters in length). By default, this string is XPSSH. |
|---|---|

## Restrictions

None.

## Examples

The following example uses a the software version string, “OpenSSH\_2.9.9p2.”

```
xp (config)# ssh-server set software-version-string OpenSSH_2.9.9p2
```

# ssh-server show public-host-key

## Purpose

Shows the public component and fingerprint of the specified host key pair.

## Format

**ssh-server show public-host-key** *<type>* **fingerprint-format** *<format>*

## Mode

Enable.

## Description

Shows the public component and fingerprint of a specific host key pair. The fingerprint is often useful for determining the authenticity of the host when connecting with a client for the first time. If necessary, you can use this command to copy the public key.

## Parameters

|                       |   |
|-----------------------|---|
| <i>&lt;type&gt;</i>   | Specifies which of the host keys to show.   |
| <b>rsa1</b>           | Shows the RSA1 public key and fingerprint.  |
| <b>rsa</b>            | Shows the RSA public key and fingerprint.   |
| <b>dsa</b>            | Shows the DSA public key and fingerprint.   |
| <i>&lt;format&gt;</i> | The format in which to display the fingerprint (optional). The default format is hexadecimal.   |
| <b>bubble-babble</b>  | Bubble babble is a method of representing the fingerprint as a string of “real” words to make the fingerprint easier to remember. The “words” are not necessarily real words, but they look more like words than a string of hexadecimal characters. Bubble-babble may be more useful than hex when verbally communicating the fingerprint to a user. |
| <b>hex</b>            | Shows the exact fingerprint in hexadecimal format. Although this format is a more concise way to display the fingerprint, it may be harder to remember and difficult to communicate verbally without transcription errors.  |

## Restrictions

None.

## Example

To show the RSA public key and fingerprint in bubble babble format, enter the following from enable mode:

```
xp(config)# ssh-server show public-host-key rsa fingerprint-format bubble-babble
```



# Chapter 72

## statistics Commands

The **statistics** commands allow the user to display statistics for various X-Pedition features. You also can clear some statistics.

### Command Summary

[Table 60](#) lists the statistics commands. The sections following the table describe the command syntax.

**Table 60. statistics commands**

|  |
|--|
| <b>statistics clear</b> <i>&lt;statistic-type&gt;</i>  |
| <b>statistics show</b> <b>appletalk-atp</b>   <b>appletalk-ddp</b>   <b>appletalk-echo</b>   <b>appletalk-interface</b>   <b>appletalk-nbp</b>   <b>appletalk-routing</b>   <b>appletalk-zip</b> |
| <b>statistics show arp</b> <i>&lt;Interface Name&gt;</i>   <b>all</b>  |
| <b>statistics show framer</b> <i>&lt;port-list&gt;</i>   |
| <b>statistics show icmp</b>  |
| <b>statistics show icmp6</b> { <i>&lt;interface name&gt;</i>   <b>all</b>   <b>aggregate</b> } { <b>summary</b>   <b>detailed</b> }  |
| <b>statistics show ip</b>  |
| <b>statistics show ipv6</b> { <i>&lt;interface name&gt;</i>   <b>all</b>   <b>aggregate</b> } { <b>summary</b>   <b>detailed</b> }   |
| <b>statistics show ip-interface</b> <i>&lt;string&gt;</i>   <b>all</b> [ <b>packets</b> ] [ <b>bytes</b> ] [ <b>errors</b> ] [ <b>input</b> ] [ <b>output</b> ]  <b>verbose</b>                  |
| <b>statistics show ipv6-interface</b> { <i>&lt;interface name&gt;</i>   <b>all</b> } { [ <b>packets</b> ] [ <b>bytes</b> ] [ <b>errors</b> ]   <b>verbose</b>   <b>detailed</b> }                |
| <b>statistics show ip-routing</b>  |
| <b>statistics show ipv6-routing</b>  |

**Table 60. statistics commands (Continued)**

|   |
|---|
| <b>statistics show ipx</b>  |
| <b>statistics show ipx-interface</b> <i>&lt;string&gt;</i>   <b>all packets bytes errors input output verbose</b> |
| <b>statistics show ipx-routing</b>  |
| <b>statistics show most-active</b>  |
| <b>statistics show multicast</b>  |
| <b>statistics show port-errors</b> <i>&lt;port/SmartTRUNK-list&gt;</i>   <b>all-ports</b>                         |
| <b>statistics show port-packets</b> <i>&lt;port-list&gt;</i>   <b>all-ports</b>                                   |
| <b>statistics show port-stats</b> <i>&lt;port/SmartTRUNK-list&gt;</i>   <b>all-ports</b>                          |
| <b>statistics show rarp</b> <i>&lt;string&gt;</i>   <b>all</b>  |
| <b>statistics show summary-stats</b>  |
| <b>statistics show tcp</b>  |
| <b>statistics show udp</b>  |
| <b>statistics show vlan all</b>   <i>&lt;string&gt;</i>   |

# statistics clear

## Purpose

Clear statistics.

## Format

**statistics clear** <statistic-type>

## Mode

Enable.

## Description

The **statistics clear** command clears port statistics, error statistics, or RMON statistics. When you clear statistics, the X-Pedition router sets the counters for the cleared statistics to 0, then begins accumulating the statistics again.

## Parameters

| <statistic-type>      | Type of statistics you want to clear. Specify one of the following:   |
|-----------------------|---|
| <b>ip</b>             | Clears all IPv4 statistics.   |
| <b>ipv6-interface</b> | Clears statistics for one or all IPv6 interfaces. Specify either:<br><br><IPv6 interface name> — Clear statistics for specified interface<br><br><b>all</b> — Clear statistics for all IPv6 interfaces                |
| <b>ipx</b>            | Clears all IPX statistics.  |
| <b>appletalk</b>      | Clears all AppleTalk statistics. When you clear statistics, the X-Pedition router sets the counters for the cleared statistics to 0, then begins accumulating the statistics again.                                   |
| <b>icmp</b>           | Clears all ICMPv4 statistics.<br><br><b>all</b> — Clear all statistics<br><br><b>input</b> — Clear input statistics<br><br><b>output</b> — Clear output statistics<br><br><b>disabled</b> — Clear disabled statistics |

|   |   |
|---|---|
| <b>icmp6</b>                            | <p>Clears the ICMPv6 statistics for one or all IPv6 interfaces. Specify either:</p> <p><i>&lt;IPv6 interface name&gt;</i> — Clear ICMPv6 statistics for this IPv6 interface</p> <p><b>all</b> — Clear ICMPv6 statistics for all IPv6 interfaces</p> |
| <b>port-errors</b>                      | <p>Clears error statistics for the specified LAN port, WAN module, or SmartTRUNK. Specify <b>all-ports</b> to clear error statistics for all ports.</p>   |
| <b>port-packets</b>                     | <p>Clears all port packet statistics for a specified POS module or list of POS modules. Specify <b>all-ports</b> to clear packet statistics for all ports.</p>  |
| <b>port-stats</b>                       | <p>Clears all normal (non-error) statistics for the specified port. Specify <b>all-ports</b> to clear port statistics for all ports.</p>  |
| <b>vlan all</b>   <i>&lt;string&gt;</i> | <p>Specify the keyword <b>all</b> to reset all counters used for per-VLAN packet accounting or enter the name of a specific VLAN.</p>   |

## Restrictions

None.



# statistics show appletalk

## Purpose

Displays various AppleTalk statistics.

## Format

**statistics show appletalk-atp|-ddp|-echo|-interface|-nbp|-routing|-zip**

## Mode

Enable.

## Parameters

|                  |  |
|------------------|--|
| <b>atp</b>       | Displays statistics for the AppleTalk Transaction Protocol.            |
| <b>ddp</b>       | Displays statistics for the Datagram Delivery Protocol                 |
| <b>echo</b>      | Displays statistics for the Echo Protocol.                             |
| <b>interface</b> | Displays interface statistics.   |
| <b>nbp</b>       | Displays statistics for the Name Binding Protocol (NBP).               |
| <b>routing</b>   | Displays statistics for the Routing Table Maintenance Protocol (RTMP). |
| <b>zip</b>       | Displays statistics for the Zone Information Protocol (ZIP).           |

## Restrictions

None.

# statistics show arp

## Purpose

Display address resolution protocol (ARP) statistics.

## Format

**statistics show arp** *<Interface Name>* | **all**

## Mode

Enable.

## Description

The **arp show statistics** command displays ARP statistics, such as the total number of ARP requests and replies.

## Parameters

|                               |   |
|-------------------------------|---|
| <i>&lt;Interface Name&gt;</i> | Displays ARP statistics for the specified interface.<br><br><b>Note:</b> Enterasys recommends that you use alphabetic characters when defining interface names—purely numeric interfaces will be interpreted as IP addresses. The X-Pedition router will display interface names up to 32 characters in length. |
| <b>all</b>                    | Displays ARP statistics for all router interfaces.  |

## Restrictions

None.

## Example

To display ARP statistics on interface 'en0':

```
xp# statistics show arp en0

Interface en0:
  1 requests sent
 19 replies sent
 0 proxy replies sent
Last 5 Requests Sent
----- no arp requests sent -----
Last 5 Replies Sent
134.141.179.129 | XP1  16:BF:21  |2000-04-17 13:12:49
134.141.179.129 | XP1  16:BF:21  |2000-04-17 13:50:15
134.141.179.129 | XP1  16:BF:21  |2000-04-17 15:32:32
134.141.179.129 | XP1  16:BF:21  |2000-04-17 16:17:19
134.141.179.129 | XP1  16:BF:21  |2000-04-17 11:12:44

Last 5 ARP packets received on wrong interface
----- no arp packets received on wrong interface -----
```

### Field Definitions

| Field  | Description  |
|--|--|
| requests sent                                  | Displays how many ARP requests have been sent out to an ARP server for address resolution.   |
| replies sent                                   | Displays how many ARP replies have been sent out to an ARP client in response to request packets.  |
| proxy replies sent                             | Displays how many proxy ARP replies have been sent out in response to request packets. A proxy router serving as a gateway to a subnet would respond with a proxy reply. |
| Last 5 Requests sent                           | Displays the last five ARP requests sent, including the following information: target MAC address, date and time sent.   |
| Last 5 Replies sent                            | Displays the last five ARP replies sent, including the following information: target IP address, date and time sent.   |
| Last 5 ARP packets received on wrong interface | Displays the last five ARP packets that has been received on the wrong interface.  |

## **statistics show framer**

### **Purpose**

Display framer statistics.

### **Format**

**statistics show framer** *<port list>*

### **Mode**

Enable.

### **Parameters**

---

|                          |                                       |
|--------------------------|---------------------------------------|
| <i>&lt;port list&gt;</i> | Specifies the port or group of ports. |
|--------------------------|---------------------------------------|

---

### **Restrictions**

None.

# statistics show icmp

## Purpose

Display statistics for Internet Control Message Protocol v4 (ICMPv4) messages.

## Format

**statistics show icmp**

## Mode

Enable.

## Parameters

None.

## Restrictions

None.

## Example

To display ICMP statistics:

```
xp# statistics show icmp
icmp:
  0 messages with bad code fields
  0 messages smaller than minimum length
  0 bad checksums
  0 messages with bad length
  0 message responses generated
```

### Field Definitions

| Field                         | Description   |
|-------------------------------|---|
| messages with bad code fields | Displays the number of ICMP messages processed by the router with a bad code field. The code field within the ICMP header uses a number to specify the message content of the ICMP message. An invalid number within the code field would show in this statistic parameter. |

| Field                                | Description   |
|--------------------------------------|---|
| messages smaller than minimum length | Displays the number of ICMP messages processed by the router that didn't meet a minimum length requirement.   |
| bad checksums                        | Displays the number of ICMP messages processed by the router with bad checksums. The checksum field within the ICMP header is used to verify that the message was transmitted error-free. A bad checksum indicates an ICMP message with errors. |
| messages with bad length             | Displays the number of ICMP messages processed by the router with bad or invalid length.  |
| message responses generated          | Displays the number of ICMP responses that have been generated by the router in response to ICMP messages.  |

# statistics show icmp6

## Purpose

Displays the summary and RFC 2466 ICMPv6 statistics for one or all IPv6 interfaces.

## Format

**statistics show icmp6** {<interface name> | **all** | **aggregate**} {**summary** | **detailed**}

## Mode

Enable.

## Description

This command can display ICMPv6 message statistics (similar to those displayed by the **statistics show icmp** command) and it also can display statistics for the MIB objects defined by RFC 2466, “Management Information Base for IP Version 6: ICMPv6 Group.”

Use the **statistics clear icmp6** {<interface name> | **all**} command to clear the ICMPv6 statistics.

## Parameters

---

|   |   |
|---|---|
| {<interface name>   <b>all</b>   <b>aggregate</b> } | Specifies which IPv6 interfaces to display statistics for.  |
|   | Enter the name of the IPv6 interface to display statistics for one interface.   |
|   | Enter <b>all</b> to display statistics for all IPv6 interfaces.   |
|   | Enter <b>aggregate</b> to sum the statistics over all IPv6 interfaces.  |
| <hr/>   |   |
| { <b>summary</b>   <b>detailed</b> }                | Specifies the type of statistics to display.  |
|   | Enter <b>summary</b> to display ICMPv6 statistics summarized by message type. If no type is specified, <b>summary</b> is assumed. |
|   | Enter <b>detailed</b> to display statistics for the objects defined in RFC 2466.  |

---

## Restrictions

None.

## Example

The following example displays summary statistics for all the IPv6 interfaces configured on the X-Pedition router. Descriptions of these fields follow this example.

```

xp# statistics show icmp6 all summary

interface name: lo1
      Received      Sent
Messages           0        0
Errors              0        0
Destination Unreachable  0        0
Echos              0        0
Echo Replies        0        0
MLD Reports         0        0
Router Advertisements  0        0
Neighbor Solicitations  0        0
Neighbor Advertisements  0        0

interface name: IPv6_1
      Received      Sent
Messages           0        6
Errors              0        0
Destination Unreachable  0        0
Echos              0        0
Echo Replies        0        0
MLD Reports         0        4
Router Solicitations  0        0
Router Advertisements  0        0
Neighbor Solicitations  0        2
Neighbor Advertisements  0        0

```

### Summary Field Definitions

| Field                   | Description  |
|-------------------------|--|
| Messages                | Total number of ICMPv6 messages sent and received                  |
| Errors                  | Total number of ICMPv6 error messages sent and received            |
| Destination Unreachable | Number of Destination Unreachable error messages sent and received |
| Echoes                  | Number of Echo Request messages sent and received                  |
| Echo Replies            | Number of Echo Reply messages sent and received                    |
| MLD Reports             | Number of Multicast Listener Discovery reports sent and received.  |
| Router Solicitations    | Number of Router Solicitation messages sent and received           |



|                         |   |
|-------------------------|---|
| Router Advertisements   | Number of Router Advertisements sent and received   |
| Neighbor Solicitations  | Number of Neighbor Solicitations sent and received  |
| Neighbor Advertisements | Number of Neighbor Advertisements sent and received |

The following example displays statistics defined in RFC 2466. Descriptions of the fields follow this example.

|  |         |                     |         |
|--|---------|---------------------|---------|
| <b>xp# statistics show icmp6 IPv6_1 detailed</b> |         |                     |         |
| interface name: IPv6_1                           |         |                     |         |
| RFC-2466 Counter                                 | Packets | RFC-2466 Counter    | Packets |
| InMsgs   | 0       | InErrors            | 0       |
| InDestUnreachs                                   | 0       | InAdminProhibs      | 0       |
| InTimeExcds                                      | 0       | InParamProblems     | 0       |
| InPktTooBigs                                     | 0       | InEchos             | 0       |
| InEchoReplies                                    | 0       | InRouterSolicits    | 0       |
| InRouterAdvs                                     | 0       | InNeighborSolicits  | 0       |
| InNeighborAdvs                                   | 0       | InRedirects         | 0       |
| InGroupMembQueries                               | 0       | InGroupMembResps    | 0       |
| InGroupMembReds                                  | 0       |                     |         |
| OutMsgs  | 6       | OutErrors           | 0       |
| OutDestUnreachs                                  | 0       | OutAdminProhibs     | 0       |
| OutTimeExcds                                     | 0       | OutParamProblems    | 0       |
| OutPktTooBigs                                    | 0       | OutEchos            | 0       |
| OutEchoReplies                                   | 0       | OutRouterSolicits   | 0       |
| OutRouterAdvs                                    | 0       | OutNeighborSolicits | 2       |
| OutNeighborAdvs                                  | 0       | OutRedirects        | 0       |
| OutGroupMembQueries                              | 0       | OutGroupMembResps   | 4       |
| OutGroupMembReds                                 | 0       |                     |         |

#### Field Definitions from RFC 2466

| Field          | Description   |
|----------------|---|
| InMsgs         | The total number of ICMP messages received by the interface which includes all those counted by InErrors. Note that this interface is the interface to which the ICMP messages were addressed which may not be necessarily the input interface for the messages |
| InErrors       | The number of ICMP messages which the interface received but determined as having ICMP-specific errors (bad ICMP checksums, bad length, etc.).  |
| InDestUnreachs | The number of ICMP Destination Unreachable messages received by the interface.  |

| Field              | Description  |
|--------------------|--|
| InAdminProhibs     | The number of ICMP destination unreachable/communication administratively prohibited messages received by the interface.   |
| InTimeExcds        | The number of ICMP Time Exceeded messages received by the interface.   |
| InParamProblems    | The number of ICMP Parameter Problem messages received by the interface.   |
| InPktTooBigs       | The number of ICMP Packet Too Big messages received by the interface.  |
| InEchos            | The number of ICMP Echo (request) messages received by the interface.  |
| InEchoReplies      | The number of ICMP Echo Reply messages received by the interface.  |
| InRouterSolicits   | The number of ICMP Router Solicit messages received by the interface.  |
| InRouterAdvs       | The number of ICMP Router Advertisement messages received by the interface.  |
| InNeighborSolicits | The number of ICMP Neighbor Solicit messages received by the interface.  |
| InNeighborAdvs     | The number of ICMP Neighbor Advertisement messages received by the interface.  |
| InRedirects        | The number of Redirect messages received by the interface.   |
| InGroupMembQueries | The number of ICMPv6 Group Membership Query messages received by the interface.  |
| InGroupMembResps   | The number of ICMPv6 Group Membership Response messages received by the interface.   |
| InGroupMembReds    | The number of ICMPv6 Group Membership Reduction messages received by the interface.  |
| OutMsgs            | The total number of ICMP messages which this interface attempted to send. Note that this counter includes all those counted by icmpOutErrors.  |
| OutErrors          | The number of ICMP messages which this interface did not send due to problems discovered within ICMP such as a lack of buffers. This value should not include errors discovered outside the ICMP layer such as the inability of IPv6 to route the resultant datagram. In some implementations there may be no types of error which contribute to this counter's value. |

| Field               | Description   |
|---------------------|---|
| OutDestUnreachs     | The number of ICMP Destination Unreachable messages sent by the interface.  |
| OutAdminProhibs     | Number of ICMP dest unreachable/communication administratively prohibited messages sent.                              |
| OutTimeExcds        | The number of ICMP Time Exceeded messages sent by the interface.  |
| OutParamProblems    | The number of ICMP Parameter Problem messages sent by the interface.  |
| OutPktTooBigs       | The number of ICMP Packet Too Big messages sent by the interface.   |
| OutEchos            | The number of ICMP Echo (request) messages sent by the interface.   |
| OutEchoReplies      | The number of ICMP Echo Reply messages sent by the interface.   |
| OutRouterSolicits   | The number of ICMP Router Solicitation messages sent by the interface.  |
| OutRouterAdvs       | The number of ICMP Router Advertisement messages sent by the interface.   |
| OutNeighborSolicits | The number of ICMP Neighbor Solicitation messages sent by the interface.  |
| OutNeighborAdvs     | The number of ICMP Neighbor Advertisement messages sent by the interface.   |
| OutRedirects        | The number of Redirect messages sent. For a host, this object will always be zero, since hosts do not send redirects. |
| OutGroupMembQueries | The number of ICMPv6 Group Membership Query messages sent.  |
| OutGroupMembResps   | The number of ICMPv6 Group Membership Response messages sent.   |
| OutGroupMembReds    | The number of ICMPv6 Group Membership Reduction messages sent.  |

## **statistics show ip**

### **Purpose**

Display Internet Protocol (IP) statistics for all IPv4 packets received or sent by the router software.

### **Format**

**statistics show ip**

### **Mode**

Enable.

### **Parameters**

None.

### **Restrictions**

IP statistics on hardware-routed IP flows are not included in the statistics displayed by this command. To see statistics collected by router hardware, use the **statistics show ip-interface** and **statistics show port-packets** commands.

## Example

To display IP statistics:

```
xp# statistics show ip
ip:
    78564 total packets received
    0 bad header checksums
    0 packets with size smaller than minimum
    0 packets with data size < data length
    0 packets with header length < data size
    0 packets with data length < header length
    0 packets with bad options
    0 packets with incorrect version number
    0 fragments received
    0 fragments dropped (dup or out of space)
    0 fragments dropped after timeout
    0 packets reassembled ok
    2984 packets for this host
    0 packets for unknown/unsupported protocol
    0 packets forwarded
    75580 packets not forwardable
    0 redirects sent
    2120 packets sent from this host
    0 packets sent with fabricated ip header
    0 output packets dropped due to no bufs, etc.
    0 output packets discarded due to no route
    0 output datagrams fragmented
    0 fragments created
    0 datagrams that can't be fragmented
```

### Field Definitions

| Field                               | Description  |
|-------------------------------------|--|
| total packets received              | The total number of IP packets forwarded and dropped by the router.  |
| bad header checksums                | The number of IP packets received with bad checksums. The checksum field within the IP header is used to verify that the packet was transmitted error-free. A bad checksum indicates an IP packet with errors. |
| packets w/size smaller than minimum | The number of IP packets received that didn't meet a minimum length requirement.   |
| packets w/data size < data length   | The number of IP packets received that contain a data size smaller than the data length specified in the IP header.  |

| Field                                    | Description  |
|--|--|
| packets w/header length < data size      | The number of IP packets received that contain an IP header length smaller than the data size within the packet.   |
| packets w/data length < header length    | The number of IP packets received that contain a data length smaller than the IP header length.  |
| packets w/incorrect version number       | The number of IP packets received with an incorrect IP version number. The IP version number field in the IP header is used to specify whether the packet is formatted for IPv4 or IPv6. |
| fragments received                       | The number of datagram fragments received by the router.   |
| fragments dropped                        | The number of datagram fragments dropped by the router.  |
| fragments dropped after timeout          | The number of datagram fragments dropped by the router after a timeout.  |
| packets reassembled ok                   | The number of IP packets containing fragmented datagrams that were reassembled successfully by the router.   |
| packets for this host                    | The total number of IP packets received that were intended for the router as the destination.  |
| packets for unknown protocol             | The number of IP packets received that are of an unknown or unsupported routed protocol.   |
| packets forwarded                        | The number of IP packets received that were forwarded on to another host.  |
| packets not forwardable                  | The total number of IP packets received that the router could not forward on to another host.  |
| redirects sent                           | The number of redirects sent by the router.  |
| packets sent from this host              | The total number of IP packets sent by the router.   |
| packets sent w/fabricated ip header      | The number of IP packets sent after attaching an IP header to the packet.  |
| output packets dropped due to no bufs    | The number of IP packets dropped before being sent due to a lack of output buffer space.   |
| output packets discarded due to no route | The number of IP packets dropped before being sent due to a lack of IP routing information.  |

---

| Field                              | Description   |
|------------------------------------|---|
| output datagrams fragmented        | The number of datagrams that were fragmented into two or more IP packets before being sent out by the router. |
| fragments created                  | The number of datagram fragments created.   |
| datagrams that can't be fragmented | The number of datagrams that were not successfully fragmented into two or more IP packets.                    |

# statistics show ipv6

## Purpose

Displays IPv6 statistics for all packets received or sent by the router software.

## Format

**statistics show ipv6** {<interface name> | **all** | **aggregate**} {**summary** | **detailed**}

## Mode

Enable.

## Description

This command can display IPv6 packet statistics (similar to those displayed by the **statistics show ip** command) when you use the **summary** keyword. This command can also can display statistics for the MIB objects defined by RFC 2465, “Management Information Base for IP Version 6: Textual Conventions and General Group,” when you use the **detailed** keyword.

## Parameters

|   |   |
|---|---|
| {<interface name>   <b>all</b>   <b>aggregate</b> } | Specifies which IPv6 interfaces to display statistics for.  |
|   | Enter the name of the IPv6 interface to display statistics for one interface.   |
|   | Enter <b>all</b> to display statistics for all IPv6 interfaces.   |
|   | Enter <b>aggregate</b> to sum the statistics over all IPv6 interfaces. (The output of the <b>statistics show ip</b> command is aggregated over all interfaces.) |
| { <b>summary</b>   <b>detailed</b> }                | Specifies the type of statistics to display.  |
|   | Enter <b>summary</b> to display summary statistics (similar to those displayed for IPv4).   |
|   | Enter <b>detailed</b> to display the objects defined in RFC 2465.   |

## Restrictions

IP statistics on hardware-routed IP flows are not included in the statistics displayed by this command. To see statistics collected by router hardware, use the **statistics show ipv6-interface** and **statistics show port-packets** commands.



## Example

The following example displays summary statistics for the IPv6 interface named IPv6\_1. The fields displayed are self-explanatory.

```
xp(statistics-show)# ipv6 IPv6_1 summary
```

|                                   |   |
|-----------------------------------|---|
| interface name: IPv6_1            |   |
| Packets Received                  | 0 |
| Received Header Errors            | 0 |
| Received Address Errors           | 0 |
| Datagrams Forwarded               | 0 |
| Unknown Protocols Received        | 0 |
| Received Packets Discarded        | 0 |
| Received Packets Delivered        | 0 |
| Output Requests                   | 6 |
| Routing Discards                  | 0 |
| Discarded Output Packets          | 0 |
| Output Packet No Route            | 0 |
| Reassembly Required               | 0 |
| Reassembly Successful             | 0 |
| Reassembly Failures               | 0 |
| Datagrams Successfully Fragmented | 0 |
| Datagrams Failing Fragmentation   | 0 |
| Fragments Created                 | 0 |

The following example displays statistics for the MIB objects described in RFC 2465 for the IPv6 interface named IPv6\_1. The output of this command displays statistics for the IPv6 traffic processed by the router software. To see statistics for the IPv6 traffic forwarded directly by the hardware, use the **statistics show ipv6-interface** command. Descriptions of the fields displayed follow this example.

```

xp# statistics show ipv6 IPv6_1 detailed

```

```

interface name: IPv6_1

```

| RFC-2465 Counter | Packets |
|------------------|---------|
| InReceives       | 0       |
| InHdrErrors      | 0       |
| InTooBigErrors   | 0       |
| InNoRoutes       | 0       |
| InAddrErrors     | 0       |
| InUnknownProtos  | 0       |
| InTruncatedPkts  | 0       |
| InDiscards       | 0       |
| InDelivers       | 0       |
| OutForwDatagrams | 0       |
| OutRequests      | 6       |
| OutDiscards      | 0       |
| OutFragOKs       | 0       |
| OutFragFails     | 0       |
| OutFragCreates   | 0       |
| ReasmReqds       | 0       |
| ReasmOKs         | 0       |
| ReasmFails       | 0       |
| InMcastPkts      | 0       |
| OutMcastPkts     | 6       |

```

ipv6 stats cleared: * Never Cleared *

```

#### Field Descriptions from RFC 2465

| Field          | Description   |
|----------------|---|
| InReceives     | The total number of input datagrams received by the interface, including those received in error.   |
| InHdrErrors    | The number of input datagrams discarded due to errors in their IPv6 headers, including version number mismatch, other format errors, hop count exceeded, errors discovered in processing their IPv6 options, etc. |
| InTooBigErrors | The number of input datagrams that could not be forwarded because their size exceeded the link MTU of outgoing interface.   |
| InNoRoutes     | The number of input datagrams discarded because no route could be found to transmit them to their destination.  |

|                  |  |
|------------------|--|
| InAddrErrors     | The number of input datagrams discarded because the IPv6 address in their IPv6 header's destination field was not a valid address to be received at this entity. This count includes invalid addresses (e.g., ::0) and unsupported addresses (e.g., addresses with unallocated prefixes). For entities which are not IPv6 routers and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address. |
| InUnknownProtos  | The number of locally-addressed datagrams received successfully but discarded because of an unknown or unsupported protocol. This counter is incremented at the interface to which these datagrams were addressed which might not be necessarily the input interface for some of the datagrams.  |
| InTruncatedPkts  | The number of input datagrams discarded because datagram frame didn't carry enough data.   |
| InDiscards       | The number of input IPv6 datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (e.g., for lack of buffer space). Note that this counter does not include any datagrams discarded while awaiting re-assembly.  |
| InDelivers       | The total number of datagrams successfully delivered to IPv6 user-protocols (including ICMP). This counter is incremented at the interface to which these datagrams were addressed which might not be necessarily the input interface for some of the datagrams.   |
| OutForwDatagrams | The number of output datagrams which this entity received and forwarded to their final destinations. In entities which do not act as IPv6 routers, this counter will include only those packets which were Source-Routed via this entity, and the Source-Route processing was successful. Note that for a successfully forwarded datagram the counter of the outgoing interface is incremented.  |
| OutRequests      | The total number of IPv6 datagrams which local IPv6 user-protocols (including ICMP) supplied to IPv6 in requests for transmission. Note that this counter does not include any datagrams counted in OutForwDatagrams.  |
| OutDiscards      | The number of output IPv6 datagrams for which no problem was encountered to prevent their transmission to their destination, but which were discarded (e.g., for lack of buffer space). Note that this counter would include datagrams counted in OutForwDatagrams if any such packets met this (discretionary) discard criterion.   |
| OutFragOKs       | The number of IPv6 datagrams that have been successfully fragmented at this output interface.  |

|                |  |
|----------------|--|
| OutFragFails   | The number of IPv6 datagrams that have been discarded because they needed to be fragmented at this output interface but could not be.  |
| OutFragCreates | The number of output datagram fragments that have been generated as a result of fragmentation at this output interface.  |
| ReasmReqds     | The number of IPv6 fragments received which needed to be reassembled at this interface. Note that this counter is incremented at the interface to which these fragments were addressed which might not be necessarily the input interface for some of the fragments.   |
| ReasmOKs       | The number of IPv6 datagrams successfully reassembled. Note that this counter is incremented at the interface to which these datagrams were addressed which might not be necessarily the input interface for some of the fragments.  |
| ReasmFails     | The number of failures detected by the IPv6 re- assembly algorithm (for whatever reason: timed out, errors, etc.). Note that this is not necessarily a count of discarded IPv6 fragments since some algorithms (notably the algorithm in RFC 815) can lose track of the number of fragments by combining them as they are received. This counter is incremented at the interface to which these fragments were addressed which might not be necessarily the input interface for some of the fragments. |
| InMcastPkts    | The number of multicast packets received by the interface  |
| OutMcastPkts   | The number of multicast packets transmitted by the interface   |

# statistics show ip-interface

## Purpose

Display IP interface statistics.

**Note:** Interface statistics originate from hardware counters on a port basis. Therefore, two interfaces on the same physical port will have identical statistics.

## Format

**statistics show ip-interface** <string>|**all** [**packets**] [**bytes**] [**errors**] [**input**] [**output**]| **verbose**

## Mode

Enable.

## Parameters

|                      |  |
|----------------------|--|
| <string>  <b>all</b> | <p>Specifies the name of an interface. Specify <b>all</b> to display IP statistics for all interfaces.</p> <p><b>Note:</b> The <b>statistics show ip-interface</b> command cannot display statistics for any interface that contains an ATM port. If a user attempts to display this information, the router will display “n/a” on the console.</p> <p><b>Note:</b> Enterasys recommends that you use alphabetic characters when defining interface names—purely numeric interfaces will be interpreted as IP addresses. The X-Pedition router will display interface names up to 32 characters in length.</p> |
| <b>packets</b>       | Specify this optional parameter to display the number of packets that have passed through the interface.   |
| <b>bytes</b>         | Specify this optional parameter to display the number of bytes that have passed through the interface.   |
| <b>errors</b>        | Specify this optional parameter to display the number of packets with errors detected through the interface.   |
| <b>input</b>         | Specify this optional parameter to display interface statistics for the input side.  |
| <b>output</b>        | Specify this optional parameter to display interface statistics for the output side.   |

|                |  |
|----------------|--|
| <b>verbose</b> | Specify this optional parameter to display statistics on the number of packets, bytes, and errors on both the input and output sides of the interface. |
|----------------|--|

## Restrictions

The **statistics show ip-interface** command cannot display statistics for any interface that contains an ATM port. If a user attempts to display this information, the router will display “n/a” on the console.

## Example

To display interface statistics on interface ‘en0’:

```
xp# statistics show ip-interface en0 verbose

Name In-frames Out-frames In-bytes Out-bytes In-errors Out-errors
en0 0      0      0      0      0      0
```

**Note:** If an asterisk (\*) appears next to the interface name, the network is administratively or operationally down.

### Field Definitions

| Field      | Description   |
|------------|---|
| In-frames  | Displays the number of packets that have entered the interface.             |
| Out-frames | Displays the number of packets that have exited the interface.              |
| In-bytes   | Displays the number of bytes that have entered the interface.               |
| Out-bytes  | Displays the number of bytes that have exited the interface.                |
| In-errors  | Displays the number of packets with errors detected entering the interface. |
| Out-errors | Displays the number of packets with errors detected exiting the interface.  |

**Note:** Interface statistics originate from hardware counters on a port basis. Therefore, two interfaces on the same physical port will have identical statistics.

# statistics show ipv6-interface

## Purpose

Displays the summary and RFC 2465 statistics for one or all IPv6 interfaces.

## Format

**statistics show ipv6-interface** {<interface name> | **all**} {[**packets**] [**bytes**] [**errors**] | **verbose** | **detailed**}

## Mode

Enable.

## Description

This command displays ingress counters for IPv6 traffic forwarded directly by the hardware. Egress counters are not available. To see statistics for the IPv6 traffic forwarded by the router software, use the **statistics show ipv6** command.

Use the **statistics clear ipv6-interface** {<interface name> | **all**} command to clear the statistics for an IPv6 interface.

## Parameters

|                               |  |
|-------------------------------|--|
| <interface name>   <b>all</b> | Specifies the interface to display statistics for.<br><br>Enter the IPv6 interface name to display statistics for one interface, or enter the <b>all</b> keyword to display statistics for all interfaces. |
| <b>packets</b>                | Display the number of packets received on the interface.   |
| <b>bytes</b>                  | Display the number of bytes received on the interface.   |
| <b>errors</b>                 | Display the number of errors received on the interface.  |
| <b>verbose</b>                | Display verbose output.  |
| <b>detailed</b>               | Display all supported RFC 2465 counters.   |

## Restrictions

None.

## Example

The following example displays the verbose output for the IPv6 interface named “IPv6\_1.”

```
xp(statistics-show)# ipv6-interface IPv6_1 verbose
```

| Name   | In-frames | In-bytes | In-errors |
|--------|-----------|----------|-----------|
| IPv6_1 | 0         | 0        | 0         |

The following example displays the detailed output for the interface named intf1. This output shows the contents of the hardware counters, showing statistics for the IPv6 traffic forwarded directly by the hardware.

```
xp# statistics show ipv6-interface intf1 detailed
```

|                       |                           |       |
|-----------------------|---------------------------|-------|
| interface name: intf1 | serviced by FEA in slot-6 |       |
| RFC-2465 Counter      | Packets                   | Bytes |
| InReceives            | 35                        | 4470  |
| InHdrErrors           | 0                         | 0     |
| InTooBigErrors        | 0                         | 0     |
| InNoRoutes            | 0                         | 0     |
| InAddrErrors          | 0                         | 0     |
| InUnknownProtos       | 0                         | 0     |
| InTruncatedPkts       | 0                         | 0     |
| InDiscards            | 0                         | 0     |
| InDelivers            | 43                        | N/A   |
| OutRequests           | 50                        | N/A   |
| OutFragFails          | 0                         | 0     |
| InMcastPkts           | 45                        | N/A   |
| OutMcastPkts          | 48                        | N/A   |

ipv6 interface stats cleared: \* Never Cleared \*

### Field Descriptions from RFC 2465

| Field          | Description   |
|----------------|---|
| InReceives     | The total number of input datagrams received by the interface, including those received in error.   |
| InHdrErrors    | The number of input datagrams discarded due to errors in their IPv6 headers, including version number mismatch, other format errors, hop count exceeded, errors discovered in processing their IPv6 options, etc. |
| InTooBigErrors | The number of input datagrams that could not be forwarded because their size exceeded the link MTU of outgoing interface.   |
| InNoRoutes     | The number of input datagrams discarded because no route could be found to transmit them to their destination.  |



|                 |  |
|-----------------|--|
| InAddrErrors    | The number of input datagrams discarded because the IPv6 address in their IPv6 header's destination field was not a valid address to be received at this entity. This count includes invalid addresses (e.g., ::0) and unsupported addresses (e.g., addresses with unallocated prefixes). For entities which are not IPv6 routers and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address. |
| InUnknownProtos | The number of locally-addressed datagrams received successfully but discarded because of an unknown or unsupported protocol. This counter is incremented at the interface to which these datagrams were addressed which might not be necessarily the input interface for some of the datagrams.  |
| InTruncatedPkts | The number of input datagrams discarded because datagram frame didn't carry enough data.   |
| InDiscards      | The number of input IPv6 datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (e.g., for lack of buffer space). Note that this counter does not include any datagrams discarded while awaiting re-assembly.  |
| InDelivers      | The total number of datagrams successfully delivered to IPv6 user-protocols (including ICMP). This counter is incremented at the interface to which these datagrams were addressed which might not be necessarily the input interface for some of the datagrams.   |
| OutRequests     | The total number of IPv6 datagrams which local IPv6 user-protocols (including ICMP) supplied to IPv6 in requests for transmission. Note that this counter does not include any datagrams counted in OutForwDatagrams.  |
| OutFragFails    | The number of IPv6 datagrams that have been discarded because they needed to be fragmented at this output interface but could not be.  |
| InMcastPkts     | The number of multicast packets received by the interface  |
| OutMcastPkts    | The number of multicast packets transmitted by the interface   |

## statistics show ip-routing

### Purpose

Display unicast IPv4 routing statistics.

### Format

**statistics show ip-routing**

### Mode

Enable.

### Parameters

None.

### Restrictions

None.

### Example

To display routing statistics:

```
xp# statistics show ip-routing
routing:
  0 bad routing redirects
  0 dynamically created routes
  0 new gateways due to redirects
  1141 destinations found unreachable
  0 uses of a wildcard route
```

### Field Definitions

| Field                 | Description  |
|-----------------------|--|
| bad routing redirects | Displays the number of bad redirects have occurred. A redirect occurs in the case where the destination interface is the same as the source interface. |

---

| Field                          | Description  |
|--------------------------------|--|
| dynamically created routes     | Displays the number of IP routes have been created using a routing protocol, as opposed to static routes which are user-defined.   |
| new gateways due to redirects  | Displays the number of new gateways have been added into the routing table due to redirects.   |
| destinations found unreachable | Displays the number of destination addresses that have been found to be unreachable in the routing table. A destination may be unreachable due to the route being expired or being unavailable due to network changes. |
| uses of a wildcard route       | Displays the number of times that a wildcard route has been used to forward a packet onto the next-hop destination.  |

## statistics show ipv6-routing

### Purpose

Displays unicast IPv6 routing statistics.

### Format

**statistics show ipv6-routing**

### Mode

Enable.

### Parameters

None.

### Restrictions

None.

### Example

The following example displays IPv6 routing statistics.

```
xp(statistics-show)# ipv6-routing
ipv6-routing:
  0 bad routing redirects
  0 dynamically created routes
  0 new gateways due to redirects
  6 destinations found unreachable
  0 uses of a wildcard route
```

### Field Definitions

| Field                 | Description  |
|-----------------------|--|
| bad routing redirects | Displays the number of bad redirects have occurred. A redirect occurs in the case where the destination interface is the same as the source interface. |

---

| Field                          | Description  |
|--------------------------------|--|
| dynamically created routes     | Displays the number of IPv6 routes have been created using a routing protocol, as opposed to static routes which are user-defined.   |
| new gateways due to redirects  | Displays the number of new gateways have been added into the routing table due to redirects.   |
| destinations found unreachable | Displays the number of destination addresses that have been found to be unreachable in the routing table. A destination may be unreachable due to the route being expired or being unavailable due to network changes. |
| uses of a wildcard route       | Displays the number of times that a wildcard route has been used to forward a packet onto the next-hop destination.  |

## **statistics show ipx**

### **Purpose**

Display internetwork packet exchange (IPX) statistics.

### **Format**

**statistics show ipx**

### **Mode**

Enable.

### **Parameters**

None.

### **Restrictions**

If you configure multiple protocol types (e.g., IP and IPX) on the same port(s), interface statistics collected for the port(s) will not be accurate—both protocols will gather port statistics.

## Example

To display IPX statistics:

```
xp# statistics show ipx
ipx:
  0 total packets received
  0 packets with bad checksums
  0 packets smaller than advertised
  0 packets smaller than a header
  0 packets forwarded
  0 packets not forwardable
  0 packets for this host
  0 packets sent from this host
  0 packets dropped due to no bufs, etc.
  0 packets discarded due to no route
  0 packets too big
  0 packets with too many hops
  0 packets of type 20
  0 packets discarded due to infiltering
  0 packets discarded due to outfiltering
  0 packets with misc protocol errors
  0 rip packets discarded due to socket buffer full
  0 sap packets discarded due to socket buffer full
  0 rip req packets discarded due to socket buffer full
  0 sap gns packets discarded due to socket buffer full
  0 packets discarded due to port of entry zero
  0 packets discarded due to sourced by us
```

### Field Definitions

| Field                           | Description  |
|---------------------------------|--|
| total packets received          | Displays the total number of IPX packets received by the router, including all forwarded and dropped packets.  |
| bad header checksums            | Displays the number of IPX packets received by the router with bad checksums. The checksum field within the IPX header is used to verify that the packet was transmitted error-free. A bad checksum indicates an IPX packet with errors. |
| packets smaller than advertised | Displays the number of IPX packets received by the router that are smaller than what the header indicates as the size.   |
| packets smaller than a header   | Displays the number of IPX packets received by the router that are smaller than the IPX header.  |

| Field                                 | Description  |
|---------------------------------------|--|
| packets forwarded                     | Displays the number of IPX packets received by the router that have been forwarded onto the next-hop destination.  |
| packets not forwardable               | Displays the total number of IPX packets received by the router that could not be forwarded onto another host.   |
| packets for this host                 | Displays the total number of IPX packets received that were intended for the router as the destination.  |
| packets sent from this host           | Displays the total number of IPX packets sent out by the router.   |
| packets dropped due to no bufs        | Displays the total number of IPX packets dropped before being sent out by the router because of lack of buffer space.  |
| packets discarded due to no route     | Displays the total number of IPX packets dropped before being sent out by the router because of no IPX routing information.  |
| packets too big                       | Displays the total number of IPX packets that exceed a size threshold.   |
| packets with too many hops            | Displays the total number of IPX packets that exceed a number of hops threshold.   |
| packets of type 20                    | Displays the total number of NetBIOS packets.  |
| packets discarded due to infiltering  | Displays the total number of incoming IPX packets that have been discarded due to filtering. Filtering is based upon various access control lists (ACL) such as IPX ACL, SAP ACL, and RIP ACL. |
| packets discarded due to outfiltering | Displays the total number of outgoing IPX packets that have been discarded due to filtering. Filtering is based upon various access control lists (ACL) such as IPX ACL, SAP ACL, and RIP ACL. |
| packets with misc protocol errors     | Displays the total number of IPX packets containing routing protocol errors.   |
| rip packets discarded                 | Displays the total number of Routing Information Protocol (RIP) packets that have been discarded due to the socket buffer being full.  |
| sap packets discarded                 | Displays the total number of Server Advertisement Protocol (SAP) packets that have been discarded due to the socket buffer being full.   |



---

| Field                                       | Description  |
|---|--|
| rip req packets discarded                   | Displays the total number of Routing Information Protocol (RIP) request packets that have been discarded due to the socket buffer being full.                    |
| sap gns packets discarded                   | Displays the total number of Service Advertisement Protocol (SAP) Get Nearest Server (GNS) packets that have been discarded due to the socket buffer being full. |
| packets discarded due to port of entry zero | Displays the total number of received IPX packets that were discarded because of a poe value of 0 in the packet header.  |
| packets discarded due to sourced by us      | Displays the total number of received IPX packets that have been discarded because they were sent by us.   |

# statistics show ipx-interface

## Purpose

Display IPX interface statistics.

**Note:** Interface statistics originate from hardware counters on a port basis. Therefore, two interfaces on the same physical port will have identical statistics.

## Format

**statistics show ipx-interface** <string>|all [packets] [bytes] [errors] [input] [output]|verbose

## Mode

Enable.

## Parameters

|                |   |
|----------------|---|
| <string> all   | Specifies the name of an interface. Specify <b>all</b> to display IPX statistics for all interfaces.<br><br><b>Note:</b> Enterasys recommends that you use alphabetic characters when defining interface names—purely numeric interfaces will be interpreted as IP addresses. The X-Pedition router will display interface names up to 32 characters in length. |
| <b>packets</b> | Specify this optional parameter to display the number of packets that have passed through the interface.  |
| <b>bytes</b>   | Specify this optional parameter to display the number of bytes that have passed through the interface.  |
| <b>errors</b>  | Specify this optional parameter to display the number of packets with errors detected through the interface.  |
| <b>input</b>   | Specify this optional parameter to display interface statistics for the input side.   |
| <b>output</b>  | Specify this optional parameter to display interface statistics for the output side.  |
| <b>verbose</b> | Specify this optional parameter to display statistics on the number of packets, bytes, and errors on both the input and output sides of the interface.  |

## Restrictions

None.

## Example

To display interface statistics on interface 'en0':

```
xp# statistics show ipx-interface en0 verbose
```

| Name | In-frames | Out-frames | In-bytes | Out-bytes | In-errors | Out-errors |
|------|-----------|------------|----------|-----------|-----------|------------|
| en0  | 0         | 0          | 0        | 0         | 0         | 0          |

### Field Definitions

| Field      | Description   |
|------------|---|
| In-frames  | Displays the number of packets that have entered the interface.             |
| Out-frames | Displays the number of packets that have exited the interface.              |
| In-bytes   | Displays the number of bytes that have entered the interface.               |
| Out-bytes  | Displays the number of bytes that have exited the interface.                |
| In-errors  | Displays the number of packets with errors detected entering the interface. |
| Out-errors | Displays the number of packets with errors detected exiting the interface.  |

**Note:** Interface statistics originate from hardware counters on a port basis. Therefore, two interfaces on the same physical port will have identical statistics.

# statistics show ipx-routing

## Purpose

Display IPX routing statistics.

## Format

**statistics show ipx-routing**

## Mode

Enable.

## Parameters

None.

## Restrictions

None.

## Example

To display routing statistics:

```
xp# statistics show ipx-routing
routing:
  0 bad routing redirects
  0 dynamically created routes
  0 new gateways due to redirects
  1141 destinations found unreachable
  0 uses of a wildcard route
```

**Field Definitions**

| Field                          | Description  |
|--------------------------------|--|
| bad routing redirects          | Displays the number of bad redirects have occurred. A redirect occurs in the case where the destination interface is the same as the source interface.   |
| dynamically created routes     | Displays the number of IPX routes have been created using a routing protocol, as opposed to static routes which are user-defined.  |
| new gateways due to redirects  | Displays the number of new gateways have been added into the routing table due to redirects.   |
| destinations found unreachable | Displays the number of destination addresses that have been found to be unreachable in the routing table. A destination may be unreachable due to the route being expired or being unavailable due to network changes. |
| uses of a wildcard route       | Displays the number of times that a wildcard route has been used to forward a packet onto the next-hop destination.  |

## **statistics show most-active**

### **Purpose**

Display active tasks.

### **Format**

**statistics show most-active**

### **Mode**

Enable.

### **Parameters**

None.

### **Restrictions**

None.

## Example

To display active tasks:

```
xp# statistics show most-active

Timestamp: 2000-04-25 17:56:32
CPU Idle : 98% (since system startup 441751425.0 sec ago)
NAME          USAGE %    RELATIVE %
-----
STP_T         0.2        47.65
PHY_POLL      0.0        17.57
L2_AGE_T      0.0        7.90
L3_AGE_T      0.0        7.10
IPC           0.0        4.60
CONS_T        0.0        4.25
STATS_T       0.0        3.96
TNTASK        0.0        2.41
SYSTEM H      0.0        0.88
HBT_T         0.0        0.82
SNMP          0.0        0.67
GATED         0.0        0.58
IPXROUTE      0.0        0.48
CONS2T        0.0        0.33
LOWEST        0.0        0.25
PPP_TASK      0.0        0.24
PINGER_T      0.0        0.11
L2_LRN_T      0.0        0.07
CDP_T         0.0        0.02
LGRP_T        0.0        0.00
MPS           0.0        0.00
TNETD         0.0        0.00
ETHH          0.0        0.00
NI H          0.0        0.00
ARP_T         0.0        0.00
HSWAP         0.0        0.00
IPRED_T       0.0        0.00
SYS_TK        0.0        0.00
SNMP_CF       0.0        0.00
WAN_TOD_      0.0        0.00
DHCP          0.0        0.00
BOUNCE        0.0        0.00
IP_T          0.0        0.00
IPX_T         0.0        0.00
PHX_T         0.0        0.00
NTP           0.0        0.00
ERROR_LO      0.0        0.00
L3_ACL_T      0.0        0.00
MCAST         0.0        0.00
PROFILE       0.0        0.00
PRI_L3MD      0.0        0.00
L3_RL_T       0.0        0.00
```

# statistics show multicast

## Purpose

Display multicast statistics.

## Format

**statistics show multicast**

## Mode

Enable.

## Parameters

None.

## Restrictions

None.

## Example

To display multicast statistics:

```
xp# statistics show multicast
multicast forwarding:
    0 multicast forwarding cache lookups
    0 multicast forwarding cache misses
    0 upcalls to mrouterd
    0 upcall queue overflows
    0 upcalls dropped due to full socket buffer
    0 cache cleanups
    0 datagrams with no route for origin
    0 datagrams arrived with bad tunneling
    0 datagrams could not be tunneled
    0 datagrams arrived on wrong interface
    0 datagrams selectively dropped
    0 datagrams dropped due to queue overflow
    0 datagrams dropped for being too large
```



**Field Definitions**

| Field                                     | Description   |
|---|---|
| multicast forwarding cache lookups        | This counter increments whenever a multicast packet does a “route” lookup in software. If a multicast packet hits the CPU and a forwarding decision already exists, the X-Pedition router increments this counter.    |
| multicast forwarding cache misses         | This counter increments whenever the CPU receives an unlearned multicast packet. A cache miss can also result in an upcall to DVMRP or PIM.   |
| upcalls to mroute                         | Number of multicast packets sent to mroute (DVMRP) for learning.  |
| upcall queue overflows                    | Number of times a packet was unsuccessfully queued for learning. Usually a result of learning many flows simultaneously.  |
| upcalls dropped due to full socket buffer | DVMRP and PIM use a routing socket to communicate with the kernel. If the X-Pedition router drops any packets queued for learning as the result of insufficient buffer space on that socket, this counter increments. |
| cache cleanups                            | Number of upcalls that timeout before servicing the upcall.   |
| datagrams with no route for origin        | The RPF check on this source address yielded no known route. In unicast this would produce an “ICMP host unreachable” message.  |
| datagrams arrived with bad tunneling      | When using IP in IP tunneling with DVMRP enabled, this field indicates that the tunneled packet was either corrupted or improperly encapsulated.  |
| datagrams could not be tunneled           | Number of packets that could not be tunneled. This is usually the result of the DF bit being set and the MTU of the tunnel interface being smaller than the size of the datagram + encapsulating IP header.           |
| datagrams arrived on wrong interface      | Number of packets received on an interface that is not the RPF upstream interface for the flow.   |
| datagrams selectively dropped             | Number of packets dropped when the router is unable to queue a packet ready for transmit. This only occurs when the router is forwarding a large number of multicast packets and is very congested.                   |
| datagrams dropped due to queue overflow   | Number of packets dropped as the result of the CPU’s forwarding queue being full.   |
| datagrams dropped for being too large     | Number of packets dropped because they were larger than the MTU on the outbound interface, and the DF bit was set.  |

## statistics show port-errors

### Purpose

Display port error statistics.

### Format

**statistics show port-errors** <port/SmartTRUNK-list>|**all-ports**

### Mode

Enable.

### Parameters

|                        |   |
|------------------------|---|
| <port/SmartTRUNK-list> | Specifies a specific port or SmartTRUNK list.                     |
| <b>all-ports</b>       | Display port error statistics for all physical and logical ports. |

### Restrictions

None.

## Example

To display port error statistics on port et.2.1:

|  |   |                            |   |
|--|---|----------------------------|---|
| xp# statistics show port-errors et.2.1 |   |                            |   |
| Port: et.2.1                           |   |                            |   |
| ----                                   |   |                            |   |
| Error Stats                            |   | Error Stats                |   |
| -----                                  |   | -----                      |   |
| CRC errors                             | 0 | Carrier sense errors       | 0 |
| Single collision (tx OK)               | 0 | Many collisions (tx OK)    | 0 |
| Many collisions (drop)                 | 0 | Late collisions            | 0 |
| Long frames >1518 bytes                | 0 | Invalid long frames        | 0 |
| Short frames <64 bytes                 | 0 | Alignment errors           | 0 |
| Deferred transmissions                 | 0 | Transmit underruns         | 0 |
| IP - bad version                       | 0 | IP - bad checksum          | 0 |
| IP - bad header                        | 0 | IP - small datagram        | 0 |
| IP - expand TTL ring                   | 0 | IPX - bad header           | 0 |
| Non-IP/IPX protocol                    | 0 | Invalid MAC encap.         | 0 |
| Internal frame tx error                | 0 | Internal frame rx error    | 0 |
| Input buffer overflow                  | 0 | Packet request overflow    | 0 |
| Out buffer (low) overflow              | 0 | Out buffer (med) overflow  | 0 |
| Out buffer (high) overflow             | 0 | Out buffer (ctrl) overflow | 0 |
| Input VLAN drop frame                  | 0 |                            |   |
| Error stats cleared * Never Cleared *  |   |                            |   |

### Field Definitions

| Field                    | Description  |
|--------------------------|--|
| CRC errors               | Displays the total frames received that are an integral number of octets in length but failed the FCS check.   |
| Single collision (tx OK) | Displays the total number of frames that successfully transmitted after only one collision.  |
| Many collisions (drop)   | Displays the total number of frames dropped after more than one collision.   |
| Long frames >1518 bytes  | Displays the total number of frames received that exceeded the maximum permitted frame size (1518 bytes) but were otherwise acceptable because they passed FCS checks and were an integral number of octets in length. |
| Short frames <64 bytes   | Displays the total number of frames that received that were less than 64 bytes in length.  |
| Deferred transmissions   | Displays the total number of frames for which the first transmission attempt was delayed because the medium was busy. This count does not include frames involved in collisions.                                       |

| Field                      | Description   |
|----------------------------|---|
| IP - bad version           | Displays the total number of IP packets dropped because the IP version was not equal to 4.  |
| IP - bad header            | Displays the total number of IP packets dropped because the header length was less than 20 bytes.   |
| IP - expand TTL ring       | Displays the total number of IP packets dropped due to expanding TTL.   |
| Non-IP/IPX protocol        | Displays the total number of packets dropped due to an unknown or bad Layer-3 protocol.   |
| Internal frame tx error    | Displays the total number of transmit frames dropped due to an OWB resync or internal transmit error.   |
| Input buffer overflow      | Displays the total number of frames dropped due to the IPP Interface Buffer full condition.   |
| Out buffer (low) overflow  | Displays the total number of frames dropped because the low priority Output Packet Manager was full.  |
| Out buffer (high) overflow | Displays the total number of frames dropped because the high priority Output Packet Manager was full.   |
| Input VLAN drop frame      | Displays the total number of frames dropped due to a VLAN table.  |
| Carrier sense errors       | Displays the number of times that the carrier sense condition was lost or never asserted when attempting to transmit a frame on a particular interface. This count increments at most once per transmission attempt, even if the carrier sense condition fluctuates during the attempt. |
| Many collisions (tx OK)    | Displays the total number of frames successfully transmitted after more than one collision.   |
| Late collisions            | Displays the total number of times a collision was detected on a particular interface later than 512 bit-times into the transmission of a packet.   |
| Invalid long frames        | Displays the total number of frames received that exceeded the 1518 byte size limit and were dropped because they were not an integral number of octets in length and/or failed FCS checks.   |
| Alignment errors           | Displays the total number of frames received that are not an integral number of octets in length and do not pass the FCS check.   |

| Field                      | Description  |
|----------------------------|--|
| Transmit underruns         | Displays the total number of frames dropped due to transmission underruns. This is a normal, self-correcting condition, but large numbers of underruns may indicate a problem. |
| IP - bad checksum          | Displays the total number of IP packets received with a bad checksum.  |
| IP - small datagram        | Displays the total number of IP packets received without a full header (payload too small).  |
| IPX - bad header           | Displays the total number of IPX packets received with too small of a header length.   |
| Invalid MAC encap.         | Displays the total number of frames dropped due to a bad or unknown MAC encapsulation.   |
| Internal frame rx error    | Displays the total number of received frames dropped due to reasons not accounted for in other counts.   |
| Packet request overflow    | Displays the total number of packet request overflows.   |
| Out buffer (med) overflow  | Displays the total number of frames dropped because the medium priority Output Packet Manager was full.  |
| Out buffer (ctrl) overflow | Displays the total number of frames dropped due to the control priority Output Packet Manager being full.  |
| Error stats cleared        | Shows the date and time when the port-error stats were last cleared.   |

## statistics show port-packets

### Purpose

Display port packet statistics.

### Format

**statistics show port-packets** <port-list>|**all-ports**

### Mode

Enable.

### Parameters

---

|                               |  |
|-------------------------------|--|
| <port-list>  <b>all-ports</b> | Specifies the port. Specify <b>all-ports</b> to display port packet statistics for all physical and logical ports. |
|-------------------------------|--|

---

### Restrictions

None.

### Example

To display port packet statistics on port et.2.1:

```
xp# statistics show port-packets et.2.1

Port: et.2.1
----
RMON Stats          Received      Transmitted
-----
Unicast frames      0              0
Multicast frames    0              0
Broadcast frames    0              0
64 byte frames      0              0
65-127 byte frames  0              0
128-255 byte frames 0              0
256-511 byte frames 0              0
512-1023 byte frames 0              0
1024-1518 byte frames 0              0
RMON stats cleared  * Never Cleared *
```

# statistics show port-stats

## Purpose

Display normal (non-error) port statistics.

## Format

**statistics show port-stats** *<port/SmartTRUNK-list>***|all-ports**

## Mode

Enable.

## Parameters

---

|   |   |
|---|---|
| <i>&lt;port/SmartTRUNK-list&gt;</i> <b> all-ports</b> | Specifies a specific port or SmartTRUNK list. |
|---|---|

---

|                  |   |
|------------------|---|
| <b>all-ports</b> | Display port statistics for all physical and logical ports. |
|------------------|---|

---

**Note:** For additional information on gathering statistics on SmartTRUNKs, see [smarttrunk show](#) on page 1159.

## Restrictions

None.

## Example

The following example displays port statistics on port et.2.1:

|  |          |             |
|--|----------|-------------|
| xp# <b>statistics show port-stats et.2.1</b> |          |             |
| Port: et.2.1                                 |          |             |
| -----  |          |             |
| Port Stats                                   | Received | Transmitted |
| -----  |          |             |
| Frames/Packets                               | 0        | 0           |
| . Switched frames (bridging)                 | 0        | 0           |
| . Local frames (bridging)                    | 0        | N/A         |
| . Routed packets                             | 0        | 0           |
| . Switched (data)                            | 0        | N/A         |
| . Consumed by CPU                            | 0        | N/A         |
| Bytes  | 0        | 0           |
| . Bridged bytes                              | 0        | 0           |
| . Routed bytes                               | 0        | 0           |
| L2 table misses                              | 0        | N/A         |
| IP table misses                              | 0        | N/A         |
| IPv6 table misses                            | 0        | N/A         |
| IPX table misses                             | 0        | N/A         |
| IP TTL expirations                           | 0        | N/A         |
| IPv6 Hop Limit Exceededs                     | 0        | N/A         |
| IPX TC expirations                           | 0        | N/A         |
| 1 minute traffic rates                       |          |             |
| . Average bits/sec                           | 0        | 0           |
| . Packet discards                            | 0        | 0           |
| . Packet errors                              | 0        | 0           |
| . Unicast packets                            | 0        | 0           |
| . Multicast packets                          | 0        | 0           |
| . Broadcast packets                          | 0        | 0           |
| Port stats cleared * Never Cleared *         |          |             |

### Port Statistics Field Definitions

| Field           | Description   |
|-----------------|---|
| Frames/Packets  | Shows the total number of frames received/transmitted on this port.   |
| Switched frames | Shows the number of frames that have been bridged or forwarded.   |
| Local frames    | Shows the number of local frames (frames destined for a port that is the same as the port of entry) that was dropped. |
| Routed packets  | Shows the total number of frames routed on this port.   |



| Field                    | Description  |
|--------------------------|--|
| Switched (data)          | Shows the number of packets that was forwarded by the hardware.  |
| Consumed by CPU          | Shows the number of packets sent to the control module to be forwarded. Includes IPv6 packets.   |
| Bytes                    | Shows the total number of bytes received/transmitted on this port.   |
| Bridged bytes            | Shows the number of total bytes that has been bridged.   |
| Routed bytes             | Shows the number of total bytes that has been routed.  |
| L2 table misses          | Shows the number of times that a Layer-2 frame could not be resolved by the L2 Table.  |
| IP table misses          | Shows the number of times that an IPv4 packet could not be resolved by the IP Routing Table.   |
| IPv6 table misses        | Shows the number of IPv6 input datagrams discarded because no route could be found to transmit them to their destination.  |
| IPX table misses         | Shows the number of times that an IPX packet could not be resolved by the IPX Routing Table.   |
| IP TTL expirations       | Shows the number of IP packets that have been received by the port with a Time-to-Live (TTL) header with a value of 1. The IP packet will then be expired at this point. |
| IPv6 Hop Limit Exceededs | Shows the number of ICMP Time Exceeded messages sent by the interface  |
| IPX TC expirations       | Shows the number of IPX packets that have been received by the port with a TC header with a value of 1. The IPX packet will then be expired at this point.               |
| Average bits/sec         | Shows an average traffic rate in bits/second for a one-minute time period for a port.  |
| Packet discards          | Shows the number of packets discarded by a port within a one-minute time period.   |
| Packet errors            | Shows the number of packets containing errors that was seen by the port within a one-minute time period.   |
| Unicast packets          | Shows the number of unicast packets that was seen by the port within a one-minute time period.   |

| Field              | Description  |
|--------------------|--|
| Multicast packets  | Shows the number of multicast packets that was seen by the port within a one-minute time period. |
| Broadcast packets  | Shows the number of broadcast packets that was seen by the port within a one-minute time period. |
| Port stats Cleared | Shows the date and time when the port stats were last cleared.                                   |

# statistics show rarp

## Purpose

Display reverse ARP statistics.

## Format

**statistics show rarp** <string>| **all**

## Mode

Enable.

## Parameters

<string>|**all**

Specifies the interface name. Specify **all** to display reverse ARP statistics for all interfaces.

**Note:** Enterasys recommends that you use alphabetic characters when defining interface names—purely numeric interfaces will be interpreted as IP addresses. The X-Pedition router will display interface names up to 32 characters in length.

## Restrictions

None.

## Example

To display reverse ARP statistics on interface 'en0':

```
xp# statistics show rarp en0
```

```
Interface en0:
```

```
  0 requests received
  0 replies sent
  0 requests received on interface with rarpd disabled
  0 requests received that failed sanity check
  0 requests received that did not result in a match
  Last 5 Requests Received
  ----- no rarp requests received -----
  Last 5 Replies Sent
  ----- no rarp replies sent -----
```

## **statistics show summary-stats**

### **Purpose**

Display recent traffic summary statistics.

### **Format**

**statistics show summary-stats**

### **Mode**

Enable.

### **Parameters**

None.

### **Restrictions**

None.

# **statistics show tcp**

## **Purpose**

Display Transmission Control Protocol (TCP) statistics for all packets received or sent by the router software.

## **Format**

**statistics show tcp**

## **Mode**

Enable.

## **Parameters**

None.

## **Restrictions**

IP statistics on hardware-routed IP flows are not included in the statistics displayed by this command. To see statistics collected by router hardware, use the **statistics show ip-interface** and **statistics show port-packets** commands.

## Example

To display TCP statistics:

```
xp# statistics show tcp
tcp:
    235 packets sent
        232 data packets (22777 bytes)
        1 data packet (494 bytes) retransmitted
        0 resends initiated by MTU discovery
        2 ack-only packets (5 packets delayed)
        0 URG only packets
        0 window probe packets
        0 window update packets
        0 control packets
    320 packets received
        227 acks (for 22776 bytes)
        3 duplicate acks
        0 acks for unsent data
        158 packets (185 bytes) received in-sequence
        0 completely duplicate packets (0 bytes)
        0 old duplicate packets
        0 packets with some dup. data (0 bytes duped)
        0 out-of-order packets (0 bytes)
        0 packets (0 bytes) of data after window
        0 window probes
        0 window update packets
        0 packets received after close
        0 discarded for bad checksums
        0 discarded for bad header offset fields
        0 discarded because packets too short
    0 connection requests
    1 connection accept
    1 bad connection attempt
    0 listen queue overflows
    1 connection established (including accepts)
    0 connections closed (including 0 drops)
        0 connections updated cached RTT on close
        0 connections updated cached RTT variance on close
        0 connections updated cached ssthresh on close
    0 embryonic connections dropped
    226 segments updated rtt (of 228 attempts)
    0 retransmit timeouts
        0 connections dropped by rexmit timeout
    0 persist timeouts
        0 connections dropped by persist timeout
    0 keepalive timeouts
        0 keepalive probes sent
        0 connections dropped by keepalive
    0 correct ACK header predictions
    88 correct data packet header predictions
```

**Field Definitions**

| Field                                     | Description   |
|---|---|
| packets sent                              | Total number of TCP packets sent by the router.   |
| data packets (bytes)                      | Number of data packets (bytes) sent.  |
| data packet (bytes) retransmitted         | Number of data packets (bytes) retransmitted due to congestion.   |
| resends initiated by MTU discovery        | Number of packets resent due to MTU discovery.  |
| ack-only packets (5 packets delayed)      | Number of ACK-only packets sent (Number of delayed ACK packets sent)  |
| URG only packets                          | Number of URG-only packets sent. The URG (Urgent Pointer) bit indicates that urgent data can be found in the TCP header.              |
| window probe packets                      | Number of packets sent for probing TCP window size.   |
| window update packets                     | Number of packets sent for updating TCP window size.  |
| control packets                           | Number of control (SYN FIN RST) packets sent.   |
| packets received                          | Total number of TCP packets received by the router.   |
| acks (bytes)                              | Number of ACK packets (bytes) received.   |
| duplicate acks                            | Number of duplicate ACK packets received.   |
| acks for unsent data                      | Number of ACK packets received for unsent data.   |
| packets (bytes) received in-sequence      | Number of data packets (bytes) received in sequence.  |
| completely duplicate packets (bytes)      | Number of completely duplicate packets (bytes) received.  |
| old duplicate packets                     | Number of old duplicate packets dropped by PAWS ( <i>Protect Against Wrapped Sequence number</i> ) mechanism as described in RFC1323. |
| packets with some dup. data (bytes duped) | Number of packets (bytes) with partially duplicate data.  |
| out-of-order packets (bytes)              | Number of out-of-order packets (bytes) received.  |
| packets (bytes) of data after window      | Number of packets (bytes) received with data after window.  |

| Field  | Description   |
|--|---|
| window probes                                    | Number of packets received for probing TCP window size.                                     |
| window update packets                            | Number of packets received for updating TCP window size.                                    |
| packets received after close                     | Number of packets received after the TCP connection closed.                                 |
| discarded for bad checksums                      | Number of packets received that were dropped due to checksum errors.                        |
| discarded for bad header offset fields           | Number of packets received that were dropped because of bad header offsets.                 |
| discarded because packets too short              | Number of packets received that were dropped because they were too short.                   |
| connection requests                              | Number of TCP connection requested.   |
| connection accept                                | Number of TCP connection accepted.  |
| bad connection attempt                           | Number of bad connection attempts (e.g., those with premature acknowledgments).             |
| listen queue overflows                           | Number of connection requests dropped due to listen queue overflows.                        |
| connection established (including accepts)       | Number of TCP connections established.  |
| connections closed (including drops)             | Number of TCP connections closed (including number of connections dropped).                 |
| connections updated cached RTT on close          | Number of times the cached RTT (round-trip time) was updated.                               |
| connections updated cached RTT variance on close | Number of times the cached RTT variance was updated.  |
| connections updated cached ssthresh on close     | Number of times the cached ssthresh variable was updated.                                   |
| embryonic connections dropped                    | Number of embryonic connections dropped.  |
| segments updated rtt (of attempts)               | Number of successful RTT updates from segments (number of attempted updates from segments). |
| retransmit timeouts                              | Number of retransmission timeouts.  |
| connections dropped by rexmit timeout            | Number of connections dropped due to retransmission timeouts.                               |
| persist timeouts                                 | Number of persistence timeouts.   |



---

| Field                                  | Description   |
|--|---|
| connections dropped by persist timeout | Number of connections dropped due to persistence timeouts.                |
| keepalive timeouts                     | Number of keepalive timeouts.   |
| keepalive probes sent                  | Number of keepalive probes sent.  |
| connections dropped by keepalive       | Number of connections dropped due to keepalive timeout                    |
| correct ACK header predictions         | Number of correct header predictions made by the router for ACK packets.  |
| correct data packet header predictions | Number of correct header predictions made by the router for data packets. |

# statistics show udp

## Purpose

Display User Datagram Protocol (UDP) statistics for all packets received or sent by the router software.

## Format

**statistics show udp**

## Mode

Enable.

## Parameters

None.

## Restrictions

IP statistics on hardware-routed IP flows are not included in the statistics displayed by this command. To see statistics collected by router hardware, use the **statistics show ip-interface** and **statistics show port-packets** commands.

## Example

To display UDP statistics:

```
xp# statistics show udp
udp:
  0 datagrams received
  0 datagrams with incomplete header
  0 datagrams with bad data length field
  0 datagrams with bad checksum
  0 datagrams dropped due to no socket
  0 broadcast/multicast datagrams dropped due to no socket
  0 datagrams dropped due to full socket buffers
  0 datagrams not for hashed pcb
  0 delivered
  0 datagrams output
```

**Field Definitions**

| <b>Field</b>   | <b>Description</b>   |
|--|--|
| datagrams received                                     | Total number of UDP datagrams received.                                      |
| datagrams with incomplete header                       | Number of datagrams dropped due to incomplete header.                        |
| datagrams with bad data length field                   | Number of datagrams dropped due to bad data lengths.                         |
| datagrams with bad checksum                            | Number of datagrams dropped due to checksum errors.                          |
| datagrams dropped due to no socket                     | Number of datagrams dropped because there was no socket.                     |
| broadcast/multicast datagrams dropped due to no socket | Number of broadcast/multicast datagrams dropped because there was no socket. |
| datagrams dropped due to full socket buffers           | Number of datagrams dropped because of full socket buffers.                  |
| datagrams not for hashed pcb                           | Number of input datagrams received that are not for hashed pcb.              |
| delivered  | Total number of datagrams received that were not dropped.                    |
| datagrams output                                       | Total number of datagrams sent.  |

# statistics show vlan

## Purpose

Display the per-VLAN-packet statistics for IP-unicast traffic.

## Format

**statistics show vlan all**|<string>

## Mode

Enable.

## Description

The **statistics show vlan** command shows IP-unicast packet statistics for all VLANs in the router or for a specific VLAN.

## Parameters

|            |   |
|------------|---|
| <b>all</b> | Display statistics for all VLANs.       |
| <string>   | Display statistics for a specific VLAN. |

## Restrictions

L4-bridging and RMON Pro must be enabled on the VLAN and the VLAN ports in order to collect per-VLAN-statistics. “N/A” will appear if the VLAN does not satisfy these restrictions.

## Example

To display UDP statistics:

```
xp# statistics show vlan

  VID   VLAN Name   Total Packets   Total Bytes
  ---   -
  1     DEFAULT    N/A             N/A
  5     red        1007114         81576234
  6     blue        1004947         81400
```

# Chapter 73

## stp Commands

The **stp** commands let you display and change settings for the default Spanning Tree.

### Command Summary

[Table 61](#) lists the **stp** commands. The sections following the table describe the command syntax.

**Table 61. stp Commands**

|  |
|--|
| <b>stp enable port</b> <port-list>   |
| <b>stp set bridging</b> [forward-delay <num>] [hello-time <num>] [max-age <num>]<br>[priority <num>]                                   |
| <b>stp set port</b> <port-list> priority <num> port-cost <num> point-to-point [ForceTrue <br>ForceFalse  Auto] edge-port [True  False] |
| <b>stp show bridging-info</b>  |
| <b>stp reset-rstp port</b> <port-list>  all-ports  |
| <b>stp set protocol-version rstp</b>   |
| <b>stp filter-bpdu</b> <port-list>  all-ports  |

**Note:** The X-Pedition router supports STP over POS, but does *not* support PVST over POS.

## stp enable port

### Purpose

Enable STP on one or more ports.

### Format

**stp enable port** *<port-list>*

### Mode

Configure.

### Description

The **stp enable port** command enables STP on the specified ports.

### Parameters

---

|                          |  |
|--------------------------|--|
| <i>&lt;port-list&gt;</i> | The ports on which you are enabling STP. You can specify a single port or a comma-separated list of ports. Example: et.1.3,et.(1-3).(4,6-8). |
|--------------------------|--|

---

### Restrictions

None.

# stp set bridging

## Purpose

Set STP bridging parameters.

## Format

```
stp set bridging [forward-delay <num>] [hello-time <num>] [max-age <num>]  
[priority <num>]
```

## Mode

Configure.

## Description

The **stp set bridging** command lets you configure the following STP parameters:

- Bridging priority
- Hello time
- Maximum age
- Forward delay

## Parameters

|                               |  |
|-------------------------------|--|
| <b>forward-delay</b><br><num> | Sets the STP forward delay for the X-Pedition router. The forward delay is measured in seconds. Specify a number from 4–30. The default is 15. |
| <b>hello-time</b> <num>       | Sets the STP hello time for the X-Pedition router. The hello time is measured in seconds. Specify a number from 1–10. The default is 2.        |
| <b>max-age</b> <num>          | Sets the STP maximum age for the X-Pedition router. Specify a number from 6–40. The default is 20.   |
| <b>priority</b> <num>         | Sets the STP bridging priority for the X-Pedition router. Specify a number from 0–65535. The default is 32768.                                 |

## Restrictions

None.

## Example

To set the bridging priority of Spanning Tree for the entire X-Pedition router to 1:

```
xp(config)# stp set bridging priority 1
```



# stp set port

## Purpose

Set STP port priority and port cost for ports.

## Format

```
stp set port <port-list> priority <num> port-cost <num>
point-to-point [ForceTrue| ForceFalse| Auto] edge-port [True| False]
```

## Mode

Configure.

## Description

The **stp set port** command sets the STP priority and port cost for individual ports.

## Parameters

|   |   |
|---|---|
| <b>port</b> <port-list>                                     | The port(s) for which you are setting STP parameters. You can specify a single port or a comma-separated list of ports.<br>Example: et.1.3,et.(1-3).(4,6-8).  |
| <b>priority</b> <num>                                       | The priority you are assigning to the port(s). Specify a number from 0– 16 inclusive. The default is 8.   |
| <b>port-cost</b> <num>                                      | The STP cost you are assigning to the port(s). Specify a number from 1– 65535. The default depends on the port speed: 1 for Gigabit (100-Mbps) ports, 10 for 100-Mbps ports, and 100 for 10-Mbps ports. |
| <b>point-to-point</b><br>[ForceTrue  <br>ForceFalse   Auto] | Specify a point-to-point or a non-point-to-point link administratively.<br>The default setting is 'Auto.'   |
| <b>edge-port</b><br>[True False]                            | Specify whether the port(s) should be initialized as a edge port or a non-edge port. The default is 'False.'  |

## Restrictions

With the ER16, an X-Pedition router can support up to 480 ports—this exceeds the 256-port limit allowed by the 8-bit port number field specified in the IEEE 802.1D-1998 standard. To accommodate the increase in the number of supported ports, Enterasys extended the port field to a 12-bit value and decreased the port priority field to a 4-bit value. As a result, the X-Pedition router allows STP or PVST port configurations with a priority of 0 to 15 only. In spite of these changes, the X-Pedition router remains compatible with other switches.

# **stp show bridging-info**

## **Purpose**

Display STP bridging information.

## **Format**

**stp show bridging-info**

## **Mode**

Enable.

## **Description**

The **stp show bridging-info** command displays STP bridging information for the X-Pedition router.

## **Parameters**

None.

## **Restrictions**

None.

# stp reset-rstp

## Purpose

Reset RSTP.

## Format

**stp reset-rstp port** <port\_list> | **all ports**

## Mode

Enable.

## Description

The **stp reset-rstp** command resets the point-to-point and edge port parameters to the user-specified values and forces the specified ports to send RSTP BPDU's until a version 0 STP BPDU is received.

## Parameters

|                  |   |
|------------------|---|
| <port_list>      | Specifies the ports for which you want to reset RSTP.           |
| <b>all-ports</b> | The all-ports keyword resets RSTP for all the X-Pedition ports. |

## Restrictions

None.

## **stp set protocol-version rstp**

### **Purpose**

Enable rapid reconfiguration on default spanning tree.

### **Format**

**stp set protocol-version rstp**

### **Mode**

Configure.

### **Description**

The **stp set protocol-version** command changes the STP version from “STP compatible” (version 0) to “Rapid Configuration” (version 2).

### **Restrictions**

STP cannot be enabled on any non-LAN ports when running RSTP.

# stp filter-bpdu

## Purpose

Filter out BPDU on a port when STP is disabled.

## Format

**stp filter-bpdu** <port-list> |**all-ports**

## Mode

Configure.

## Description

The **stp filter-bpdu** command sets up a filter on the specified port for BPDU's when STP is disabled.

## Parameters

|                  |   |
|------------------|---|
| <port-list>      | List of ports to which you will apply the filter. |
| <b>all-ports</b> | All ports.  |

## Restrictions

Can be used only when STP is disabled.



# Chapter 74

## system Commands

The **system** commands let you display and change system parameters.

### Command Summary

[Table 62](#) lists the **system** commands. The sections following the table describe the command syntax.

**Table 62. system Commands**

|  |
|--|
| <b>system are-promimage upgrade module</b> <number> [ <b>tftp-server</b> <IPaddr-or-hostname> <b>filename</b> <filename>]   [ <b>tftp-url</b> <URL>]   |
| <b>system disable inputportlevel-rate-limiting slot</b> <numbers>  |
| <b>system enable aggregate-rate-limiting slot</b> <number>   |
| <b>system failover master-cm</b>   |
| <b>system hotswap out in slot</b> <number>   |
| <b>system image add</b> { <b>tftp-server</b> <IPaddr-or-hostname> <b>filename</b> <filename>/<br><b>tftp-url</b> <URL> } [ <b>destination</b> { <b>backup-cm</b>   <b>primary-cm</b>   <b>all</b> }] |
| <b>system image choose</b> <filename> [ <b>backup-cm</b>   <b>primary-cm</b>   <b>all</b> ]  |
| <b>system image delete</b> <filename> [ <b>backup-cm</b>   <b>primary-cm</b>   <b>all</b> ]  |
| <b>system image list</b> [ <b>primary-cm</b>   <b>backup-cm</b>   <b>all</b> ]   |
| <b>system ipv6-fpga upgrade</b>  |
| <b>system kill ssh-session</b> <session-id>  |
| <b>system kill telnet-session</b> <session-id>   |

Table 62. system Commands (Continued)

|   |
|---|
| <b>system l3-deep-buckets module &lt;num&gt; set on</b>   |
| <b>system promimage upgrade tftp-server &lt;IPaddr-or-hostname&gt; file-name &lt;filename&gt;</b><br>{destination primary-cm  backup-cm} <br><b>tftp-url &lt;URL&gt; {destination primary-cm   backup-cm} </b><br><b>file-name {tftp-server &lt;IPaddr-or-hostname&gt;  destination primary-cm  backup-cm} </b><br><b>destination primary-cm   backup-cm {tftp-server &lt;IPaddr-or-hostname&gt; filename</b><br><b>&lt;filename&gt;}  {filename &lt;filename&gt; tftp-server &lt;IPaddr-or-hostname&gt;}  {tftp-url &lt;URL&gt;}</b> |
| <b>system set backup-cm-timeout seconds &lt;seconds&gt;</b>   |
| <b>system set bootprom netaddr &lt;IPaddr&gt; netmask &lt;IPnetmask&gt; tftp-server &lt;IPaddr&gt;</b><br><b>[tftp-gateway &lt;IPaddr&gt;]</b>  |
| <b>system set console level &lt;level&gt; use-syslog-levels</b>   |
| <b>system set contact &lt;system-contact&gt;</b>  |
| <b>system set cpu-utilization-trap min-threshold &lt;value&gt; max-threshold &lt;value&gt;</b>  |
| <b>system set date year &lt;year&gt; month &lt;month&gt; day &lt;day&gt; hour &lt;hour&gt; min &lt;min&gt;</b><br><b>second &lt;sec&gt;</b>   |
| <b>system set dns server &lt;IPaddr&gt;[,&lt;IPaddr&gt;[,&lt;IPaddr&gt;]] domain &lt;name&gt;</b>   |
| <b>system set dst-changing [s-wk &lt;num&gt;] [s-dow &lt;num&gt;] [s-mo &lt;num&gt;] [s-hr &lt;num&gt;]</b><br><b>[s-min &lt;num&gt;] [e-wk &lt;num&gt;] [e-dow &lt;num&gt;] [e-mo &lt;num&gt;] [e-hr &lt;num&gt;]</b><br><b>[e-min &lt;num&gt;] dst-fixed [s-mo &lt;num&gt;] [s-day &lt;num&gt;] [s-hr &lt;num&gt;] [s-min &lt;num&gt;]</b><br><b>[e-mo &lt;num&gt;] [e-day &lt;num&gt;] [e-hr &lt;num&gt;] [e-min &lt;num&gt;] dst-manual</b>   |
| <b>system set dst-fixed [s-mo &lt;num&gt;] [s-day &lt;num&gt;] [s-hr &lt;num&gt;] [s-min &lt;num&gt;]</b><br><b>[e-mo &lt;num&gt;] [e-day &lt;num&gt;] [e-hr &lt;num&gt;] [e-min &lt;num&gt;] dst-manual</b>  |
| <b>system set dst-manual</b>  |
| <b>system set extended-debug [inhibit-master-reboot]   [enable-intr-monitor &lt;num&gt;]  </b><br><b>[enable-pkt-capture]</b>   |
| <b>system set idle-timeout serial  telnet  ssh &lt;timeout&gt;</b>  |
| <b>system set location &lt;location&gt;</b>   |
| <b>system set login-banner &lt;string&gt; none file-name &lt;string&gt;</b>   |
| <b>system set malloc</b>  |
| <b>system set name &lt;system-name&gt;</b>  |
| <b>system set password &lt;mode&gt; &lt;string&gt; none</b>   |
| <b>system set password-policy auth-grace-timeout &lt;grace&gt;  change-after-first-login {on off} </b><br><b>expire-warning &lt;warn&gt;  history-size &lt;size&gt;  lifetime &lt;time&gt;  login-failure-grace-time</b><br><b>&lt;fail-time&gt;  maximum-failed-logins &lt;fails&gt;  minimum-length &lt;minimum&gt;</b><br><b>verification {on   off}</b>   |



Table 62. system Commands (Continued)

|  |
|--|
| <b>system set poweron-selftest</b> [on  quick]   |
| <b>system set show-config</b> alphabetical   |
| <b>system set spooler-memory-limit</b> <memory-limit>  |
| <b>system set syslog</b> [server <hostname-or-IPaddr>] [local] [level <level-type>]<br>[facility <syslog-facility-type>] [source <source-IPaddr>] [buffer-size <size>]                       |
| <b>system set syslog-levels</b> <facility> level <level>   |
| <b>system set terminal baud</b> <baud-rate>  <b>columns</b> <number> <b>rows</b> <number>  |
| <b>system set tftpsource</b> <IP address>  |
| <b>system set timezone</b> <timezone> <minutes>  |
| <b>system set user</b> <username> <new-password> <b>password-option</b> [never-expires  normal]<br><b>privilege-level</b> [login  enable] <b>status</b> [always-enabled   disabled  enabled] |
| <b>system show</b> <system-parm>   |
| <b>system show capacity</b> all   chassis   task   cpu   memory  |
| <b>system show syslog</b> levels   |

# system are-promimage upgrade

## Purpose

Upgrade the boot prom on a specific ARE module.

## Format

**system are-promimage upgrade module** <number> [**tftp-server** <IPaddr-or-hostname>  
**filename** <filename>] | [**tftp-url** <URL>]

## Mode

Enable.

## Description

The **system set data-pkts-threshold** command allows you to upgrade the boot prom on a specific ARE module.

## Parameters

|                        |   |
|------------------------|---|
| <b>module</b> <number> | The module number of the ARE module to upgrade.   |
| <IPaddr-or-hostname>   | The IP address or host name of the TFTP server. The tftp-url is not allowed when using this parameter.            |
| <filename>             | The name of the software image file—required when using the tftp-server option.                                   |
| <URL>                  | The TFTP URL (e.g., tftp://10.1.2.3/images/img.tar.gz). The tftp-server is not allowed when using this parameter. |

## Restrictions

None.

## Example

To use the tftp-server parameter to download the boot prom image file “are.tar.gz” from the TFTP server 10.1.2.3 to a specific ARE module:

```
xp# system are-promimage upgrade module 3 tftp-server 10.1.2.3 filename are.tar.gz
```

To use the tftp-url parameter to download the boot prom image file “are.tar.gz” from the TFTP server 10.1.2.3 to a specific ARE module:

```
xp# system are-promimage upgrade module 3 tftp-url tftp://10.1.2.3/images/are.tar.gz
```

## system disable inputportlevel-rate-limiting slot

### Purpose

Disables Input Port Level Rate Limiting on a specific slot(s) and allows aggregate rate limiting policies to use the credit buckets reserved for port-level rate limiting policies.

### Format

**system disable inputportlevel-rate-limiting slot** *<numbers>*

### Mode

Configure.

### Description

The **system disable inputportlevel-rate-limiting** command disables Input Port Level Rate Limiting on a specific slot(s) and makes the credit buckets reserved for port-level rate limiting policies available for aggregate rate limiting policies.

### Parameters

---

|                                    |                                     |
|------------------------------------|-------------------------------------|
| <b>slot</b> <i>&lt;numbers&gt;</i> | The occupied slot or list of slots. |
|------------------------------------|-------------------------------------|

---

### Restrictions

None.

# system enable aggregate-rate-limiting

## Purpose

Enables Input Port Level and Aggregate Rate Limiting.

## Format

**system enable aggregate-rate-limiting slot <numbers>**

## Mode

Configure.

## Description

The **system enable aggregate-rate-limiting** command enables port level and aggregate rate limiting features on the router. There are two modes of operation for rate limiting available on the X-Pedition router: per-flow rate limiting and aggregate rate limiting. By default, the per-flow rate limiting mode is enabled.

By using this command, you are disabling per-flow rate limiting and enabling aggregate rate limiting and port level rate limiting.

To revert back to per-flow rate limiting, negate this command.

## Parameters

---

|                             |                                       |
|-----------------------------|---------------------------------------|
| <b>slot &lt;numbers&gt;</b> | The slot numbers you wish to disable. |
|-----------------------------|---------------------------------------|

---

## Restrictions

Aggregate and flow-aggregate rate limiting are not supported on 802.1q trunk ports.

## Example

To enable aggregate rate limiting:

```
xp# system enable aggregate-rate-limiting slot 1
```

# system failover master-cm

## Purpose

Force a failover from the master to backup Control Module.

## Format

**system failover master-cm**

## Mode

Enable.

## Description

The system failover master-cm command allows you to force a failover from the master CM to the backup CM. With the backup CM acting as the master CM, you can upgrade the boot firmware. Refer to the *Enterasys X-Pedition User Reference Manual* for details.

**Note:** In a dual Control Module configuration, the MAC address of the Primary Control Module in slot “CM/0” is used for both Control Modules after the system is booted. If the Control Module in slot “CM/0” is removed and not replaced after a fail-over, or if it is replaced with a new Control Module and the system is rebooted, the system will use the MAC address of the Control Module in slot 1 (i.e., the new Control Module).

## Parameters

None.

## Restrictions

None.

# system hotswap

## Purpose

Activates or deactivates a line card.

## Format

**system hotswap out|in slot** <number>

## Mode

Enable.

## Description

The **system hotswap out** command deactivates a line card in a specified slot on the X-Pedition router, causing it to go offline. The command performs the same function as if you had pressed the Hot Swap button on the line card.

The **system hotswap in** command causes a line card that was deactivated with the **system hotswap out** command to go online again. The command performs the same function as if you had removed the card from its slot and inserted it again.

See the *Enterasys X-Pedition User Reference Manual* for more information on hot swapping line cards.

## Parameters

|                      |  |
|----------------------|--|
| <b>out</b>           | Causes the line card in the specified slot to be deactivated.  |
| <b>in</b>            | Causes an inactive line card in the specified slot to be reactivated.  |
|                      | <b>Note:</b> The <b>system hotswap in</b> command works only on a line card that was deactivated with the <b>system hotswap out</b> command. |
| <b>slot</b> <number> | Is the slot where the line card resides. Specify any number between 1-16.  |

## Restrictions

None.

## Example

To deactivate the line card in slot 7 on the X-Pedition router:

```
xp# system hotswap out slot 7
```



# system image add

## Purpose

Copy a system software image to the X-Pedition router.

## Format

```
system image add { tftp-server <IPaddr-or-hostname> filename <filename>| tftp-url <URL> }
[destination { backup-cm| primary-cm| all }]
```

## Mode

Enable.

## Description

The **system image add** command copies a system software image from a TFTP server into the PCMCIA Flash Module on the Control Module. By default, if the X-Pedition router has two Control Modules, the system software image is copied to both Control Modules.

**Note:** The X-Pedition router supports PCMCIA Flash Modules obtained from Enterasys Networks only. For information regarding the PCMCIA Virtual File systems VFS1 and VFS2, see the *Enterasys X-Pedition User Reference Manual*.

## Parameters

|   |  |
|---|--|
| <IPaddr-or-hostname>  | The IP address or host name of the TFTP server. The tftp-url is not allowed when using this parameter.   |
| <filename>  | The name of the system software image file—required when using the tftp-server option.   |
| <URL>   | The TFTP URL (e.g., tftp://10.1.2.3/images/img.tar.gz). The tftp-server is not allowed when using this parameter.  |
| <b>destination</b><br>{ <b>backup-cm</b>   <b>primary-cm</b>   <b>all</b> } | <p><b>Note:</b> When a user selects the <b>primary-cm</b> or <b>backup-cm</b> option, the router will prompt the user about adding the image to <i>both</i> CMs.</p> <p><b>primary-cm</b> Copies the system software image to the <i>Primary</i> Control Module only.</p> <p><b>backup-cm</b> Copies the system software image to the <i>Backup</i> Control Module only.</p> <p><b>all</b> Select this option to add the image to all CMs.</p> |

## Restrictions

None.

## Example

In the following examples, the image file `img.tar.gz` is located in a folder in the root directory named `images` on the TFTP server `10.1.2.3`.

To use the `tftp-server` parameter to download the software image file “`img.tar.gz`” from the TFTP server `10.1.2.3` to the both control modules:

```
xp# system image add tftp-server 10.1.2.3 filename img.tar.gz destination primary-cm
xp# system image add tftp-server 10.1.2.3 filename img.tar.gz destination backup-cm
xp# system image add tftp-server 10.1.2.3 filename img.tar.gz
```

To use the `tftp-url` parameter to download the software image file “`images/img.tar.gz`” from the TFTP server `10.1.2.3` to both control modules:

```
xp# system image add tftp-url tftp://10.1.2.3/images/img.tar.gz destination primary-cm
xp# system image add tftp-url tftp://10.1.2.3/images/img.tar.gz destination backup-cm
xp# system image add tftp-url tftp://10.1.2.3/images/img.tar.gz
```

# system image choose

## Purpose

Select a system software image file.

## Format

**system image choose** <filename> [**backup-cm**| **primary-cm**| **all**]

## Mode

Enable.

## Description

The **system image choose** command specifies the system software image file on the PCMCIA Flash Module that you want the X-Pedition router to use the next time the system reboots.

**Note:** The X-Pedition router supports PCMCIA Flash Modules obtained from Enterasys Networks only. For information regarding the PCMCIA Virtual File systems VFS1 and VFS2, see the *Enterasys X-Pedition User Reference Manual*.

## Parameters

|                   |  |
|-------------------|--|
| <filename>        | The name of the system software image file.  |
| <b>primary-cm</b> | This parameter specifies that the image file is chosen for the primary control module.             |
| <b>backup-cm</b>  | This parameter specifies that the image file is chosen for the backup control module.              |
| <b>all</b>        | Select this option to use the image file specified as the next boot image on both Control Modules. |

## Restrictions

None.

# system image delete

## Purpose

Deletes a system software image file from the PCMCIA Flash Module.

## Format

**system image delete** <filename> [**backup-cm**| **primary-cm**| **all**]

## Mode

Enable.

## Description

The **system image delete** command deletes a system software image file from the PCMCIA Flash Module on the Control Module.

**Note:** The X-Pedition router supports PCMCIA Flash Modules obtained from Enterasys Networks only. For information regarding the PCMCIA Virtual File systems VFS1 and VFS2, see the *Enterasys X-Pedition User Reference Manual*.

## Parameters

|                   |  |
|-------------------|--|
| <filename>        | The name of the system software image file you want to delete.   |
| <b>primary-cm</b> | This parameter deletes the image file from the <i>Primary</i> Control Module only.   |
| <b>backup-cm</b>  | This parameter deletes the image file from the <i>Backup</i> Control Module only.  |
| <b>all</b>        | Select this option to delete the image file from both Control Modules. The router will prompt users before removing the image. |

## Restrictions

None.

# system image list

## Purpose

Lists the system software image files on the PCMCIA Flash Module.

## Format

**system image list** [**primary-cm**| **backup-cm**| **all**]

## Mode

Enable.

## Description

The **system image list** command lists the system software image files contained on the PCMCIA Flash Module on the Control Module.

**Note:** The X-Pedition router supports PCMCIA Flash Modules obtained from Enterasys Networks only. For information regarding the PCMCIA Virtual File systems VFS1 and VFS2, see the *Enterasys X-Pedition User Reference Manual*.

## Parameters

|                   |   |
|-------------------|---|
| <b>primary-cm</b> | This parameter lists the image files on the <i>Primary</i> Control Module.  |
| <b>backup-cm</b>  | This parameter lists the image files on the <i>Backup</i> Control Module.   |
| <b>all</b>        | Select this option to display all the images on both Control Modules. If you do not specify any of these options, this command defaults to <b>all</b> . |

## Restrictions

None.

# system ipv6-fpga upgrade

## Purpose

Upgrade the FPGA on a specific IPV6 module.

## Format

**system ipv6-fpga upgrade module** <number> [**tftp-server** <IPaddr-or-hostname>  
**filename** <filename>] | [**tftp-url** <URL>]

## Mode

Enable.

## Description

The system ipv6-fpga upgrade command allows you to upgrade the FPGA on a specific IPV6 module.

## Parameters

|                        |   |
|------------------------|---|
| <b>module</b> <number> | The module number of the IPV6 module to upgrade.  |
| <IPaddr-or-hostname>   | The IP address or host name of the TFTP server. The tftp-url is not allowed when using this parameter.                |
| <filename>             | The name of the software image file—required when using the tftp-server option.                                       |
| <URL>                  | The TFTP URL (e.g., tftp://10.1.2.3/images/fpga_ver2.xsvf). The tftp-server is not allowed when using this parameter. |

## Restrictions

None.

## Example

To use the tftp-server parameter to download the FPGA image file “fpga\_ver2.xsvf” from the TFTP server 10.1.2.3 to a specific IPV6 module, enter the following:

```
xp# system ipv6-fpga upgrade module 3 tftp-server 10.1.2.3 filename fpga_ver2.xsvf
```

To use the tftp-url parameter to download the boot prom image file “fpga\_ver2.xsvf” from the TFTP server 10.1.2.3 to a specific IPV6 module, enter the following:

```
xp# system ipv6-fpga upgrade module 3 tftp-url tftp://10.1.2.3/images/fpga_ver2.xsvf
```

# system kill ssh-session

## Purpose

Terminates an active Secure Shell session.

## Format

**system kill ssh-session** <session-id>

## Mode

Enable.

## Description

Terminates the active SSH session specified. Use the **system show users** command to get the ID of the session you want to terminate.

## Parameters

---

|              |   |
|--------------|---|
| <session-id> | The ID (0-3) of the session to terminate. |
|--------------|---|

---

## Restrictions

None.

## Example

To terminate SSH session 2, enter the following:

|                                  |
|----------------------------------|
| <b>system kill ssh-session 2</b> |
|----------------------------------|



# system kill telnet-session

## Purpose

Kills a specified Telnet session.

## Format

**system kill telnet-session** <session-id>

## Mode

Enable.

## Description

The **system kill telnet-session** command kills the Telnet session specified by the session ID. Use the **system show users** command to display the list of current Telnet users and session IDs.

## Parameters

|              |  |
|--------------|--|
| <session-id> | The Telnet connection slot number, which can be 0, 1, 2, or 3. The <b>system show users</b> command displays the session ID number in the first column. You can only specify one session ID per <b>system kill telnet-session</b> command. |
|--------------|--|

## Restrictions

None.

## Example

To show the active Telnet sessions.

```
xp# system show users
Current Terminal User List:
# Login ID      Mode           From           LoginTimestamp
-----
0               enabled        console        Thu Feb 22 13:07:412001
2               enabled        10.9.0.1       Thu Feb 22 13:07:592001
3               login-prompt   10.9.0.1
3               login-prompt   10.9.0.1
```

Then, to kill Telnet session 2:

```
xp# system kill telnet-session 2  
Telnet session 2 (from 10.9.0.1) killed
```

# system l3-deep-buckets

## Purpose

Enables deep hashing on a specified module.

## Format

**system l3-deep-buckets module <num> set on**

## Mode

Configure.

## Description

Use the **system l3-deep-buckets** command to enable deep hashing on a specified module.

Deep hashing allows for more than four hash buckets (levels within a particular entry for a hash value) within an entry in the L3 lookup table. Although hashing should provide an even distribution across the lookup table, there is still a possibility that more than four flows may end up at a particular entry in the lookup table.

Allowing for more than four entries through deep hashing will prevent thrashing, but may cause less-than-wirespeed performance due to the extra amount of entries. This is because thrashing will reduce performance to a greater extent than deep hashing. But although deep hashing may result in less-than-wirespeed performance, it still performs much better than if it were thrashing.

## Parameters

|                               |  |
|-------------------------------|--|
| <b>module &lt;num&gt; all</b> | Is a slot number on the X-Pedition router. Specify any number between 1 and 16. The hashing algorithm change affects all ports on the line card in the slot. Specify <b>all</b> to enable deep hashing on all slots. |
| <b>on</b>                     | Enables deep hashing on the module. Negate this command from active configuration to disable l3 deep hashing   |

## Restrictions

None.

## Example

To enable deep hashing on slot 7:

```
xp(config)# system l3-deep-buckets module 7 set on
```

# system promimage upgrade

## Purpose

Upgrades the boot PROM software on primary and secondary Control Modules.

## Format

```
system promimage upgrade tftp-server <IPaddr-or-hostname> file-name <filename>
{ destination primary-cm | backup-cm } | tftp-url <URL> { destination primary-cm |
backup-cm } | file-name { tftp-server <IPaddr-or-hostname> | destination primary-cm |
backup-cm } | destination primary-cm | backup-cm { tftp-server <IPaddr-or-hostname>
filename <filename> } | { filename <filename> tftp-server <IPaddr-or-hostname> } |
{ tftp-url <URL> }
```

## Mode

Enable.

## Description

The **system promimage upgrade** command copies and installs a boot PROM software image from a TFTP server onto the internal memory on the Primary and Backup Control Module. By default the system copies the bootprom image to both the primary and secondary control modules. The boot PROM software image is loaded when you power on the X-Pedition router and in turn loads the system software image file.

## Parameters

|                                   |   |
|-----------------------------------|---|
| <i>&lt;IPaddr-or-hostname&gt;</i> | The IP address or host name of the TFTP server. The tftp-url is not allowed when using this parameter.                              |
| <i>&lt;filename&gt;</i>           | The name of the boot PROM software image file—required when using the tftp-server option.   |
| <i>&lt;URL&gt;</i>                | The TFTP URL (e.g., tftp://10.1.2.3/images/img.tar.gz). The tftp-server is not allowed when using this parameter.                   |
| <b>primary-cm</b>                 | Copies the system software image only to the primary Control Module.  |
| <b>backup-cm</b>                  | Copies the system software image only to the backup Control Module.   |
| <b>Note:</b>                      | If you do not specify a control module, the X-Pedition router will load the Boot Firmware onto both Control Modules simultaneously. |

## Restrictions

None.

## Example

In the following examples, the boot-prom image named prom-image is located in a folder in the root directory named images on the TFTP server 10.50.89.88.

To load a new boot PROM image onto the Backup Control Module only, enter the following command from Enable mode:

**Note:** If you do not specify a control module, the XP will load the Boot Firmware onto both control modules simultaneously. To load a new boot PROM image onto both Control Modules using the tftp-url option, enter the following:

```
xp# system promimage upgrade tftp-url tftp://10.50.89.88/qa/prom-upgrade destination primary-cm
```

```
Downloading image 'qa/prom-upgrade' from host '10.50.89.88'
tftp complete
checksum valid. Ready to program.
flash found at 0xbfc00000
erasing...
programming...
verifying...
programming successful.
Programming complete.
system promimage upgrade tftp://10.50.89.88/qa/prom-upgrade destination backup- cm
system promimage upgrade tftp://10.50.89.88/qa/prom-upgrade
```

To load a new boot PROM image onto both Control Modules using the tftp-server option, enter the following:

```
xp# system promimage upgrade tftp-server 10.50.89.88 filename prom-upgrade destination
primary-cm
```

```
Downloading image 'prom-upgrade' from host '10.50.89.88'
tftp complete
checksum valid. Ready to program.
flash found at 0xbfc00000
erasing...
programming...
verifying...
programming successful.
Programming complete.
system promimage upgrade tftp-server 10.50.89.88 filename prom-upgrade
destination backup-cm
system promimage upgrade tftp-server 10.50.89.88 filename prom-upgrade
```

To upgrade the PROM image from a URL:

```
xp# system promimage upgrade 10.136.2.9 /qa/prom-upgrade
xp# system promimage upgrade 10.136.2.9 /qa/prom-upgrade primary-cm
xp# system promimage upgrade 10.136.2.9 /qa/prom-upgrade backup-cm
```

```
xp# system promimage upgrade 10.136.2.9 bp3200
```

```
Downloading image 'bp3200' from host '10.136.2.9'
image is a prom upgrade to version 'prom-E3.2.0.0'
%SYS-I-PRIMARY_CM_MSG, TFTP Complete.
%SYS-I-PRIMARY_CM_MSG, Checksum valid. Ready to program.
%HBT-E-NOBACKUPCP, There is no backup module present
%SYS-W-PRIMARY_CM, Warning from Primary CM: Failed to upgrade PROM on backup CM.
%SYS-I-PRIMARY_CM_MSG, Flash Found.
%SYS-I-PRIMARY_CM_MSG, Erasing.
%SYS-I-PRIMARY_CM_MSG, Programming.
%SYS-I-PRIMARY_CM_MSG, Verifying.
%SYS-I-PRIMARY_CM_MSG, Programming Successful.
%SYS-I-PRIMARY_CM_MSG, Programming Complete.
```

# system set backup-cm-timeout

## Purpose

Set backup-CM timeout value.

## Format

**system set backup-cm-timeout seconds** <seconds>

## Mode

Configure.

## Description

The **system set backup-cm-timeout** command sets the amount of time the backup Control Module will use to determine failure of the primary Control Module. If the secondary Control Module does not receive a heartbeat from the primary Control Module for a time equal to or greater than the time-out value, the secondary Control Module takes over as the primary Control Module. Typically, the primary Control Module sends heartbeats to the secondary Control Module at specific intervals. If the primary Control Module becomes too busy to send heartbeats to the secondary Control Module, you can change this interval and extend the timeout.

## Parameters

|           |   |
|-----------|---|
| <seconds> | The number of seconds (4-1000) the backup Control Module waits without receiving a heartbeat from the primary Control Module before taking over as the primary control module. By default, this value is 4 seconds. |
|-----------|---|

## Restrictions

None.



# system set bootprom

## Purpose

Sets parameters for the boot PROM.

## Format

```
system set bootprom netaddr <IPaddr> netmask <IPnetmask> tftp-server <IPaddr>  
[tftp-gateway <Ipaddr>]
```

## Mode

Configure.

## Description

The **system set bootprom** command sets parameters to aid in booting the X-Pedition system software image remotely over the network. You can use this command to set the X-Pedition router's IP address, subnet mask, TFTP boot server address, and gateway address.

**Note:** These parameters apply only to the Control Module's en0 Ethernet interface (labeled "10/100 Mgmt"). This port is a management port only, and is not intended to perform routing.

## Parameters

|                              |   |
|------------------------------|---|
| <b>netaddr</b> <IPaddr>      | The IP address the X-Pedition router uses during the boot exchange with the TFTP boot server. |
| <b>netmask</b> <IPnetmask>   | The subnet mask the X-Pedition router uses during the boot exchange.                          |
| <b>tftp-server</b> <IPaddr>  | The TFTP boot server's IP address.  |
| <b>tftp-gateway</b> <Ipaddr> | The gateway that connects the X-Pedition router to the TFTP boot server.                      |

## Restrictions

None.

## Example

The command in the following example configures the X-Pedition router to use IP address 10.50.88.2 to boot over the network from TFTP boot server 10.50.89.88.

```
xp(config)# system set bootprom netaddr 10.50.88.2 netmask 255.255.0.0 tftp-server 10.50.89.88
```

# system set console level

## Purpose

This command allows users to select the minimum error message severity level to display to the console.

## Format

**system set console level** <level> **use-syslog-levels**

## Mode

Configure.

## Parameters

|                          |  |
|--------------------------|--|
| <level>                  | The minimum console message level.   |
| <b>fatal</b>             | Display fatal messages only.   |
| <b>error</b>             | Display fatal and error messages only.   |
| <b>warning</b>           | Display fatal, error, and warning messages only.   |
| <b>audit</b>             | Display fatal, error, audit, and warning messages only.  |
| <b>info</b>              | Display all messages.  |
| <b>use-syslog-levels</b> | Select this option to apply the level as the default console message severity level and override the level defined by the <b>system set syslog-levels</b> command. |

## Restrictions

None.

# system set contact

## Purpose

Set the contact name and information for this X-Pedition router.

## Format

**system set contact** <system-contact>

## Mode

Configure.

## Description

The **system set contact** command sets the name and contact information for the network administrator responsible for this X-Pedition router.

## Parameters

---

|                  |   |
|------------------|---|
| <system-contact> | A string listing the name and contact information for the network administrator responsible for this X-Pedition router. If the string contains blanks or commas, you must use the quotation marks around the string. (Example: “ <b>Jane Doe, janed@corp.com, 408-555-5555 ext. 555</b> ”.) |
|------------------|---|

---

## Restrictions

None.

# system set cpu-utilization-trap

## Purpose

Configure the threshold parameters for sending a CPU threshold exceeded trap.

## Format

**system set cpu-utilization-trap min-threshold** <value> **max-threshold** <value>

## Mode

Configure.

## Description

The **system set cpu-utilization** command allows you to configure the threshold values used to control the sending of the CPU threshold exceeded trap. The max-threshold value controls the utilization percentage at which a trap is sent. The min-threshold value controls the utilization percentage where the trap sending logic will be armed. When the CPU utilization exceeds the max-threshold value, one trap is sent—no more traps are sent until the CPU utilization falls below the min-threshold value and exceeds the max-threshold value again. If either value is zero, no trap is generated.

## Parameters

|                      |  |
|----------------------|--|
| <b>min-threshold</b> | The percentage value (0-99) to reach before <i>arming</i> the trap.                  |
| <b>max-threshold</b> | The utilization percentage value (0-99) to exceed before <i>generating</i> the trap. |

## Restrictions

None.

# system set date

## Purpose

Set the system time and date.

## Format

```
system set date year <year> month <month> day <day> hour <hour> min <min>  
second <sec>
```

## Mode

Enable.

## Description

The **system set date** command sets the system time and date for the X-Pedition router. The X-Pedition router keeps the time in a battery-backed realtime clock. To display the time and date, enter the **system show date** command.

## Parameters

|                              |   |
|------------------------------|---|
| <b>year</b> <number>         | Four-digit number for the year. (Example: <b>2001</b> )                           |
| <b>month</b><br><month-name> | Name of the month. You must spell out the month name.<br>(Example: <b>March</b> ) |
| <b>day</b> <day>             | Number from 1 – 31 for the day.   |
| <b>hour</b> <hour>           | Number from 0 – 23 for the hour. (The number <b>0</b> means midnight.)            |
| <b>minute</b> <minute>       | Number from 0 – 59 for the hour.  |
| <b>second</b> <second>       | Number from 0 – 59 for the second.  |

## Restrictions

None.

# system set dns

## Purpose

Configure the X-Pedition router to reach up to three DNS servers.

## Format

**system set dns server** [**[**“<IPaddr> [<IPaddr>] [<IPaddr>][**]**” **domain** <name>

## Mode

Configure.

## Description

The **system set dns** command configures the X-Pedition router to reach up to three DNS servers. You also can specify the domain name to use for each DNS query.

## Parameters

|  |   |
|--|---|
| [“<IPaddr><br><IPaddr><br><IPaddr>][“] | IP address of the DNS server. Specify the address in dotted-decimal notation. You can specify up to three DNS servers separated by single spaces in the command line.<br><br><b>Note:</b> If you specify more than one IP address, you must surround the IP address specification with a set of quotes. |
| <domain-name>                          | Domain name for which the server is an authority.   |

## Restrictions

None.

## Example

To configure one DNS server and configure the X-Pedition DNS domain name to “mrb.com”:

```
xp(config)# system set dns server 10.1.2.3 domain mrb.com
```

To configure three DNS servers and configure the X-Pedition DNS domain name to “mrb.com”:

```
xp(config)# system set dns server “10.1.2.3 10.2.10.12 10.3.4.5” domain mrb.com
```

# system set dst-changing

## Purpose

Sets Daylight Saving Time according to specific days.

## Format

```
system set dst-changing [s-wk <num>] [s-dow <num>] [s-mo <num>] [s-hr <num>]  
[s-min <num>] [e-wk <num>] [e-dow <num>] [e-mo <num>] [e-hr <num>] [e-min <num>]
```

## Mode

Configure.

## Description

If Daylight Saving Time is in effect in your local time zone, use one of the **system set dst-** commands to enable it on the X-Pedition router (see [system set dst-fixed on page 1370](#) and [system set dst-manual on page 1372](#)). When you enable automatic DST settings, the settings do not affect the system until the time change arrives. When Daylight Saving Time starts (s-mo, s-hr, etc.), the system time will automatically advance one hour. At the end of Daylight Saving Time (e-mo, e-hr, etc.), the system clock will subtract one hour is. To disable Daylight Saving Time settings on the X-Pedition router, negate this command. (The UCT offset stays the same during all of this.)

## Parameters

|                    |   |
|--------------------|---|
| <b>s-wk</b> <num>  | This optional parameter specifies the starting week of the month. Specify a number between 1 and 5. The following is a description of the values: 1-first week, 2-second week, 3-third week, 4-fourth week, 5-last week. The default value is 1.  |
| <b>s-dow</b> <num> | This optional parameter specifies the starting day of the week. Specify a number between 1 and 7. The following is a description of the values: 1-Sunday, 2-Monday, 3-Tuesday, 4-Wednesday, 5-Thursday, 6-Friday, 7-Saturday. The default value is 1.   |
| <b>s-mo</b> <num>  | This optional parameter specifies the starting month of the year. Specify a number between 1 and 12. The following is a description of the values: 1-January, 2-February, 3-March, 4-April, 5-May, 6-June, 7-July, 8-August, 9-September, 10-October, 11-November, 12-December. The default value is 1. |



|                    |   |
|--------------------|---|
| <b>s-hr</b> <num>  | This optional parameter specifies the starting hour of the day. Specify a number between 0 and 23. This is based upon a 24-hour day, where 0-beginning of the first hour and 23-beginning of the last hour for that day. The default value is 0.  |
| <b>s-min</b> <num> | This optional parameter specifies the starting minute of the hour. Specify a number between 0 and 59. This is based upon a 60-minute hour, where 0-beginning of the first minute and 59-beginning of the last minute for that hour. The default value is 0.   |
| <b>e-wk</b> <num>  | This optional parameter specifies the ending week of the month. Specify a number between 1 and 5. The following is a description of the values: 1-first week, 2-second week, 3-third week, 4-fourth week, 5-last week. The default value is 1.  |
| <b>e-dow</b> <num> | This optional parameter specifies the ending day of the week. Specify a number between 1 and 7. The following is a description of the values: 1-Sunday, 2-Monday, 3-Tuesday, 4-Wednesday, 5-Thursday, 6-Friday, 7-Saturday. The default value is 1.   |
| <b>e-mo</b> <num>  | This optional parameter specifies the ending month of the year. Specify a number between 1 and 12. The following is a description of the values: 1-January, 2-February, 3-March, 4-April, 5-May, 6-June, 7-July, 8-August, 9-September, 10-October, 11-November, 12-December. The default value is 1. |
| <b>e-hr</b> <num>  | This optional parameter specifies the ending hour of the day. Specify a number between 0 and 23. This is based upon a 24-hour day, where 0-beginning of the first hour and 23-beginning of the last hour for that day. The default value is 0.  |
| <b>e-min</b> <num> | This optional parameter specifies the ending minute of the hour. Specify a number between 0 and 59. This is based upon a 60-minute hour, where 0-beginning of the first minute and 59-beginning of the last minute for that hour. The default value is 0.   |

## Restrictions

None.

## Example

To set Daylight Saving Time to start at midnight on the last Sunday of March and end at 2:00 A.M. on the first Saturday of October every year:

```
xp(config)# system set dst-changing s-wk 5 s-dow 1 s-mo 3 e-wk 1 e-dow 7 e-mo 10 e-hr 2
```

# system set dst-fixed

## Purpose

Sets Daylight Saving Time automatically according to specific dates.

## Format

```
system set dst-fixed [s-mo <num>] [s-day <num>] [s-hr <num>] [s-min <num>] [e-mo <num>]  
[e-day <num>] [e-hr <num>] [e-min <num>]
```

## Mode

Configure.

## Description

If Daylight Saving Time is in effect in your local time zone, use one of the **system set dst-** commands to enable it on the X-Pedition router (see [system set dst-changing on page 1368](#) and [system set dst-manual on page 1372](#)). When you enable automatic DST settings, the settings do not affect the system until the time change arrives. When Daylight Saving Time starts (s-mo, s-hr, etc.), the system time will automatically advance one hour. At the end of Daylight Saving Time (e-mo, e-hr, etc.), the system clock will subtract one hour. To disable Daylight Saving Time settings on the X-Pedition router, negate this command. (The UCT offset stays the same during all of this.)

## Parameters

|                    |   |
|--------------------|---|
| <b>s-mo</b> <num>  | This optional parameter specifies the starting month of the year. Specify a number between 1 and 12. The following is a description of the values: 1-January, 2-February, 3-March, 4-April, 5-May, 6-June, 7-July, 8-August, 9-September, 10-October, 11-November, 12-December. The default value is 1. |
| <b>s-day</b> <num> | This optional parameter specifies the starting day of the month. Specify a number between 1 and 31. This is based upon a 31-day month, where 1-first day and 31-thirty first day for that month. The default value is 1.  |
| <b>s-hr</b> <num>  | This optional parameter specifies the starting hour of the day. Specify a number between 0 and 23. This is based upon a 24-hour day, where 0-beginning of the first hour and 23-beginning of the last hour for that day. The default value is 0.  |
| <b>s-min</b> <num> | This optional parameter specifies the starting minute of the hour. Specify a number between 0 and 59. This is based upon a 60-minute hour, where 0-beginning of the first minute and 59-beginning of the last minute for that hour. The default value is 0.   |

|                    |   |
|--------------------|---|
| <b>e-mo</b> <num>  | This optional parameter specifies the ending month of the year. Specify a number between 1 and 12. The following is a description of the values: 1-January, 2-February, 3-March, 4-April, 5-May, 6-June, 7-July, 8-August, 9-September, 10-October, 11-November, 12-December. The default value is 1. |
| <b>e-day</b> <num> | This optional parameter specifies the ending day of the month. Specify a number between 1 and 31. This is based upon a 31-day month, where 1-first day and 31-thirty first day for that month. The default value is 1.  |
| <b>e-hr</b> <num>  | This optional parameter specifies the ending hour of the day. Specify a number between 0 and 23. This is based upon a 24-hour day, where 0-beginning of the first hour and 23-beginning of the last hour for that day. The default value is 0.  |
| <b>e-min</b> <num> | This optional parameter specifies the ending minute of the hour. Specify a number between 0 and 59. This is based upon a 60-minute hour, where 0-beginning of the first minute and 59-beginning of the last minute for that hour. The default value is 0.   |

## Restrictions

None.

## Example

To set Daylight Saving Time to start at 3:00 a.m. on April 1st and end at midnight on the 15th of September every year:

```
xp(config)# system set dst-fixed s-mo 4 s-day 1 s-hr 3 e-mo 9 e-day 15
```

# system set dst-manual

## Purpose

Allows you to set the system time forward by one hour after you save the command into active configuration. Negating this command will set the system time back one hour.

## Format

**system set dst-manual**

## Mode

Configure.

## Description

If Daylight Saving Time is in effect in your local time zone, use one of the **system set dst-**commands to enable it on the X-Pedition router (see [system set dst-changing on page 1368](#), and [system set dst-fixed on page 1370](#)). When you enable automatic DST settings, the settings do not affect the system until the time change arrives. When Daylight Saving Time starts (s-mo, s-hr, etc.), the system time will automatically advance one hour. At the end of Daylight Saving Time (e-mo, e-hr,etc.), the system clock will subtract one hour is. To disable Daylight Saving Time settings on the X-Pedition router, negate this command. (The UCT offset stays the same during all of this.)

## Parameters

None.

## Restrictions

None.

# system set extended-debug

## Purpose

Sets various runtime debug extensions.

## Format

```
system set extended-debug [inhibit-master-reboot] | [enable-intr-monitor <num>] |  
[enable-pkt-capture]
```

## Mode

Configure (diagnostic mode).

## Description

The **system set extended-debug** command is a system tuning command used only under the direction of Enterasys support personnel.

## Parameters

|                                     |   |
|-------------------------------------|---|
| <b>inhibit-master-reboot</b>        | This optional parameter prevents the former Master CPU from rebooting during a redundant CPU failover.  |
| <b>enable-intr-monitor</b><br><num> | This optional parameter allows you to set the amount of time for which to disable interrupts. If system interrupts exceed this value, the router will display an error. By default, this duration is 1000 milliseconds. This duration also includes the amount of time that splnet is on. |
| <b>enable-pkt-capture</b>           | Enabling this optional parameter will capture and save the last 10 packets.   |

## Restrictions

None.

# system set idle-timeout

## Purpose

Set the console idle timeout value.

## Format

**system set idle-timeout serial| telnet| ssh** *<timeout>*

## Mode

Configure.

## Description

Use the **system set idle-timeout** command to define the amount of time (in minutes) to remain idle before the control module terminates the communication session.

## Parameters

|                        |   |
|------------------------|---|
| <b>serial</b>          | Use this parameter to set the timeout value for a <i>serial</i> console connection.   |
| <b>telnet</b>          | Use this parameter to set the timeout value for a <i>telnet</i> console connection.   |
| <b>ssh</b>             | Use this parameter to set the timeout value for a <i>secure shell</i> console connection.   |
| <i>&lt;timeout&gt;</i> | The amount of time to remain idle (0-60 minutes) before disconnecting a communication session. By default, this value is 5 minutes. To disable the timeout, enter a value of 0. |

## Restrictions

None.

## Example

To set a secure shell timeout of 30 minutes, enter the following from configuration mode:

```
xp(config)# system set idle-timeout ssh 30
```

# system set location

## Purpose

Set the system location.

## Format

**system set location** <location>

## Mode

Configure.

## Description

The **system set location** command adds a string describing the location of the X-Pedition router. The system name and location can be accessed by SNMP managers.

## Parameters

---

|            |  |
|------------|--|
| <location> | A string describing the location of the X-Pedition router. If the string contains blanks or commas, you must use quotation marks around the string. (Example: <b>"Bldg C, network control room"</b> .) |
|------------|--|

---

## Restrictions

None.

# system set login-banner

## Purpose

Set the system login banner.

## Format

**system set login-banner** <string>/none|file-name name <string>

## Mode

Configure.

## Description

The **system set login-banner** command configures the initial login banner that one sees when logging into the X-Pedition router. The banner may span multiple lines by adding line-feed characters in the string, “\n”.

## Parameters

|                                   |  |
|-----------------------------------|--|
| <string>                          | Is the text of the login banner for the X-Pedition router. Banners that include more than one word must be inclosed in quotation marks (i.e., “This is a multi-word banner”). When you include the new line (“\n”) command in the banner, the banner may span multiple lines. You may also use the tab (“\t”) command to include tabs in the banner. It is not common to use both the new line and tab commands in a banner. |
| <b>none</b>                       | Specifies that no login-banner be used on the X-Pedition router.   |
| <b>file-name name</b><br><string> | Specifies the name of the file containing the login banner.  |

## Restrictions

None.

## Example

The following example configures a multi-line login banner:

```
xp(config)# system set login-banner “Core Router #1\nUnauthorized Access Prohibited”
```



The next person to log into the X-Pedition router would see the following:

```
Core Router #1
Unauthorized Access Prohibited

Press RETURN to activate console...
```

To use a login banner from a file, enter the following:

```
xp(config)# system set login-banner file-name name the_banner_file
```

If you do not want any login-banner at all, enter the following:

```
xp(config)# system set login-banner none
```

# **system set malloc**

## **Purpose**

Sets the caller trace for the system malloc functionality.

## **Format**

**system set malloc debug**

## **Mode**

Configure (diagnostic mode).

## **Description**

The **system set malloc** command is a system tuning command used only under the direction of Enterasys support personnel.

## **Parameters**

None.

## **Restrictions**

None.

# system set name

## Purpose

Set the system name.

## Format

**system set name** <system-name>

## Mode

Configure.

## Description

The **system set name** command configures the name of the X-Pedition router. The X-Pedition name will use the name as part of the command prompt.

## Parameters

---

|               |  |
|---------------|--|
| <system-name> | The hostname of the X-Pedition router. If the string contains blanks or commas, you must use quotation marks around the string (e.g., “ <b>Mega-Corp</b> X-Pedition #27”). |
|---------------|--|

---

## Restrictions

None.

# system set password

## Purpose

Set passwords for various CLI access modes.

## Format

**system set password** *<mode>* *<string>*|**none**

## Mode

Configure.

## Description

The **system set password** command sets or changes the passwords for the Login, Enable, and Configure access modes.

**Note:** If a password is configured for the Enable mode, the X-Pedition router prompts for the password when you enter the **enable** command. Otherwise, the X-Pedition router displays a message advising you to configure an Enable password, then enters the Enable mode. From the Enable mode, you can access the Configure mode to make configuration changes. Configuration mode access may require a password.

## Parameters

|                                     |   |
|-------------------------------------|---|
| <i>&lt;mode&gt;</i>                 | The access mode for which you are setting a password. Specify one of the following:<br><br><b>login</b> The password required to start a CLI session. The X-Pedition router prompts for this password when the system finishes booting.<br><br><b>enable</b> The password for entering the Enable mode.<br><br><b>configure</b> The password for entering Configure mode. |
| <i>&lt;string&gt;</i>   <b>none</b> | The password. If you specify <b>none</b> , no password is required.<br><br><b>Note:</b> You cannot use the string “none” as a password.   |

## Restrictions

The X-Pedition router stores passwords in the Startup configuration file. If you copy a configuration file from one X-Pedition router to another, the passwords in the file also are copied and will be required on the new X-Pedition router.

When you activate a new password by copying the password set command to the active configuration, the X-Pedition router replaces the command with a **system set hashed-password** command, which hides the password text in the configuration file so that the password is not visible to others if they examine the configuration file.

To remove a password, enter the following command while in Configure mode:

```
xp(config)# system set password <mode> none
```

# system set password-policy

## Purpose

This command allows you to configure the optional password-related selections. These include the minimum password length, the number of login attempts allowed, and selecting an aging time. For added security, passwords entered into the system appear as asterisks and a password history prevents the use of the 5 previous passwords.

## Format

```
system set password-policy auth-grace-timeout <grace>| change-after-first-login {on|off}|  
expire-warning <warn>| history-size <size>| lifetime <time>|  
login-failure-grace-time <fail-time>| maximum-failed-logins <fails>|  
minimum-length <minimum> verification {on | off}
```

## Mode

Configure.

## Parameters

|   |   |
|---|---|
| <b>auth-grace-timeout</b><br><grace>        | Specifies the amount of time, in seconds, a user has to attempt to successfully log in. After this period expires, the user is disconnected (by default, 60 seconds). This value overrides any value configured by <b>ssh-server set auth-grace-timeout</b> . For details on this command, see <a href="#">ssh-server set auth-grace-timeout on page 1248</a> . |
| <b>change-after-first-login</b> [on   off]  | Select <b>on</b> to require users to change their password after their first login. By default, this option is <b>off</b> .   |
| <b>expire-warning</b><br><warn>             | The number of days prior to password expiration to warn users that their passwords will expire. By default, 14 days.  |
| <b>history-size</b> <size>                  | The number of passwords to keep in user password histories. By default, 5.<br><br><b>Note:</b> To prevent a user from cycling through passwords to reuse an old one, deny the user access to configuration mode—this will prevent the user from resetting the password until the current one expires.   |
| <b>lifetime</b> <time>                      | The duration (in days) that the password will remain valid. By default, 90 days.  |
| <b>login-failure-grace-time</b> <fail-time> | The amount of time to wait once a user reaches the maximum number of failed login attempts before the counter resets and the user is allowed to try again. By default, the router will wait 60 minutes.   |

|   |  |
|---|--|
| <b>maximum-failed-logins</b> < <i>fails</i> > | The number of login failures allowed before disabling a user's account—by default, this value is 6. Entering 0 allows users an unlimited number of attempts. |
| <b>minimum-length</b> < <i>minimum</i> >      | The minimum allowable length for user passwords (the default value is 8). Enter 0 if you do not require a minimum length.                                    |
| <b>verification</b> [on  off]                 | Enables prompt to confirm password entry when adding new users or when changing passwords (the default is <b>on</b> ).                                       |

## Restrictions

None.

## system set poweron-selftest

### Purpose

Specify the type of Power-On-Self-Test (POST) to perform during system bootup.

### Format

**system set poweron-selftest** [on|quick]

### Mode

Configure.

### Description

The **system set poweron-selftest** command configures the type of Power-On-Self-Test (POST) the X-Pedition router should perform during the next system bootup. By default, no POST is performed during system bootup. To perform POST, you must use this command to specify which type of test to run, **quick** or **full**. Once POST enabled, to turn off POST, you simply negate this command (using the **negate** command).

### Parameters

|              |   |
|--------------|---|
| <b>on</b>    | The X-Pedition router will perform a <b>full</b> test during the next system bootup.  |
| <b>quick</b> | The X-Pedition router will perform a <b>quick</b> test during the next system bootup. |

### Restrictions

None.



# system set show-config

## Purpose

Specify how configuration commands should be displayed.

## Format

**system set show-config alphabetical**

## Mode

Configure.

## Description

The **show** and **system show active-config** commands normally display the configuration commands in the order that they are executed. The **system set show-config** command changes the way the configuration commands are shown.

## Parameters

|                     |   |
|---------------------|---|
| <b>alphabetical</b> | Shows the configuration commands in alphabetical order. |
|---------------------|---|

## Restrictions

None.

## Example

To display the configuration commands in alphabetical order:

```
xp(config)# system set show-config alphabetical
```

# system set spooler-memory-limit

## Purpose

Increase the amount of memory allocated to the system spooler.

## Format

**system set spooler-memory-limit** *<memory-limit>*

## Mode

Configure.

## Description

The system spooler buffers CLI output before sending it to a display device. If the %SYS-W-SPOOLOVERFLOW message appears, use the **system set spooler-memory-limit** command to increase the amount of memory allocated to the system spooler. Use caution when increasing the spooler memory limit—increasing the limit to a very high value can adversely affect other areas of the system that may be low on available memory.

## Parameters

---

|                             |   |
|-----------------------------|---|
| <i>&lt;memory-limit&gt;</i> | The amount of memory (300-4000) in kilobytes to allow the system spooler to use. By default, this value is 800. |
|-----------------------------|---|

---

## Restrictions

None.

## Example

To set the spooler memory limit to 1,000 KB use the following:

```
xp(config)# system set spooler-memory-limit 1000
```

# system set syslog

## Purpose

The **system set syslog** command identifies the Syslog server to which the X-Pedition router should send system messages. You can control the type of messages sent based on message severity (controlled by the option **level**) and the facility selected. On the Syslog server, you can decide what to do with these messages based on the level as well as the facility. For example, you might choose to discard the messages, write them to a file or send them out to the console. You can further identify the source of the system messages sent to the Syslog server by specifying a source IP address for the Syslog on the X-Pedition router.

The X-Pedition router keeps the last *<n>* messages in a local circular buffer. By default, this buffer keeps the last 50 Syslog messages. You can change the buffer size to hold anywhere from 10–200 messages. To view the current buffer size, enter the **system show syslog buffer** command.

## Format

```
system set syslog [server <hostname-or-IPaddr>] [local] [level <level-type>]  
[facility <syslog-facility-type>] [source <source-IPaddr>] [buffer-size <size>]
```

## Mode

Configure.

## Parameters

|                                       |   |
|---------------------------------------|---|
| <b>server</b><br><hostname-or-IPaddr> | <p>Hostname or IP address of the Syslog server.</p> <p>If the syslog server is not receiving messages, enter the <b>system show syslog</b> command to view the number of sent and unsent messages. If there are multiple sent messages (e.g., 50) and no unsent messages (i.e., 0), a misconfiguration may exist on the server side. You may also use the <b>system show syslog buffer</b> command to display the last 20 sent messages, or <b>system show syslog buffer number &lt;num&gt;</b> to display the last <i>n</i> sent messages followed by any unsent messages.</p> <p><b>Note:</b> When using the <b>system show syslog buffer</b> command, if the total number of sent messages is fewer than 20, the X-Pedition router will also display any unsent messages—as long as the total number of messages displayed does not exceed 20 (or the number specified).</p> |
|---------------------------------------|---|

|                           |   |              |                           |              |   |                |   |              |  |             |  |
|---------------------------|---|--------------|---------------------------|--------------|---|----------------|---|--------------|--|-------------|--|
| <b>[local]</b>            | <p>This parameter logs Syslog messages to a local log file, <b>int-flash/cfg/syslog</b>—even if you have not configured a remote Syslog server.</p> <p><b>Note:</b> The local flash is <i>NOT the flash card</i>. It is the X-Pedition internal buffer.</p> <p>Each time the router reboots and the Syslog facility initializes, the local Syslog file moves to <b>int-flash/cfg/syslog.bak</b> and a new log is created. Local logging is subject to the Syslog filtering mechanism. To display the contents of the local log files use either of the following:</p> <p>xp# file type syslog</p> <p>xp# file type syslog.bak</p> <p><b>Note:</b> You may still use the <b>system show syslog buffer</b> command to display the buffered messages.</p>  |              |                           |              |   |                |   |              |  |             |  |
| <b>level</b> <level-type> | <p>Level of messages you want the X-Pedition router to log. Specify one of the following:</p> <table><tr><td data-bbox="599 898 651 926"><b>fatal</b></td><td data-bbox="764 898 1036 926">Logs only fatal messages.</td></tr><tr><td data-bbox="599 953 659 980"><b>error</b></td><td data-bbox="764 953 1192 980">Logs fatal messages and error messages.</td></tr><tr><td data-bbox="599 1008 695 1035"><b>warning</b></td><td data-bbox="764 1008 1295 1066">Logs fatal messages, error messages, and warning messages. This is the default.</td></tr><tr><td data-bbox="599 1094 659 1121"><b>audit</b></td><td data-bbox="764 1094 1365 1152">Logs fatal messages, error messages, warning messages, and audit messages.</td></tr><tr><td data-bbox="599 1180 646 1207"><b>info</b></td><td data-bbox="764 1180 1336 1207">Logs all messages, including informational messages.</td></tr></table> | <b>fatal</b> | Logs only fatal messages. | <b>error</b> | Logs fatal messages and error messages. | <b>warning</b> | Logs fatal messages, error messages, and warning messages. This is the default. | <b>audit</b> | Logs fatal messages, error messages, warning messages, and audit messages. | <b>info</b> | Logs all messages, including informational messages. |
| <b>fatal</b>              | Logs only fatal messages.   |              |                           |              |   |                |   |              |  |             |  |
| <b>error</b>              | Logs fatal messages and error messages.   |              |                           |              |   |                |   |              |  |             |  |
| <b>warning</b>            | Logs fatal messages, error messages, and warning messages. This is the default.   |              |                           |              |   |                |   |              |  |             |  |
| <b>audit</b>              | Logs fatal messages, error messages, warning messages, and audit messages.  |              |                           |              |   |                |   |              |  |             |  |
| <b>info</b>               | Logs all messages, including informational messages.  |              |                           |              |   |                |   |              |  |             |  |

|   |  |
|---|--|
| <b>facility</b><br><syslog-facility-type> | Type of facility under which you want messages to be sent. By default, unless specified otherwise, messages are sent under facility <i>local7</i> . The facility-type can be one of the following:                             |
| <b>kern</b>                               | kernel messages  |
| <b>user</b>                               | user messages  |
| <b>daemon</b>                             | daemon messages  |
| <b>local0</b>                             | Reserved for local use   |
| <b>local1</b>                             | Reserved for local use   |
| <b>local2</b>                             | Reserved for local use   |
| <b>local3</b>                             | Reserved for local use   |
| <b>local4</b>                             | Reserved for local use   |
| <b>local5</b>                             | Reserved for local use   |
| <b>local6</b>                             | Reserved for local use   |
| <b>local7</b>                             | Reserved for local use   |
| <b>source</b><br><source-IPaddr>          | Source IP address of the messages sent to the Syslog server. You must specify a Unicast IP address in the form a.b.c.d.  |
| <b>buffer-size</b> <size>                 | The Syslog message buffer size. The size specifies how many messages the Syslog buffer can hold. You can specify a number from 10 – 200, giving the buffer a capacity to hold from 10– 200 Syslog messages. The default is 50. |

## Restrictions

None.

## Example

To enable the syslog client on the X-Pedition router, enter the **system set syslog server** command into the configuration. After you make the configuration active, the router will begin logging syslog messages (if you enter this command in the startup configuration, the X-Pedition router will also log boot messages). To send messages to a directly connected server, enter the following:

```
xp(config)# vlan create vlan_server port-based
xp(config)# vlan add port et.1.1 to vlan_server
xp(config)# interface create ip servernet address-netmask 10.1.1.1/24 vlan vlan_server
xp(config)# system set syslog server 10.1.1.50
```

For a server located at 192.168.1.230:

```
xp(config)# system set syslog server 192.168.1.230
```

For a server located at 192.168.1.230 that logs to facility local6 with a minimum syslog level of info:

```
xp(config)# system set syslog server 192.168.1.230 facility local6 level info
```

For a server located at admin.mycompany.com:

```
xp(config)# system set syslog server admin.mycompany.com
```

**Note:** If you specify a server name, you will need to configure a DNS entry for that server in your domain. If DNS is not running, the X-Pedition router will not be able to resolve the name and the router will eventually drop syslog messages.

To set up a simple syslog server with the syslog server denoted as an IP address:

```
xp(config)# vlan create servernet port-based
xp(config)# vlan add ports et.3.3 to servernet
xp(config)# vlan add ports et.3.7 to servernet
xp(config)# vlan add ports et.3.8 to servernet
xp(config)# interface create ip servers address-netmask 10.10.10.1/24 vlan servernet
xp(config)# system set syslog server 10.10.10.76
```

To set up a simple syslog server with the syslog server denoted as a DNS name:

```
xp(config)# vlan create servernet port-based
xp(config)# vlan add ports et.3.3 to servernet
xp(config)# vlan add ports et.3.7 to servernet
xp(config)# vlan add ports et.3.8 to servernet
xp(config)# interface create ip servers address-netmask 10.10.10.1/24 vlan servernet
xp(config)# system set dns server 10.10.10.55
xp(config)# system set dns domain mycompany.com
xp(config)# system set syslog server logmach
```

The following example demonstrates how to set up a complex server were the facility specified is LOG\_LOCAL6, the system logs only error messages and above, and the sent buffer-size is 10. All syslog messages from this router will be sourced with the IP address of 10.10.10.1:

```
xp(config)# vlan create servernet port-based  
xp(config)# vlan add ports et.3.3 to servernet  
xp(config)# vlan add ports et.3.7 to servernet  
xp(config)# vlan add ports et.3.8 to servernet  
xp(config)# interface create ip servers address-netmask 10.10.10.1/24 vlan servernet  
xp(config)# system set dns server 10.10.10.55  
xp(config)# system set syslog server logmach.mycompany.com facility local6 source 10.10.10.1 level  
error buffer-size 10
```

To log only fatal and error level messages to the Syslog server on 10.1.43.77:

```
xp(config)# system set syslog server 10.1.43.77 level error
```

# system set syslog-levels

## Purpose

This command allows users to override the default Syslog message severity level for a given error message facility. See [system show syslog levels on page 1408](#) for a list of error message facilities. The [system set syslog on page 1387](#) command is used to establish the default message severity level.

## Format

**system set syslog-levels** <facility> **level** <level>

## Mode

Configure.

## Parameters

|            |  |   |
|------------|--|---|
| <facility> | This parameter identifies which error message facility to set to the selected level. |   |
| <level>    | The minimum Syslog message level.  |   |
|            | <b>fatal</b>   | Log fatal messages only.                            |
|            | <b>error</b>   | Log fatal and error messages only.                  |
|            | <b>warning</b>   | Log fatal, error, and warning messages only.        |
|            | <b>audit</b>   | Log fatal, error, audit, and warning messages only. |
|            | <b>info</b>  | Log all messages.                                   |

## Restrictions

None.



# system set terminal

## Format

**system set terminal baud** *<baud-rate>* | **columns** *<number>* **rows** *<number>*

## Mode

Configure.

## Description

The **system set terminal** command globally sets parameters for a serial console's baud rate, output columns, and output rows.

## Parameters

|                                      |  |
|--------------------------------------|--|
| <b>baud</b> <i>&lt;baud-rate&gt;</i> | Sets the baud rate. You can specify one of the following: <ul style="list-style-type: none"> <li>– <b>300</b></li> <li>– <b>600</b></li> <li>– <b>1200</b></li> <li>– <b>2400</b></li> <li>– <b>4800</b></li> <li>– <b>9600</b></li> <li>– <b>19200</b></li> <li>– <b>38400</b></li> </ul> |
| <b>columns</b> <i>&lt;number&gt;</i> | Default number of columns (20—32767 inclusive).  |
| <b>rows</b> <i>&lt;number&gt;</i>    | Default number of rows (0—32767 inclusive). Enter 0 to disable pagination.   |

## Restrictions

None.

## Example

The command in the following example sets the baud rate for the management terminal connected to the System Control module.

```
xp(config)# system set terminal baud 38400
```

## system set tftpsource

### Purpose

Set the IP address to use when uploading file to a TFTP server.

### Format

**system set tftpsource** *<Ip address>*

### Mode

Configure.

### Description

Use this command to specify the source address to use when uploading files to a TFTP server. The IP Address must be a directly connected or management IP address. By default, the X-Pedition router will use the default source address (usually the IP address of the outgoing interface). To change the source address, please refer to the **copy active to tftpserver** command.

### Parameters

|                           |  |
|---------------------------|--|
| <i>&lt;Ip address&gt;</i> | The IP address to use when uploading files to the TFTP server. |
|---------------------------|--|

### Example

|   |
|---|
| xp# <b>system set tftpsource 10.50.88.2</b> |
|---|

# system set timezone

## Purpose

Sets time zone information or time offset.

## Format

**system set timezone** <timezone>|<minutes>

## Mode

Configure.

## Description

The **system set timezone** command sets the local time zone for the X-Pedition router. You can use one of the time zone keywords to specify the local time zone or specify the time offset in minutes. You must configure the time zone in order to use NTP (Network Time Protocol) to synchronize the X-Pedition real time clock.

## Parameters

|               |   |  |
|---------------|---|--|
| <timezone>    | Sets the time zone using one of the following keywords: |  |
| <b>est</b>    | Eastern Standard Time (UCT -05:00)                      |  |
| <b>cst</b>    | Central Standard Time (UCT -06:00)                      |  |
| <b>mst</b>    | Mountain Standard Time (UCT -07:00)                     |  |
| <b>pst</b>    | Pacific Standard Time (UCT -08:00)                      |  |
| <b>uct-12</b> | Eniwetok, Kawajalein (UCT -12:00)                       |  |
| <b>uct-11</b> | Midway Island, Samoa (UCT -11:00)                       |  |
| <b>uct-10</b> | Hawaii (UCT -10:00)                                     |  |
| <b>uct-9</b>  | Alaska (UCT -09:00)                                     |  |
| <b>uct-8</b>  | Pacific Standard Time (UCT -08:00)                      |  |
| <b>uct-7</b>  | Mountain Standard Time (UCT -07:00)                     |  |
| <b>uct-6</b>  | Central Standard Time (UCT -06:00)                      |  |
| <b>uct-5</b>  | Eastern Standard Time (UCT -05:00)                      |  |
| <b>uct-4</b>  | Caracas, La Paz (UCT -04:00)                            |  |
| <b>uct-3</b>  | Buenos Aires, Georgetown (UCT -03:00)                   |  |

|                        |  |
|------------------------|--|
| <b>uct-2</b>           | Mid-Atlantic (UCT -02:00)  |
| <b>uct-1</b>           | Azores, Cape Verde Island (UCT -01:00)   |
| <b>uct</b>             | Greenwich, London, Dublin (UCT)  |
| <b>uct+1</b>           | Berlin, Madrid, Middle European Time, Paris (UCT +01:00)   |
| <b>uct+2</b>           | Athens, Helsinki, Istanbul, Cairo (UCT +02:00)   |
| <b>uct+3</b>           | Moscow, Nairobi, Riyadh (UCT +03:00)   |
| <b>uct+4</b>           | Abu Dhabi, Kabul(UCT +05:00)   |
| <b>uct+5</b>           | Pakistan (UCT +05:00)  |
| <b>uct+5:30</b>        | India (UCT +05:30)   |
| <b>uct+6</b>           | Bangladesh (UCT +06:00)  |
| <b>uct+7</b>           | Bangkok, Jakarta (UCT +07:00)  |
| <b>uct+8</b>           | Beijing, Hong Kong, Singapore(UCT +08:00)  |
| <b>uct+9</b>           | Japan, Korea (UCT +09:00)  |
| <b>uct+10</b>          | Sydney, Guam (UCT +10:00)  |
| <b>uct+11</b>          | Solomon Is. (UCT +11:00)   |
| <b>uct+12</b>          | Fiji, Marshall Is. Auckland (UCT +12:00)   |
| <i>&lt;minutes&gt;</i> | Specify the time zone offset in minutes. Valid values are between -720 minutes to + 720 minutes. |

## Restrictions

None.

## Example

To set the local time zone to Pacific Standard Time (UCT -8:00).

```
xp(config)# system set timezone pst
```

# system set user

## Purpose

The audit trail monitors what administrative changes are performed on the system and who performs them. The **system set user** command allows network administrators to create an account for each user and specify a user ID, password, and access privileges.

See also [system set password-policy on page 1382](#).

## Format

```
system set user <username> [new-password] [password-option {never-expires| normal}]
[privilege-level {login | enable| config}] [status {always-enabled | disabled| enabled}]
```

## Mode

Configure.

## Parameters

|  |   |
|--|---|
| <username>   | The name selected for this user.  |
| <b>new-password</b>  | The router will ask you for the password only after you execute this command—do not enter it as part of this parameter. You must always enter a password when creating an account for a new user or when changing the access privileges for an existing user.                                     |
| <b>password-option</b><br>[never-expires  <br><b>normal</b> ]  | When you select the <b>normal</b> option (the default), the router assigns a lifetime limit to the current user's password. To exempt this user from the password lifetime limit, specify <b>never-expires</b>  |
| <b>privilege-level</b> [login<br>  <b>enable</b> ]   | The mode or privilege where the current user can gain access to the system. You must specify login (non-enable user mode) or enable mode.   |
| <b>status</b><br>[always-enabled  <br><b>disabled</b>   <b>enabled</b> ]                               | To prevent this user account from being disabled after too many failed login attempts, specify <b>always-enabled</b> . To disable this user account, specify <b>disable</b> . To disable the account when the router detects too many failed login attempts, select <b>enabled</b> (the default). |
| <b>Note:</b> Once users are configured, the login prompt changes to request the username and password. |   |

## Restrictions

None.

# system show

## Purpose

Show system information.

## Format

**system show** <system-param>

## Mode

Enable.

## Description

The **system show command** shows the active settings for the following system parameters:

- Active configuration (CLI configuration of the running system)
- Size of the Syslog message buffer
- Contact information for the X-Pedition administrator (if you set one using the **system set contact** command)
- Current system time and date (if you set them using **system set date** command)
- Time that has elapsed since the X-Pedition router was rebooted and the system time and date when the last reboot occurred
- IP address(es) and domain name of DNS servers the X-Pedition router can use (if you set them using **system set dns** command)
- Hardware information
- Location of the X-Pedition router (if you set one using the **system set location** command)
- System name of the X-Pedition router (if you set one using the **system set name** command)
- IP address or hostname of Syslog server and the message level (if you set these parameters using the **system set syslog** command)
- Configuration changes in the scratchpad that are waiting for activation
- Software version running on the Control Module
- Last five Telnet connections to the X-Pedition router
- Current Telnet sessions on the X-Pedition router
- CPU and other resource usage

## Parameters

|                                  |   |  |
|----------------------------------|---|--|
| <code>&lt;system-parm&gt;</code> | System parameter you want to display. Specify one of the following: |  |
|                                  | <b>6000-backplane-status</b> (Advanced Router Module only)          | Shows backplane status of the Advanced Router Module for the SmartSwitch 6000 (6SSRM-02 5SSRM-02).   |
|                                  | <b>active-config</b>  | Shows the active configuration of the system.  |
|                                  | <b>bootlog</b>  | Shows the contents of the boot log file, which contains all the system messages generated during bootup.   |
|                                  | <b>bootprom</b>   | Shows boot PROM parameters for TFTP downloading of the system image. This information is useful only if you have configured the system to download the system image via TFTP.  |
|                                  | <b>buffer-size</b>  | Determines the size (10-200) of the <i>sent</i> buffer. The default value is <b>50</b> .   |
|                                  | <b>capacity all  chassis  task  cpu  memory</b>                     | Shows usage information about various resources on the X-Pedition router. See <a href="#">system show capacity on page 1404</a> .  |
|                                  | <b>contact</b>  | Shows the contact information (administrator name, phone number, and so on).   |
|                                  | <b>cpu-utilization</b>  | Shows the percentage of the CPU that is currently being used.  |
|                                  | <b>date</b>   | Shows the system time and date.  |
|                                  | <b>dns</b>  | Shows the IP addresses and domain names for the DNS servers the X-Pedition router can use.   |
|                                  | <b>environmental-info</b>   | Shows environmental information, such as temperature and power supply status.  |
|                                  | <b>hardware</b>   | Shows detailed hardware information about installed CPUs, switching fabrics, and line cards.   |
|                                  | <b>idle-timeout serial telnet</b>                                   | Shows the timeout value (in minutes). If the communication interface remains idle past <b>idle-timeout</b> value, the communication session will be closed by the system. You can specify a timeout value for a serial connection or a telnet connection. A value of 0 means that the <b>idle-timeout</b> feature is disabled. |
|                                  | <b>location</b>   | Shows the X-Pedition router's location.  |
|                                  | <b>login-banner</b>   | Shows the X-Pedition login banner. The login banner can be configured using the <b>system set login-banner</b> command.  |

|   |  |
|---|--|
| <b>name</b>                             | Shows the X-Pedition name.   |
| <b>poweron-selftest-mode</b>            | Shows the type of Power-On Self Test (POST) that should be performed, if any.  |
| <b>scratchpad</b>                       | Shows the configuration changes in the scratchpad. These changes have not yet been activated.  |
| <b>security-log</b>                     | Displays information on up to five previous users who logged in to the X-Pedition router using TACACS+ or RADIUS.  |
| <b>ssh-access</b>                       | Shows a summary of the last five SSH clients to access the router.   |
| <b>startup-config</b>                   | Shows the contents of the Startup configuration file.  |
| <b>super-diag basic <br/>max-detail</b> | Displays several show commands at once to produce a "snapshot" of the router's current state. The <b>basic</b> option displays basic commands such as <b>system show version</b> and <b>file type bootlog</b> . The <b>max-detail</b> option displays everything the basic option does, plus other commands. Depending on the router's configuration, the output of this command may be extremely verbose. Users should run this command only under the direction of Enterasys Support personnel.  |
| <b>switching-fabric</b>                 | Shows the status of switching fabric cards.  |
| <b>syslog</b>                           | The X-Pedition router can store up to 2000 boot messages to send to the Syslog server—5000 during boot—in the <i>unsent</i> message queue. The X-Pedition router can also store the last 50 <i>sent</i> messages in memory. The Syslog parameter allows you to display the IP address of the Syslog server and the level of messages the X-Pedition router sends to the server (e.g., Minimum Syslog level: INFO, Buffer Size: 50 sent messages 15 unsent messages).   |
| <b>syslog buffer</b>                    | <p>Displays up to 20 of the most recently sent messages. If the total number of sent messages is fewer than 20, the X-Pedition router will also display any unsent messages—as long as the total number of messages does not exceed 20. The X-Pedition router uses “(*)” to denote an unsent Syslog message. See <a href="#">Example on page 1402</a>.</p> <p><b>number</b> &lt;num&gt;    The total number of messages to display.</p> <p><b>levels</b>    Displays the minimum Syslog levels configured for each facility. The following example depicts a sample configuration (refer to <a href="#">Facility Support on page 59</a> and <a href="#">Logging Methods on page 63</a> for further information).</p> |



```
xp# system show syslog levels
```

```
Syslog levels for error message facilities
```

```
----- INFO ----->
```

```
RMON SSH
```

```
----- AUDIT ----->
```

```
SNMP TELNETD VLAN
```

```
----- WARNING ----->
```

```
BGP OSPF PIM RIP
```

```
----- ERROR ----->
```

|              |         |         |           |             |           |
|--------------|---------|---------|-----------|-------------|-----------|
| ACL          | ACL_LOG | AGGRGEN | ATM_DIAG  | ATM         | ARP       |
| AUTH         | BGP     | CDP     | CLI       | CONFIG      | CONS      |
| CTRONCHASSIS | DDT     | DVMRP   | ECCMEM    | ERR         | ETH       |
| FDDI         | GARP    | GATED   | GVRP      | HBT         | INTERFACE |
| IGMP         | IP      | IPC     | IPHELPER  | IPRED       | STRNK     |
| LOADBAL      | L2TM    | L3AGE   | MIRRORING | MULTICAST   | NETSTAT   |
| NI           | NTP     | OSPF    | PHY_POLL  | PIM         | PING      |
| POLICY       | PPP     | PROFILE | PTY       | QOS         | RCP       |
| RDISC        | RES     | RIP     | RL        | RMON        | SIO       |
| SNMP         | SONET   | SR      | SSH       | STATIC      | STATS     |
| STP          | MSTP    | SYSLOG  | SYS       | TELNETD     | TFTP      |
| TR           | TIT3CLI | VLAN    | UNICAST   | WAN         | WC        |
| SAM          | ARE     | ATALK   | COMMON    | NAT         | NETFLOW   |
| PBR          | DHCPD   | IPX     | RARPD     | RELAY       | IPV6      |
| NDISC        | RIPNG   | RTADVD  | PING6     | TRACEROUTE6 |           |

```
----- FATAL ----->
```

```
PTY
```

|                      |   |
|----------------------|---|
| <b>telnet-access</b> | Lists the last five Telnet connections to the X-Pedition router.                        |
| <b>terminal</b>      | Shows the default terminal settings (number of rows, number of columns, and baud rate). |
| <b>timezone</b>      | Shows the time zone offset from UCT in minutes.   |
| <b>uptime</b>        | Shows how much time has elapsed since the most recent reboot.                           |
| <b>users</b>         | Shows the current Telnet connections to the X-Pedition router.                          |

| version | Shows the software version running on the X-Pedition router. |
|---------|--|
|---------|--|

## Restrictions

None.

## Example

Use the **show** command showing configured syslog parameters:

```
xp# system show syslog
```

```
Syslog host: 10.10.10.76, Facility: LOG_LOCAL6
Minimum syslog level: INFO, Buffer Size: 50 sent messages 89 unsent messages
Source IP address: 10.10.10.1
```

Display the actual buffer showing the last 10 messages sent:

```
xp# system show syslog buffer number 10
```

```
2001-10-26 11:31:37 %SYS-W-NOPASSWD, no password for enable, use 'system set password' in Config mode
2001-10-26 11:31:35 %SYS-W-NOPASSWD, no password for login, use 'system set password' in Config mode
2001-10-26 11:31:35 %SYS-I-NETSTART, network interfaces are now enabled
2001-10-26 11:31:35 %SNMP-I-ENABLED, SNMP Agent enabled
2001-10-26 11:31:35 %GATED-I-RECONFIGDONE, Routing configuration changes completed (pid 0x80e763a8).
2001-10-26 11:31:35 %OSPF-I-ROUTERIDFND, OSPF Router Id found: 172.1.1.1
2001-10-26 11:31:34 %STP-I-PORT_STATUS, Port status change detected: et.5.8 - Port Down
2001-10-26 11:31:34 %STP-I-PORT_STATUS, Port status change detected: et.5.7 - Port Down
2001-10-26 11:31:34 %STP-I-PORT_STATUS, Port status change detected: et.5.6 - Port Down
2001-10-26 11:31:34 %STP-I-PORT_STATUS, Port status change detected: et.5.5 - Port Down
(*) denotes an unsent syslog message
```

To display last 10 messages sent to the Syslog server and any unsent messages, enter the following:

```
xp-181-11# system show syslog buffer number 10
```

```
2001-10-26 11:31:35 %SYS-I-NETSTART, network interfaces are now enabled
2001-10-26 11:31:35 %SNMP-I-ENABLED, SNMP Agent enabled
2001-10-26 11:31:35 %GATED-I-RECONFIGDONE, Routing configuration changes completed (pid 0x80e763a8).
2001-10-26 11:31:35 %OSPF-I-ROUTERIDFND, OSPF Router Id found: 172.1.1.1
2001-10-26 11:31:34 %STP-I-PORT_STATUS, Port status change detected: et.5.8 - Port Down
2001-10-26 11:31:34 %STP-I-PORT_STATUS, Port status change detected: et.5.7 - Port Down
2001-10-26 11:31:34 %STP-I-PORT_STATUS, Port status change detected: et.5.6 - Port Down
2001-10-26 11:31:34 %STP-I-PORT_STATUS, Port status change detected: et.5.5 - Port Down
2001-10-26 11:31:37 (*) %SYS-W-NOPASSWD, no password for enable, use 'system set password' in Config mode
2001-10-26 11:31:35 (*) %SYS-W-NOPASSWD, no password for login, use 'system set password' in Config mode
(*) denotes an unsent syslog message
```

To display information on the last users to log in to the X-Pedition router using TACACS+ or RADIUS, enter the following:

```
xp-181-11# system show security-log

User ID           : johnny
tty               : tty1
Security Type     : Radius
Last AAA server used : 10.136.15.101
Number of Sessions : 1
Start Session Time : 2002-06-27 09:10:16
Connection Status  : Currently Connected
Last Session ended at : 2002-06-27 09:09:54
Time Last Accessed : 2002-06-27 09:26:34
Last Command      : system show security-log
Current Mode       : Enable
Config command Cntr : 0
Enable command Cntr : 1
Login command Cntr  : 3
Total command Cntr  : 4
```

### Field Descriptions

|                              |  |
|------------------------------|--|
| <b>User ID</b>               | The user ID used to log in   |
| <b>tty</b>                   | Connected through  |
| <b>Security Type</b>         | The security methodology used  |
| <b>Last AAA server used</b>  | Authenticated to what authentication server  |
| <b>Start Session Time</b>    | The timestamp of when the user connected to the router. If not currently connected, this indicates the previous connection time.         |
| <b>Connection Status</b>     | Indicates whether or not the user's connection is active.  |
| <b>Last Session ended at</b> | The timestamp of the first time the user connected since boot. If this is the first time, the "First time connected since boot" message. |
| <b>Time Last Accessed</b>    | The timestamp of the most recent command entered by the user.  |
| <b>Last Command</b>          | The most recent command entered.   |
| <b>Current Mode</b>          | The active CLI mode (i.e., enable, config, login).   |
| <b>Config command Cntr</b>   | The number of commands executed from configuration mode.   |
| <b>Enable command Cntr</b>   | The number of commands executed from enable mode.  |
| <b>Login command Cntr</b>    | The number of commands executed from login mode.   |
| <b>Total command Cntr</b>    | The total number of commands executed.   |

# system show capacity

## Format

**system show capacity all | chassis | task | cpu | memory**

## Mode

Enable.

## Description

The **system show capacity** command displays information about the X-Pedition resources.

## Parameters

|                |   |
|----------------|---|
| <b>all</b>     | Shows all the capacity MIB information. |
| <b>chassis</b> | Shows the chassis capacity information. |
| <b>task</b>    | Shows the task capacity information.    |
| <b>cpu</b>     | Shows the CPU capacity information.     |
| <b>memory</b>  | Shows the memory capacity information.  |

## Restrictions

None.

## Example

To display usage information for all X-Pedition resources:

|                                   |                |                 |                   |                         |                          |       |       |
|-----------------------------------|----------------|-----------------|-------------------|-------------------------|--------------------------|-------|-------|
| xp# system show capacity all      |                |                 |                   |                         |                          |       |       |
| Capacity MIB Chassis Information: |                |                 |                   |                         |                          |       |       |
| Total Slots                       | Used Slots     | Free Slots      | CPU Redundancy    | Power Supply Redundancy | Switch Fabric Redundancy |       |       |
| -----                             | -----          | -----           | -----             | -----                   | -----                    |       |       |
| 8                                 | 7              | 1               | Present           | Present                 | No Support               |       |       |
| Capacity MIB Task Information:    |                |                 |                   |                         |                          |       |       |
| Index                             | Name           | Count           | Task Status       | Memory Used             |                          |       |       |
| -----                             |                | -----           | -----             | -----                   |                          |       |       |
| 1                                 | CONS_T         | 2               | Suspended (event) | 8096                    |                          |       |       |
| 6                                 | IPX_T          | 16996           | Suspended (event) | 8096                    |                          |       |       |
| 11                                | STATS_T        | 169939          | Suspended (event) | 8096                    |                          |       |       |
| 16                                | PHY_POLL       | 339892          | Suspended (event) | 16384                   |                          |       |       |
| 21                                | L3_ACL_T       | 1               | Suspended (event) | 16192                   |                          |       |       |
| 26                                | IPC            | 2               | Suspended (event) | 8096                    |                          |       |       |
| 31                                | PINGER_T       | 7623            | Suspended (event) | 8096                    |                          |       |       |
| 36                                | BOUNCE         | 2               | Suspended (event) | 8096                    |                          |       |       |
| 41                                | CONS2T         | 2               | Suspended (event) | 8096                    |                          |       |       |
| Capacity MIB Storage Information: |                |                 |                   |                         |                          |       |       |
| Type                              | Description    | Size            | Free              | Used                    | Block                    | Remov | Fail  |
| -----                             |                | -----           | -----             | -----                   | -----                    | ----- | ----- |
| CPU                               | Internal CPU   | 4194304         | 3837935           | 356369                  | 16                       | True  | 0     |
| FLASH                             | Internal Flash | 756             | 745               | 11                      | 64                       | True  | 0     |
| L2HW                              | port et.2.1    | 5888            | 5887              | 1                       | 64                       | True  | 0     |
| L2HW                              | port et.2.2    | 5888            | 5887              | 1                       | 64                       | True  | 0     |
| L2HW                              | port et.2.3    | 5888            | 5887              | 1                       | 64                       | True  | 0     |
| L2HW                              | port et.2.4    | 5888            | 5887              | 1                       | 64                       | True  | 0     |
| L2HW                              | port et.2.5    | 5888            | 5887              | 1                       | 64                       | True  | 0     |
| L2HW                              | port et.2.6    | 5888            | 5887              | 1                       | 64                       | True  | 0     |
| L2HW                              | port et.2.7    | 5888            | 5887              | 1                       | 64                       | True  | 0     |
| L2HW                              | port et.2.8    | 5888            | 5887              | 1                       | 64                       | True  | 0     |
| L2HW                              | port et.3.1    | 5888            | 5887              | 1                       | 64                       | True  | 0     |
| L2HW                              | port et.3.2    | 5888            | 5887              | 1                       | 64                       | True  | 0     |
| L2HW                              | port et.3.3    | 5888            | 5887              | 1                       | 64                       | True  | 0     |
| L2HW                              | port et.3.4    | 5888            | 5887              | 1                       | 64                       | True  | 0     |
| .                                 |                |                 |                   |                         |                          |       |       |
| Capacity MIB CPU Information:     |                |                 |                   |                         |                          |       |       |
| Slot                              | Util           | L3 Learned/Aged | L2 Learned/Aged   | NIA Received/Xmt        |                          |       |       |
| -----                             | -----          | -----           | -----             | -----                   |                          |       |       |
| 0                                 | 1              | 0 /0            | 0 /0              | 0 /75684                |                          |       |       |
| xp#                               |                |                 |                   |                         |                          |       |       |

## Field Definitions

| Field   | Description   |
|---|---|
| <i>Capacity MIB Chassis Information displays information about the chassis:</i> |   |
| Total Slots   | The total number of slots in the chassis, including the slot for the CPU. |
| Used Slots  | The number of used slots, including the slot used by the CPU.             |
| Free Slots  | The number of available slots.  |
| CPU Redundancy  | A redundant control module is present.                                    |
| Power Supply Redundancy   | A redundant power supply is present.                                      |
| Switch Fabric Redundancy  | A redundant switch fabric is installed (XP-8600 only).                    |

*Capacity MIB Task Information displays information about the tasks scheduled for the CPU:*

|             |  |
|-------------|--|
| Index       | The unique index assigned to the task.   |
| Name        | The encrypted name assigned to the task. This is unique for each type of task.   |
| Count       | The number of times the task was scheduled to run. This represents a cumulative count from the time the router was started.  |
| Task Status | The current status of the task. The task status can be <i>Ready</i> (task is scheduled and ready), <i>Suspended</i> (task is waiting for something, such as a queue or memory), <i>Finished</i> , or <i>Terminated</i> . |
| Memory Used | The amount of memory consumed by the task. This can be used to monitor the excess memory used by a particular task and is expressed in bytes.  |

*Capacity Storage Information provides information about the non-volatile memory devices in the router:*

|             |   |
|-------------|---|
| Type        | The type of storage device.                                   |
| Description | Describes the storage device.                                 |
| Size        | The total memory capacity of the device, expressed in blocks. |

| Field  | Description  |
|--------|--|
| Free   | The amount of free memory in the device, expressed in blocks./   |
| Used   | The size of the used memory on the device, expressed in blocks. This includes blocks of memory that are used only partially.   |
| Block  | The size of the memory blocks in the memory device. This is the minimum block size of memory returned when requesting memory. This value is expressed in bytes.                          |
| Remove | Indicates whether or not the memory can be removed.  |
| Fail   | The number of times a memory allocation in the memory device has failed. For Layer-2 and Layer-3 hardware, this refers to the number of times a full hash bucket condition has been met. |

*Capacity MIB CPU Information displays information about the various hardware tables:*

|              |   |
|--------------|---|
| Slot         | The slot number of the CPU.   |
| Utilization  | The CPU utilization expressed as an integer percentage. This is calculated over the last 5 seconds at a 0.1 second interval as a simple average.  |
| L3 Learned   | The total number of new Layer-3 flows the CPU has processed and programmed into the Layer-3 hardware flow tables. Layer-3 flows are IP or IPX packets that are routed from one subnet to another. |
| L3 Aged      | The total number of Layer-3 flows that were removed from the Layer-3 hardware flow table across all modules.  |
| L2 Learned   | The total number of Layer-2 flows or addresses learned.   |
| L2 Aged      | The total number of Layer-2 flows that were removed from the Layer-2 lookup tables.   |
| NIA Received | The total number of packets received by the NIA chip. This is useful in gauging how many packets are forwarded to the CPU for processing.   |
| NIA XMT      | The total number of packets transmitted by the NIA chip. This is useful in determining how much the CPU communicates directly with management stations and other routes.                          |

## **system show syslog levels**

### **Purpose**

This command allows users to view the Syslog message facility levels. The output for each facility indicates the minimum Syslog message level configured.

### **Format**

**system show syslog levels**

### **Mode**

Enable.

### **Parameters**

None.

### **Restrictions**

None.

### **Example**

The following example uses the Syslog configuration below:

```
system set syslog server 10.136.15.101 local level error
system set syslog-levels RMON level info
system set syslog-levels SNMP level audit
system set syslog-levels VLAN level audit
system set syslog-levels SSH level info
system set syslog-levels OSPF level warning
system set syslog-levels RIP level warning
system set syslog-levels BGP level warning
system set syslog-levels PIM level warning
system set syslog-levels TELNETD level audit
system set syslog-levels PTY level fatal
```



```

xp# system show syslog levels
Syslog levels for error message facilities

----- INFO ----->
RMON SSH

----- AUDIT ----->
SNMP TELNETD VLAN

----- WARNING ----->
BGP OSPF PIM RIP

----- ERROR ----->
ACL          ACL_LOG  AGGRGEN      ATM_DIAG     ATM          ARP
AUTH         BGP      CDP          CLI          CONFIG       CONS
CTRONCHASSIS DDT      DVMRP       ECCMEM       ERR          ETH
FDDI         GARP     GATED       GVRP        HBT          INTERFACE
IGMP         IP       IPC         IPHELPER     IPRED        STRNK
LOADBAL      L2TM    L3AGE      MIRRORING   MULTICAST    NETSTAT
NI           NTP     OSPF       PHY_POLL    PIM          PING
POLICY       PPP     PROFILE    PTY         QOS          RCP
RDISC        RES     RIP        RL          RMON        SIO
SNMP         SONET   SR         SSH         STATIC       STATS
STP          MSTP    SYSLOG     SYS         TELNETD     TFTP
TR           TIT3CLI VLAN        UNICAST     WAN          WC
SAM          ARE     ATALK      COMMON      NAT          NETFLOW
PBR          DHCPD   IPX        RARPD       RELAY        IPV6
NDISC        RIPNG   RTADVD     PING6       TRACEROUTE6

----- FATAL ----->
PTY

```

### Field Descriptions

|          |  |
|----------|--|
| ACL      | Access Control List                    |
| ACL_LOG  | Access Control List Log                |
| AGGRGEN  | Aggregated/Generated Root              |
| ARE      | Advanced Routing Engine                |
| ARP      | Address Resolution Protocol            |
| ATALK    | Apple-Talk                             |
| ATM      | Asynchronous Transfer Mode             |
| ATM_DIAG | Asynchronous Transfer Mode Diagnostics |
| AUTH     | Authentication                         |
| BGP      | Border Gateway Protocol                |

|              |  |
|--------------|--|
| CDP          | Cabletron/Cisco Discovery Protocol         |
| CLI          | Command Line Interface                     |
| COMMON       | Common Command Line Interface              |
| CONFIG       | Configuration                              |
| CONS         | Console                                    |
| CTRONCHASSIS | Chassis-Related                            |
| DDT          | Dynamic Disassembly Tool                   |
| DHCPD        | Dynamic Host Configuration Protocol        |
| DVMRP        | Distance Vector Multicast Routing Protocol |
| ECCMEM       | Error Correcting Code Memory               |
| ERR          | Error                                      |
| ETH          | 10Base-T Ethernet Driver                   |
| FDDI         | Fiber Distributed Data Interface           |
| GARP         | Generic Attribute Registration Protocol    |
| GATED        | Gate Daemon                                |
| GVRP         | GARP VLAN Registration Protocol            |
| HBT          | Control Module Heartbeat                   |
| IGMP         | Internet Group Membership Protocol         |
| INTERFACE    | Interface                                  |
| IP           | IP Stack                                   |
| IPC          | The IPC facility used by WAN               |
| IPHELPER     | The IP Helper and BOOTP/DHCP Relay Agent   |
| IPRED        | IP Redundancy (VRRP)                       |
| IPV6         | IP Stack Version 6                         |
| IPX          | Internet Packet Exchange                   |
| L2TM         | Layer-2 Table Manager                      |
| L3AGE        | Layer-3 Aging facility                     |
| LOADBAL      | Load Balance                               |
| MIRRORING    | Mirroring                                  |
| MSTP         | Multiple Spanning Tree Protocol            |
| MULTICAST    | Multicast                                  |
| NAT          | Network Address Translation                |
| NDISC        | Neighbor Discovery                         |
| NETFLOW      | NetFlow                                    |
| NETSTAT      | Netstat                                    |

|          |  |
|----------|--|
| NI       | Network Interface Driver                     |
| NTP      | Network Time Protocol                        |
| OSPF     | Open Shortest Path First                     |
| PBR      | IP Policy                                    |
| PHY_POLL | Phy_Poll                                     |
| PIM      | Protocol Independent Multicast               |
| PING     | Ping   |
| PING6    | Ping Version 6                               |
| POLICY   | Policy                                       |
| PPP      | Point-to-Point Protocol                      |
| PROFILE  | Profile                                      |
| PTY      | Pseudo TTY                                   |
| QOS      | Quality of Service                           |
| RARPD    | Reverse Address Resolution Protocol          |
| RCP      | Remote Copy Protocol                         |
| RDISC    | Router Discovery                             |
| RELAY    | Relay  |
| RES      | Resolver                                     |
| RIP      | Routing Information Protocol                 |
| RIPNG    | Routing Information Protocol Next Generation |
| RL       | Rate Limit                                   |
| RMON     | Remote Network Monitoring                    |
| RTADVD   | Router Advertisement Daemon                  |
| SAM      | Security Attack Monitor                      |
| SIO      | Serial Input/Output                          |
| SNMP     | Simple Network Management Protocol           |
| SONET    | Packet-Over-Sonet                            |
| SR       | Temperature-Related Messages                 |
| SSH      | Secure Shell                                 |
| STATIC   | Static Address                               |
| STATS    | Statistics                                   |
| STP      | Spanning Tree Protocol                       |
| STRNK    | SmartTRUNK                                   |
| SYS      | System                                       |
| SYSLOG   | Syslog                                       |

|             |                                |
|-------------|--------------------------------|
| T1T3CLI     | T1/T3 Configuration Commands   |
| TELNETD     | Telnet                         |
| TFTP        | Trivial File Transfer Protocol |
| TR          | Traceroute                     |
| TRACEROUTE6 | Traceroute for IPv6 packets    |
| UNICAST     | Unicast                        |
| VLAN        | Virtual Local Area Network     |
| WAN         | Wide Area Network              |
| WC          | Web Cache                      |

# Chapter 75

## tacacs-plus Commands

The **tacacs-plus** commands let you secure access to the X-Pedition router using the TACACS Plus protocol. When users log in to the X-Pedition router or try to access Enable mode, they are prompted for a password. If TACACS Plus authentication is enabled on the X-Pedition router, it will contact a TACACS Plus server to verify the user. If the user is verified, he or she is granted access to the X-Pedition router.

### Notes:

- The X-Pedition router currently supports the Password Authentication Protocol (PAP) method of authentication but not the Challenge Handshake Authentication Protocol (CHAP) method.
- The X-Pedition router no longer supports TACACS and will ignore any commands used for it in the configuration—without generating an error.

## Command Summary

[Table 63](#) lists the **tacacs-plus** commands. The sections following the table describe the command syntax.

**Table 63. tacacs-plus Commands**

|  |
|--|
| <b>tacacs-plus accounting command level</b> <i>&lt;level&gt;</i> |
| <b>tacacs-plus accounting shell</b> start stop all               |
| <b>tacacs-plus accounting snmp</b> active startup                |
| <b>tacacs-plus accounting system</b> fatal error warning info    |
| <b>tacacs-plus authentication</b> login enable system            |

**Table 63. tacacs-plus Commands (Continued)**

|  |
|--|
| <b>tacacs-plus enable</b>  |
| <b>tacacs-plus set server</b> <IPaddr> [ <b>port</b> <number>] [ <b>timeout</b> <number>] [ <b>retries</b> <number>]<br>[ <b>deadtime</b> <number>] [ <b>key</b> <string>] [ <b>source</b> <IFname_IPaddr>]                        |
| <b>tacacs-plus set</b> [ <b>timeout</b> <number>] [ <b>retries</b> <number>] [ <b>deadtime</b> <number>] [ <b>key</b> <string>]<br>[ <b>source</b> <IFname_IPaddr>] [ <b>last-resort password</b>   <b>succeed</b>   <b>deny</b> ] |
| <b>tacacs-plus show stats</b>  all   |

# tacacs-plus accounting command level

## Purpose

Causes the specified types of commands to be logged to the TACACS Plus server.

## Format

**tacacs-plus accounting command level** <level>

## Mode

Configure.

## Description

The **tacacs-plus accounting command level** command allows you specify the types of commands that are logged to the TACACS Plus server. The user ID and timestamp are also logged.

## Parameters

|           |   |
|-----------|---|
| <level>   | Specifies the type(s) of commands that are logged to the TACACS Plus server. Enter one of the following values: |
| <b>5</b>  | Log Configure commands.   |
| <b>10</b> | Log all Configure and Enable commands.  |
| <b>15</b> | Log all Configure, Enable, and User commands.   |

## Restrictions

None.

## Example

To cause Configure, Enable, and User mode commands to be logged on the TACACS Plus server:

```
xp(config)# tacacs-plus accounting command level 15
```

# tacacs-plus accounting shell

## Purpose

Causes an entry to be logged on the TACACS Plus server when a shell is stopped or started on the X-Pedition router.

## Format

**tacacs-plus accounting shell start|stop|all**

## Mode

Configure.

## Description

The **tacacs-plus accounting shell** command allows you to track shell usage on the X-Pedition router. It causes an entry to be logged on the TACACS Plus server when a shell is started or stopped. You can specify that an entry be logged when a shell is started, when a shell is stopped, or when a shell is either started or stopped.

## Parameters

|              |   |
|--------------|---|
| <b>start</b> | Logs an entry when a shell is started.                  |
| <b>stop</b>  | Logs an entry when a shell is stopped                   |
| <b>all</b>   | Logs an entry when a shell is either started or stopped |

## Restrictions

None.

## Example

To cause an entry to be logged on the TACACS Plus server when a shell is either started or stopped on the X-Pedition router:

```
xp(config)# tacacs-plus accounting shell all
```



# tacacs-plus accounting snmp

## Purpose

Logs to the TACACS Plus server any changes made to the startup or active configuration via SNMP.

## Format

**tacacs-plus accounting snmp active|startup**

## Mode

Configure.

## Description

The **tacacs-plus accounting snmp** command allows you to track changes made to the active or startup configuration through SNMP. It causes an entry to be logged on the TACACS Plus server whenever a change is made to the ACL configuration. You can specify that an entry be logged to the active or startup configuration.

## Parameters

|                |   |
|----------------|---|
| <b>active</b>  | Logs an entry when a change is made to the active configuration.  |
| <b>startup</b> | Logs an entry when a change is made to the startup configuration. |

## Restrictions

None.

## Example

To cause an entry to be logged on the TACACS Plus server whenever an ACL configuration change is made via SNMP to the active configuration:

```
xp(config)# tacacs-plus accounting snmp active
```

## **tacacs-plus accounting system**

### **Purpose**

Specifies the type(s) of messages to be logged on the TACACS Plus server.

### **Format**

**tacacs-plus accounting system fatal|error|warning|info**

### **Mode**

Configure.

### **Description**

The **tacacs-plus accounting system** command allows you to specify the types of messages that are logged on the TACACS Plus server.

### **Parameters**

|                |  |
|----------------|--|
| <b>fatal</b>   | Logs only fatal messages.                                  |
| <b>error</b>   | Logs fatal messages and error messages.                    |
| <b>warning</b> | Logs fatal messages, error messages, and warning messages. |
| <b>info</b>    | Logs all messages, including informational messages.       |

### **Restrictions**

None.

### **Example**

To log only fatal and error messages on the TACACS Plus server:

```
xp(config)# tacacs-plus accounting system error
```

# tacacs-plus authentication

## Purpose

Causes TACACS Plus authentication to be performed at either the X-Pedition login prompt or when the user tries to access Enable mode.

## Format

**tacacs-plus authentication login|enable|system**

## Mode

Configure.

## Description

The **tacacs-plus authentication** command allows you to specify when TACACS Plus authentication is performed: either when a user logs in to the X-Pedition router, or tries to access Enable mode.

## Parameters

|               |   |
|---------------|---|
| <b>login</b>  | Authenticates users at the X-Pedition login prompt.                         |
| <b>enable</b> | Authenticates users when they try to access Enable mode.                    |
| <b>system</b> | Authenticates \$enab<n>\$user when they try to access Enable or Login mode. |

## Restrictions

None.

## Example

To perform TACACS Plus authentication at the X-Pedition login prompt:

```
xp(config)# tacacs-plus authentication login
```

# **tacacs-plus enable**

## **Purpose**

Enables TACACS Plus authentication on the X-Pedition router. TACACS Plus authentication is disabled by default on the X-Pedition router.

## **Format**

**tacacs-plus enable**

## **Mode**

Configure.

## **Description**

The **tacacs-plus enable** command causes TACACS Plus authentication to be activated on the X-Pedition router. You set TACACS Plus-related parameters with the **tacacs-plus set**, **tacacs-plus accounting shell**, and **tacacs-plus authorization** commands, then use the **tacacs-plus enable** command to activate TACACS Plus authentication.

## **Parameters**

None.

## **Restrictions**

None.

## **Example**

The following commands set TACACS Plus-related parameters on the X-Pedition router. The commands are then activated with the **tacacs-plus enable** command:

```
xp(config)# tacacs-plus set server 207.135.89.15
xp(config)# tacacs-plus set timeout 30
xp(config)# tacacs-plus authentication login
xp(config)# tacacs-plus accounting shell all
xp(config)# tacacs-plus enable
```

# tacacs-plus set

## Purpose

Sets default parameters for authenticating the X-Pedition router through a TACACS-Plus server.

## Format

**tacacs-plus set** [**timeout** <number>] [**retries** <number>] [**deadtime** <number>] [**key** <string>]  
[**source** <IFname\_IPaddr>] [**last-resort password|succeed|deny**]

## Mode

Configure.

## Description

The **tacacs-plus set** command allows you to set TACACS-Plus-related parameters on the X-Pedition router, how long to wait for the TACACS-Plus server to authenticate the user, an encryption key, and what to do if the TACACS-Plus server does not reply by a given time.

## Parameters

|                          |   |
|--------------------------|---|
| <b>timeout</b> <number>  | Is the maximum time (1-30) in seconds to wait for a TACACS-Plus server to reply. The default is 3 seconds.  |
| <b>retries</b> <number>  | The default number of times (1-10) to attempt to contact a server.  |
| <b>deadtime</b> <number> | The length of time for transaction requests to skip over a TACACS-Plus server—up to a maximum of 1440 minutes (24 hours). This command causes the X-Pedition router to mark as “dead” any TACACS-Plus server that fails to respond to authentication requests, thus avoiding the wait for the request to timeout before trying the next configured server. Additional requests for a TACACS-Plus server marked as “dead” will skip the server for the duration of minutes specified (unless all servers are marked “dead”). |
| <b>key</b> <string>      | An encryption key shared with the TACACS-Plus server. The maximum length of this string is 128 bytes.<br><br>If you do not specify an encryption key, the TACACS-Plus packet will not be encrypted (the default). If you defined multiple TACACS-Plus servers and need to encrypt only <i>some</i> of them, use the <b>key</b> parameter of the <b>tacacs-plus set server</b> command to encrypt the servers. You cannot remove the key on an individual server after creating the default key.                             |

|                                  |   |
|----------------------------------|---|
| <b>source</b><br><Ifname_IPaddr> | Sets the source interface name or IP address for TACACS-Plus messages.<br><br>Enterasys recommends that you use alphabetic characters when defining interface names—purely numeric interfaces will be interpreted as IP addresses. The X-Pedition router will display interface names up to 32 characters in length.  |
| <b>last-resort</b>               | Is the action to take if a TACACS-Plus server does not reply within the time specified by the <b>timeout</b> parameter. Specify one of the following:<br><br><b>password</b> The user is prompted for the password set with <b>system set password</b> command (if one has been set).<br><br><b>succeed</b> Access to the X-Pedition router is granted.<br><br><b>deny</b> Unable to connect to TACACS server, access to the X-Pedition router is denied. |

## Restrictions

None.

## Example

The following commands specify that hosts 137.72.5.9 and 137.72.5.41 are TACACS Plus servers, and the X-Pedition router should wait no more than 30 seconds for a response from one of these servers. If a response from a TACACS-Plus server doesn't arrive in 30 seconds, the user is prompted for the password that was set with the X-Pedition **system set password** command.

```
xp(config)# tacacs-plus set server 137.72.5.9
xp(config)# tacacs-plus set server 137.72.5.41
xp(config)# tacacs-plus set timeout 30
xp(config)# tacacs-plus set last-resort password
```

# tacacs-plus set server

## Purpose

Sets parameters for authenticating the X-Pedition router through a specific TACACS-Plus server.

## Format

**tacacs-plus set server** <IPaddr> [**port** <number>] [**timeout** <number>] [**retries** <number>] [**deadtime** <number>] [**key** <string>] [**source** <Ifname\_IPaddr>]

## Mode

Configure.

## Description

The **tacacs-plus set server** command allows you to set TACACS-Plus-related parameters on the X-Pedition router, including the IP address of a specific TACACS-Plus server, how long to wait for the TACACS-Plus server to authenticate the user, an encryption key, and what to do if the TACACS-Plus server does not reply by a given time.

## Parameters

|                          |  |
|--------------------------|--|
| <b>server</b> <IPaddr>   | IP address of a TACACS-Plus server. You can enter up to five TACACS Plus servers. Enter one server per <b>tacacs-plus set server</b> command.  |
| <b>port</b> <number>     | TACACS-Plus TCP port you will use (1-65535). The default port is 49.   |
| <b>timeout</b> <number>  | Maximum time (1-30) in seconds to wait for a TACACS Plus server to reply. The default is 3 seconds.  |
| <b>retries</b> <number>  | Default number of times (1-10) to attempt to contact this TACACS server.   |
| <b>deadtime</b> <number> | Length of time for transaction requests to skip over a TACACS server—up to a maximum of 1440 minutes (24 hours). This command causes the X-Pedition router to mark as “dead” any TACACS server that fails to respond to authentication requests, thus avoiding the wait for the request to timeout before trying the next configured server. Additional requests for a TACACS server marked as “dead” will skip the server for the duration of minutes specified (unless all servers are marked “dead”). |
| <b>key</b> <string>      | Encryption key to be shared with the TACACS-Plus server. The maximum length of this string is 128 bytes.   |

---

|                                  |  |
|----------------------------------|--|
| <b>source</b><br><IFname_IPaddr> | Sets the source interface name or IP address for TACACS-Plus messages.   |
| <b>Note:</b>                     | Enterasys recommends that you use alphabetic characters when defining interface names—purely numeric interfaces will be interpreted as IP addresses. The X-Pedition router displays interface names up to 32 characters in length. |

---

## Restrictions

None.

## Example

The following commands specify that hosts 137.72.5.9 and 137.72.5.41 are TACACS-Plus servers, and the X-Pedition router should wait no more than 30 seconds for a response from one of these servers. If a response from a TACACS Plus server doesn't arrive in 30 seconds, the user is prompted for the password that was set with the X-Pedition **system set password** command.

```
xp(config)# tacacs-plus set server 137.72.5.9
xp(config)# tacacs-plus set server 137.72.5.41
xp(config)# tacacs-plus set timeout 30
xp(config)# tacacs-plus set last-resort password
```



# tacacs-plus show

## Purpose

Displays information about TACACS Plus configuration on the X-Pedition router.

## Format

**tacacs-plus show stats**|all

## Mode

Enable.

## Description

The **tacacs-plus show** command displays statistics and configuration parameters related to TACACS Plus configuration on the X-Pedition router. The statistics displayed include:

- accepts**    Number of times each server responded and validated the user successfully.
- rejects**    Number of times each server responded and denied the user access, either because the user wasn't known, or the wrong password was supplied.
- timeouts**   Number of times each server did not respond.

## Parameters

|              |   |
|--------------|---|
| <b>stats</b> | Displays the accepts, rejects, and timeouts for each TACACS Plus server.  |
| <b>all</b>   | Displays the configuration parameters set with the <b>tacacs-plus set</b> command, in addition to the accepts, rejects, and timeouts for each TACACS Plus server. |

## Restrictions

None.

## Example

To display configuration parameters and TACACS Plus server statistics:

```
xp# tacacs-plus show all
TACACS+ status:          ACTIVE
TACACS+ last resort:      Succeed when server fails
Command Level Logging:    15 - Log Configure, Enable and User Commands
Default TACACS+ timeout (seconds): 3
Default TACACS+ retries:  3
Default TACACS+ deadtime (minutes):0
Default TACACS+ key:      net
Default TACACS+ source IP address: Let system decide

TACACS+ servers listed in order of priority:

Server:          10.136.16.102
Port:            49
Timeout (seconds): <Default>
Retries:         <Default>
Deadtime (minutes): 3
Key:             net
Source IP:        <Default>
Server is dead. Will be made tested again in 2 minutes

Server:          10.136.15.100
Port:            49
Timeout (seconds): <Default>
Retries:         <Default>
Deadtime (minutes): <Default>
Key:             net
Source IP:        <Default>

Server:          10.136.15.101
Port:            49
Timeout (seconds): <Default>
Retries:         <Default>
Deadtime (minutes): <Default>
Key:             net
Source IP:        <Default>

TACACS+ server host statistics:

Host      Accepts  Rejects  Timeouts
10.136.16.102  0      0      3
10.136.15.100  1      0      0    * Sever being used
10.136.15.101  0      0      0
```

# Chapter 76

## telnet Command

### Format

**telnet** <hostname-or-IPaddr> [**socket** <socket-number>]

### Mode

User or Enable.

### Description

The **telnet** command allows you to open a Telnet session to the specified host.

### Parameters

|                                  |   |
|----------------------------------|---|
| <hostname-or-IPaddr>             | The host name or IP address of the remote computer that you want to access.   |
| <b>socket</b><br><socket-number> | The TCP port through which the Telnet session will be opened. If this parameter is not specified, the Telnet port (socket number 23) is assumed. This parameter can be used to test other ports; for example, socket number 21 is the port for FTP. |

### Restrictions

Secure Shell (**ssh**) is a “secure” replacement for Telnet. SSH provides the same remote access to the X-Pedition router that Telnet provides, but does so securely by encrypting all session data—including passwords.

**Note:** When you enable the SSH server, the X-Pedition router automatically disables Telnet access.

---

## Example

To open a Telnet session on the host “xp4”:

```
xp# telnet xp4
```

# Chapter 77

## traceroute Command

This chapter describes the **traceroute** command.

### traceroute

#### Purpose

Trace the path a packet takes to reach a remote IPv4 or IPv6 host from the X-Pedition router or from a user-specified source address.

#### Format

```
traceroute{<IPv4addr> | <IPv6addr> | <hostname> [ipv6]}  
[<IPv4 Parameters> | <IPv6 Parameters>]
```

#### Mode

User.

#### Description

The **traceroute** command traces the route taken by a packet to reach a remote IP host. If you enter an IPv4 address or hostname, ICMPv4 Echo Request messages are sent. If you enter an IPv6 address or hostname (identified with the **ipv6** keyword), ICMPv6 Echo Requests will be sent.

The **traceroute** command examines the route taken by a packet traveling from a source to a destination. By default, the source of the packet is the X-Pedition router. However, if you are tracing the path to an IPv4 host, the IPv4 parameter **source** allows you to specify a different source and track the route between it and a destination.

The route is calculated by initially sending a probe (ICMP Echo Request packet) from the source to the destination with a TTL of 1. Each intermediate router that is not able to reach the final destination directly will send back an ICMP Time Exceeded message. Subsequent probes from the source will increase the TTL value by 1. As each Time Exceeded message is received, the program keeps track of the address of each intermediate gateway.

When tracing the path to an IPv4 host, the probing stops when the packet reaches the destination or the TTL exceeds the **max-ttl** value. When tracing the path to an IPv6 host, the process continues until the destination is reached or until the command is interrupted with the terminal interrupt key sequence.

Use the optional IPv4 parameters listed below with an IPv4 address or hostname, and the optional IPv6 parameters listed below with an IPv6 address or hostname.

## Parameters

---

|                                      |   |
|--------------------------------------|---|
| <code>&lt;IPv4addr&gt; /</code>      | Specifies the destination host.   |
| <code>&lt;IPv6addr&gt; /</code>      |   |
| <code>&lt;hostname&gt; [ipv6]</code> | If you enter an IPv4 address or an IPv4 hostname, the router will send ICMPv4 Echo Requests.<br><br>If you enter an IPv6 address or an IPv6 hostname followed by the <b>ipv6</b> keyword, the router will send ICMPv6 Echo Requests. By default, <i>hostname</i> is assumed to be IPv4. The <b>ipv6</b> keyword must be specified to declare a hostname an IPv6 hostname. |

---

## IPv4 Parameters

---

|  |   |
|--|---|
| <b>max-ttl</b> <code>&lt;num&gt;</code>    | Maximum number of gateways (“hops”) to trace. Default is 30.  |
| <b>probes</b> <code>&lt;num&gt;</code>     | Number of probes to send  |
| <b>size</b> <code>&lt;num&gt;</code>       | Packet size of each probe. Default is 40 bytes.   |
| <b>source</b> <code>&lt;host&gt;</code>    | Hostname or IPv4 address of the source  |
| <b>tos</b> <code>&lt;num&gt;</code>        | Type of Service value in the probe packet   |
| <b>wait-time</b> <code>&lt;secs&gt;</code> | Maximum time in seconds to wait for a response  |
| <b>verbose</b>                             | Displays results in verbose mode  |
| <b>no-route</b>                            | Ignores the routing table and sends a probe to a host on a directly attached network. If the destination is not on the local network, an error is returned. |

---

## IPv6 Parameters

|                        |  |
|------------------------|--|
| <b>wait-time</b> <sec> | The time to wait in seconds before issuing another Echo Request with the same TTL. The default is 1 second. The maximum value is 100 seconds.                                  |
| <b>probes</b> <num>    | The number of times to re-issue Echo Requests with the same TTL before incrementing the TTL for the next message. The default is 3 retries. The maximum value is 1000 retries. |

## Restrictions

None.

## Example

To display the route from the X-Pedition router to the host *othello* in verbose mode:

```
xp# tracert othello verbose
tracert to 20.1.1.1 (20.1.1.1), 30 hops max, 40 byte packets
 1
 36 bytes from 20.1.1.1 to 20.1.1.2 : icmp type 3 (Dest Unreachable) code 3

 4: x45000028
 8: xbd1e0000
12: x0111d2a2
16: x14010102
20: x14010101
24: xbd1d829b
28: x00140000
32: x0000002f
 20.1.1.1 (20.1.1.1) 36 bytes to 20.1.1.2 20 ms
 36 bytes from 20.1.1.1 to 20.1.1.2 : icmp type 3 (Dest Unreachable) code 3

 4: x45000028
 8: xbd1f0000
12: x0111d2a1
16: x14010102
20: x14010101
24: xbd1d829c
28: x00140000
32: x0000002f
 0 ms *
```





# Chapter 78

## vlan Commands

The **vlan** commands allow the user to perform the following tasks:

- Create VLANs
- List VLANs
- Add ports to VLANs
- Deny the addition of new ports to VLANs
- Change the port membership of VLANs
- Make a VLAN port either a trunk port or an access port

### Command Summary

[Table 64](#) lists the **vlan** commands. The sections following the table describe the command syntax.

**Table 64. vlan Commands**

|   |
|---|
| <b>vlan add ports</b> <port-list> <b>to</b> <vlan-name>   |
| <b>vlan create</b> <vlan-name> <type> <b>id</b> <num>   |
| <b>vlan default-vlan ports</b> <port-list> <b>on</b> <vlan-name>                                  |
| <b>vlan enable l4-bridging</b> <b>on</b> <vlan-name>  |
| <b>vlan forbid ports</b> <port-list> <b>from</b> <string>   |
| <b>vlan make</b> <port-type> <port-list>  |
| <b>vlan multi-add ports</b> <port-list> <b>to</b> <basename> <b>id</b> <num> <b>through</b> <num> |
| <b>vlan multi-create</b> <basename> <type> <b>id</b> <num> <b>through</b> <num>                   |
| <b>vlan show</b>  |
| <b>vlan untagged ports</b> <port-list> <b>on</b> <vlan-name>                                      |

## vlan add ports

### Purpose

Adds ports to a VLAN.

### Format

**vlan add ports** <port-list> **to** <vlan-name>

### Mode

Configure.

### Description

The **vlan add ports** command adds ports and trunk ports to an existing VLAN. You do not need to specify the VLAN type when you add ports (you specify the VLAN type when you create the VLAN). For information about creating VLANs, see [vlan create on page 1435](#).

### Parameters

|             |  |
|-------------|--|
| <port-list> | The ports you are adding to the VLAN. You can specify a single port or a comma-separated list of ports. Example: et.1.3,et.(1-3).(4,6-8).        |
| <vlan-name> | Name of the VLAN to which you are adding ports.<br><br><b>Note:</b> The X-Pedition router will display VLAN names up to 32 characters in length. |

### Restrictions

The VLAN to which you add ports must already exist. To create a VLAN, use the **vlan create** command. An access port can be added to only one IP VLAN, one IPX VLAN, and one bridged-protocols VLAN.

# vlan create

## Purpose

Creates a VLAN based on ports or protocol.

## Format

**vlan create** <vlan-name> <type> [**id** <num>]

## Mode

Configure.

## Description

The **vlan create** command creates a VLAN definition. You can create a port-based VLAN or a protocol-based VLAN. For information about adding ports and trunk ports to a VLAN, see [vlan add ports on page 1434](#).

## Parameters

|              |  |
|--------------|--|
| <vlan-name>  | Name of the VLAN. The VLAN name is a string up to 32 characters long.  |
| <b>Note:</b> | The VLAN name cannot begin with an underscore ( _ ) or the word "SYS_". The names "control," "default," "blackhole," "reserved," and "learning" cannot be used. The X-Pedition router will display VLAN names up to 32 characters in length. |

---

|                       |   |
|-----------------------|---|
| <b>&lt;type&gt;</b>   | <p>The type of VLAN you are adding. The VLAN type determines the types of traffic the X-Pedition router will forward on the VLAN. Specify any combination of the first seven types that follow <b>or</b> specify <b>port-based</b>:</p> <p><b>ip</b> Create this VLAN for IP traffic</p> <p><b>ipx</b> Create this VLAN for IPX traffic</p> <p><b>appletalk</b> Create this VLAN for AppleTalk traffic</p> <p><b>dec</b> Create this VLAN for DECnet traffic</p> <p><b>sna</b> Create this VLAN for SNA traffic</p> <p><b>ipv6</b> Create this VLAN for IPv6 traffic</p> <p><b>bridged-protocols</b> Create this VLAN for extended VLAN types (DEC, SNA, Appletalk, IPv6), and non-IP and non-IPX protocols</p> <p><b>Note:</b> You can specify a combination of <b>ip</b>, <b>ipx</b>, <b>appletalk</b>, <b>dec</b>, <b>sna</b>, <b>ipv6</b>, and <b>bridged-protocols</b>. If you specify <i>any</i> of the extended VLAN types (<b>sna</b>, <b>dec</b>, <b>appletalk</b>, <b>ipv6</b>) with the <b>bridged-protocols</b> option, then all the other extended VLAN types are removed from the VLAN. See <a href="#">Table 65</a>.</p> |
| <b>port-based</b>     | <p>Create this VLAN for all traffic types listed above (port-based VLAN).</p> <p><b>Note:</b> You can specify a combination of <b>ip</b>, <b>ipx</b>, <b>appletalk</b>, <b>dec</b>, <b>sna</b>, <b>ipv6</b>, and <b>bridged-protocols</b> <i>or</i> you can specify <b>port-based</b>; you cannot specify <b>port-based</b> with any of the other options.</p>  |
| <b>id &lt;num&gt;</b> | <p>ID of this VLAN. The ID must be unique. You can specify a number from 2 – 4094. If more than one X-Pedition router will be configured with the same VLAN, you must specify the same VLAN ID on each router. If the ID is not specified, the X-Pedition router will assign the smallest ID from 2 – 4094 that has not already been assigned.</p>  |

---

**Table 65. Extended VLAN Types and Exclusions**

| Configuration Command  | Protocols Included in VLAN                     | Protocols Excluded from VLAN                    |
|--|--|---|
| <b>vlan create &lt;vlan-name&gt; ip</b>                            | <b>IP</b>                                      | <b>IPX, SNA, IPv6, DECnet, Appletalk, Other</b> |
| <b>vlan create &lt;vlan-name&gt; ip bridged-protocols</b>          | <b>IP, SNA, DECnet, IPv6, Appletalk, Other</b> | <b>IPX</b>                                      |
| <b>vlan create &lt;vlan-name&gt; ip bridged-protocols sna</b>      | <b>IP, SNA, Other</b>                          | <b>IPX, IPv6, DECnet, Appletalk</b>             |
| <b>vlan create &lt;vlan-name&gt; ip bridged-protocols sna ipv6</b> | <b>IP, SNA, IPv6, Other</b>                    | <b>IPX, DECnet, Appletalk</b>                   |

## Restrictions

The following *cannot* be used for VLAN names:

- control
- default
- blackhole
- reserved
- learning
- names starting with an underscore (\_) or “sys\_”

**Note:** The X-Pedition router will display VLAN names up to 32 characters in length.

**Note:** Specify both SNA and bridged-protocol to successfully create an SNA based VLAN. The SNA-protocol-based VLAN (implemented in version 3.0 and later) needs to be configured with the following command:

**vlan create sna bridged-protocols id <id#>**

in order to forward all SNA protocol types. Refer to the following Technical Bulletin for more detail: TB0973-1

If assigning a VLAN to a trunk port, the user should specify an ID instead of allowing the router to automatically assign an ID.

## Examples

The following command creates a VLAN 'blue' for IP, SNA, non-IPX, non-DECnet, non-Appletalk, non-IPv6 protocols:

```
xp(config)# vlan create blue ip bridged-protocols sna
```

The following command creates a VLAN 'red' for IP, non-IPX, and extended VLAN types SNA, DECnet, Appletalk, and IPv6:

```
xp(config)# vlan create red ip bridged-protocols
```

# vlan default-vlan ports

## Format

**vlan default-vlan ports** <port-list> **on** <vlan-name>

## Mode

Configure.

## Description

The **vlan default-vlan ports** command specifies which VLAN to assign untagged packets received on this port. When a user adds a trunk port to a VLAN with the **vlan add ports** command, the router sets the default VLAN to VLAN 1 (DEFAULT VLAN). Users may change the default setting by using this command.

After changing the default VLAN on a trunk port, the port is no longer associated with the previous default VLAN. For example, the default VLAN is changed from VLAN 1 to VLAN 2; all ingress traffic tagged with VLAN ID 1 will be dropped. However, changing the default VLAN again, such as VLAN 2 to VLAN 3, does not cause the ingress traffic tagged with VLAN ID 2 to be dropped, unless VLAN ID 2 is specifically disassociated with the port.

## Parameters

|             |   |
|-------------|---|
| <port-list> | The ports to which to assign the default VLAN. Users may specify a single port or a comma-separated list of ports. For example: et.1.3, et.(1-3).(4,6-8).                 |
| <vlan-name> | The name of the VLAN to use as the default VLAN for the specified ports.<br><br><b>Note:</b> The X-Pedition router will display VLAN names up to 32 characters in length. |

## Restrictions

The VLAN must already exist and users should have added the ports to the VLAN with the **vlan add ports** command.

This command can be used only with trunk ports. It is not used with access ports.

# vlan enable

## Purpose

Enable VLAN specific features.

## Format

**vlan enable l4-bridging on** <vlan-name>

## Mode

Configure.

## Description

The **vlan enable** command allows you to enable VLAN features.

## Parameters

|                       |  |
|-----------------------|--|
| <vlan-name>           | The name of the VLAN.<br><br><b>Note:</b> The X-Pedition router will display VLAN names up to 32 characters in length. |
| <b>l4-bridging on</b> | This optional parameter enables Layer-4 bridging.  |

## Restrictions

None.



# vlan forbid ports

## Purpose

Forbids ports from being added to an existing VLAN.

## Format

**vlan forbid ports** <port-list> **from** <string>

## Mode

Configure.

## Description

The **vlan forbid ports** command prevents the addition of new ports to a VLAN.

## Parameters

|             |  |
|-------------|--|
| <port-list> | Specifies forbidden ports. You can specify a single port or use commas to specify a list of ports. For example: et.1.3, et.(1-3), (4,6-8). |
| <string>    | Specifies name of a valid VLAN.  |
|             | <b>Note:</b> The X-Pedition router will display VLAN names up to 32 characters in length.  |

## Restrictions

None.

## Example

The following command forbids ports et.1.1 and et.1.2 from VLAN red:

```
xp(config)# vlan forbid ports et.1.(1-2) from red
```

# vlan make

## Purpose

Configures the specified ports into either trunk or access ports.

## Format

**vlan make trunk-port** <port-list>

## Mode

Configure.

## Description

The **vlan make** command turns a port into a VLAN trunk or VLAN access port. A VLAN trunk port can forward traffic for multiple VLANs. Use trunk ports when you want to connect X-Pedition switches together and send traffic for multiple VLANs on a single network segment connecting the switches. When you create a trunk port, you must use the **vlan add ports** command to add the trunk port to a VLAN.

**Note:** When you create a VLAN trunk, make sure the port you use is not already assigned to an existing VLAN (other than the default). After you define the trunk, you must convert it to 802.1Q in order to add it to an existing non-default VLAN.

By default, the default VLAN (VLAN ID 1) is always assigned to all VLAN trunks. Enter the following command from Configure mode to filter default VLAN traffic from a trunk:

|   |  |
|---|--|
| Filter default VLAN traffic from a list of trunk ports. | filters add address-filter name NODEFAULTVLAN<br>source-mac ffffff:ffffff source-mac-mask<br>000000:000000 vlan 1 in-port-list <port-list> |
|---|--|

## Parameters

|                   |  |
|-------------------|--|
| <b>trunk-port</b> | The port forwards traffic for multiple VLANs. The X-Pedition router will encapsulate all traffic in IEEE 802.1Q tag headers. All ports are access-ports by default. Access-ports forward traffic only for the VLANs to which you have added the ports, and the traffic will be untagged. To turn a trunk-port into an access-port, negate the <b>vlan make trunk-port</b> command. |
| <port-list>       | The ports you are configuring. You can specify a single port or a comma-separated list of ports. Example: et.1.3,et.(1-3).(4,6-8).   |

## **Restrictions**

Link aggregation groups (LGs) cannot be changed from access-ports to trunk-ports or from trunk-ports to access-ports if they belong to any VLAN other than the default. Therefore the LG must be removed from all VLANs, prior to executing this command, then added back in after execution.

# vlan multi-add

## Purpose

Adds ports to multiple VLANS. Used with the vlan multi-create command.

## Format

**vlan multi-add ports** *<port-list>* **to** *<basename>* **id** *<num>* **through** *<num>*

## Mode

Configure.

## Description

The **vlan multi-add ports** command adds ports to existing VLANS created with the vlan multi-create command.

## Parameters

|                                   |  |
|-----------------------------------|--|
| <i>&lt;port-list&gt;</i>          | The ports you are adding to the VLANS. You can specify a single port or a comma-separated list of ports. Example: et.1.3,et.(1-3).(4,6-8). |
| <i>&lt;basename&gt;</i>           | The basename of the VLANS to add ports to.   |
| <b>id</b> <i>&lt;num&gt;</i>      | The starting ID of the VLANS to add ports to.  |
| <b>through</b> <i>&lt;num&gt;</i> | The ending ID of the VLANS to add ports to.  |

## Restrictions

The VLANS to which you add ports must already exist. To create multiple VLANS, use the vlan multi-create command. Ports must be trunk ports to be used with this command.

## Example

The following command adds ports to VLANS RED2, RED3, RED4, and RED5.

**vlan multi-add ports gi.1.1-2 to RED id 2 through 5**

# vlan multi-create

## Purpose

Creates multiple VLANS based on ports or protocol.

## Format

**vlan multi-create** *<basename>* *<type>* **id** *<num>* **through** *<num>*

## Mode

Configure.

## Description

The **vlan multi-create** command creates multiple VLANS. The name of the VLAN will be the basename appended with the VLAN ID.

## Parameters

|                         |   |
|-------------------------|---|
| <i>&lt;basename&gt;</i> | The basename of the VLAN. VLAN IDS will be appended to the basename for the VLAN name. The X-Pedition router will display VLAN names up to 32 characters in length. |
|-------------------------|---|

|                            |   |
|----------------------------|---|
| <b>&lt;type&gt;</b>        | <p>The type of VLAN you are adding. The VLAN type determines the types of traffic the X-Pedition router will forward on the VLAN. Specify any combination of the first seven types that follow <i>or</i> specify <b>port-based</b>:</p> <p><b>ip</b> Create this VLAN for IP traffic</p> <p><b>ipx</b> Create this VLAN for IPX traffic</p> <p><b>appletalk</b> Create this VLAN for AppleTalk traffic</p> <p><b>dec</b> Create this VLAN for DECnet traffic</p> <p><b>sna</b> Create this VLAN for SNA traffic</p> <p><b>ipv6</b> Create this VLAN for IPv6 traffic</p> <p><b>bridged-protocols</b> Create this VLAN for extended VLAN types (DEC, SNA, Appletalk, IPv6), and non-IP and non-IPX protocols</p> <p><b>Note:</b> You can specify a combination of <b>ip</b>, <b>ipx</b>, <b>appletalk</b>, <b>dec</b>, <b>sna</b>, <b>ipv6</b>, and <b>bridged-protocols</b>. If you specify <i>any</i> of the extended VLAN types (<b>sna</b>, <b>dec</b>, <b>appletalk</b>, <b>ipv6</b>) with the <b>bridged-protocols</b> option, then all the other extended VLAN types are removed from the VLAN. See <a href="#">Table 66</a>.</p> |
| <b>port-based</b>          | <p>Create this VLAN for all traffic types listed above (port-based VLAN)</p> <p><b>Note:</b> You can specify a combination of <b>ip</b>, <b>ipx</b>, <b>appletalk</b>, <b>dec</b>, <b>sna</b>, <b>ipv6</b>, and <b>bridged-protocols</b> <i>or</i> you can specify <b>port-based</b>; you cannot specify <b>port-based</b> with any of the other options.</p>   |
| <b>id &lt;num&gt;</b>      | The starting ID of the VLANS to be created. This ID must be smaller than the end ID.  |
| <b>through &lt;num&gt;</b> | The ending ID of the VLANS to be created.   |

Table 66. Extended VLAN Types and Exclusions

| Configuration Command      | Protocols Included in VLAN | Protocols Excluded from VLAN             |
|----------------------------|----------------------------|--|
| vlan create <vlan-name> ip | IP                         | IPX, SNA, IPv6, DECnet, Appletalk, Other |

| Configuration Command                                 | Protocols Included in VLAN              | Protocols Excluded from VLAN |
|---|---|------------------------------|
| vlan create <vlan-name> ip bridged-protocols          | IP, SNA, DECnet, IPv6, Appletalk, Other | IPX                          |
| vlan create <vlan-name> ip bridged-protocols sna      | IP, SNA, Other                          | IPX, IPv6, DECnet, Appletalk |
| vlan create <vlan-name> ip bridged-protocols sna ipv6 | IP, SNA, IPv6, Other                    | IPX, DECnet, Appletalk       |

## Restrictions

The following *cannot* be used for VLAN names:

- control
- default
- blackhole
- reserved
- learning
- names starting with an underscore (\_) or “sys\_”

**Note:** The X-Pedition router will display VLAN names up to 32 characters in length.

**Note:** Specify both SNA and bridged-protocol to successfully create an SNA based VLAN. The SNA-protocol-based VLAN (implemented in version 3.0 and later) needs to be configured with the following command:

**vlan multi-create** <basename> **sna bridged-protocols id** <num> **through** <num>

in order to forward all SNA protocol types. Refer to the following Technical Bulletin for more detail: TB0973-1

## Example:

The following command creates VLANS RED2, RED3, RED4, and RED5.

```
vlan multi-create RED id 2 through 5
```

## **vlan show**

### **Purpose**

Displays a list of all active VLANs on the X-Pedition router.

### **Format**

**vlan show**

### **Mode**

User or Enable.

### **Description**

The **vlan show** command lists all the VLANs that have been configured on the X-Pedition router.

### **Parameters**

None.

### **Restrictions**

None.



# vlan untagged ports

## Format

**vlan untagged ports** <port-list> **on** <vlan-name>

## Mode

Configure.

## Description

The **vlan untagged ports** command specifies that a port previously added to the VLAN with **vlan add ports** command will send untagged packets. This command only applies to egress traffic.

## Parameters

|             |   |
|-------------|---|
| <port-list> | The port(s) to use when sending untagged packets. Users may specify a single port or a comma-separated list of ports.<br>For example, et.1.3, et.(1-3).(4,6-8). |
| <vlan-name> | Name of the VLAN to which you are specifying untagged ports.<br><br><b>Note:</b> The X-Pedition will display VLAN names up to 32 characters in length.          |

## Restrictions

The VLAN must already exist and the ports should have been added previously to the VLAN with the **vlan add ports** command.



# Chapter 79

## web-cache Commands

The **web-cache** commands allow you to transparently redirect HTTP requests to a group of local cache servers. This feature can provide faster user responses and reduce demands for WAN bandwidth.

### Command Summary

[Table 67](#) lists the **web-cache** commands. The sections following the table describe the command syntax.

**Table 67. web-cache Commands**

|  |
|--|
| <b>web-cache</b> <cache-name> <b>apply interface</b> <interface-name>  |
| <b>web-cache clear</b> all cache-name <cache-name>   |
| <b>web-cache</b> <cache-name> <b>create bypass-list range</b> <ipaddr-range>  <b>list</b> <ipaddr-list>  <b>acl</b> <acl-name>   |
| <b>web-cache</b> <cache-name> <b>create server-list</b> <server-list-name> <b>range</b> <ipaddr-range>  <b>list</b> <ipaddr-list>  |
| <b>web-cache</b> <cache-name> <b>permit deny hosts range</b> <ipaddr-range>  <b>list</b> <ipaddr-list>  <b>acl</b> <acl-name>  |
| <b>web-cache</b> <cache-name> <b>set</b> [ <b>maximum-connections</b> <number>]   [ <b>http-port</b> <port-number>]   [ <b>round-robin</b> { <b>range</b> <ipaddr-range>  <b>list</b> <ipaddr-list>}]   [ <b>server-options</b> { <b>ping-interval</b> <number>   <b>ping-attempts</b> <number>   <b>app-interval</b> <number>   <b>app-attempts</b> <number>   <b>no-application-check</b> }] |
| <b>web-cache show</b> [all] [cache-name <cache-name> all] [servers cache <cache-name> all]   |

# web-cache apply interface

## Purpose

Applies a caching policy to an interface.

## Format

**web-cache** *<cache-name>* **apply interface** *<interface-name>*

## Mode

Configure.

## Description

The **web-cache apply** command lets you apply a configured cache policy to an outbound interface to start the redirection. The interface to which the cache policy is applied is typically the interface that connects to the Internet. This command redirects outbound HTTP traffic to the cache servers.

## Parameters

|                               |   |
|-------------------------------|---|
| <i>&lt;cache-name&gt;</i>     | The name of a cache policy configured with the <b>web-cache create server-list</b> command.   |
| <i>&lt;interface-name&gt;</i> | The name of the outbound interface that connects to the actual Web server. Typically, this is the interface that connects to the Internet.<br><br><b>Note:</b> Enterasys recommends that you use alphabetic characters when defining interface names—purely numeric interfaces will be interpreted as IP addresses. The X-Pedition router displays interface names up to 32 characters in length. |

## Restrictions

None.

## Example

To apply the caching policy 'websrv1' to the interface 'inet2':

```
xp(config)# web-cache websrv1 apply interface inet2
```

# web-cache clear

## Purpose

Clears statistics for the specified caching policy.

## Format

**web-cache clear all|cache-name** *<cache-name>*

## Mode

Enable.

## Description

The **web-cache clear** command lets you clear statistics for all caching policies or for specified policies.

## Parameters

|  |   |
|--|---|
| <b>all</b>                                     | Clears statistics for all caching policies.         |
| <b>cache-name</b><br><i>&lt;cache-name&gt;</i> | Clears statistics for the specified caching policy. |

## Restrictions

None.

## Examples

To clear statistics for the caching policy 'websrv1':

```
xp# web-cache clear cache-name websrv1
```

# web-cache create bypass-list

## Purpose

Defines the destination sites for which HTTP requests are not redirected to the cache servers, but sent direct.

## Format

```
web-cache <cache-name> create bypass-list range <ipaddr-range>|list <ipaddr-list>|  
acl <acl-name>
```

## Mode

Configure.

## Description

Certain web sites require authentication of source IP addresses for user access. Requests to these sites cannot be sent to the cache servers. The **web-cache create bypass-list** command allows you to define the destinations to which HTTP requests must be sent directly without redirection to a cache server. You can specify a range of IP addresses, a list of up to four IP addresses, or an ACL that qualifies these hosts.

## Parameters

|                                |  |
|--------------------------------|--|
| <cache-name>                   | The name of the caching policy for which the specified hosts will not apply.   |
| <b>range</b><br><ipaddr-range> | A range of host IP addresses in the form “176.89.10.10 176.89.10.50”. This adds the hosts 176.89.10.10, 176.89.10.11, etc., through 176.89.10.50 to the bypass list.   |
| <b>list</b> <ipaddr-list>      | A list of up to four destination IP addresses in the form “176.89.10.10 176.89.10.11 176.89.10.12”.  |
| <b>acl</b> <acl-name>          | Name of the ACL profile that defines the packet profile to bypass. The ACL may contain either <b>permit</b> or <b>deny</b> keywords. The <b>web-cache create bypass-list</b> command only looks at the following ACL rule parameter values: protocol, source IP address, destination IP address, source port, destination port, and TOS. |

## Restrictions

None.

## Examples

To specify the hosts 176.89.10.10 and 176.89.10.11 for the bypass list for the caching policy 'webserv1':

```
xp(config)# web-cache webserv1 create bypass-list list "176.89.10.10 176.89.10.11"
```

To specify the hosts defined in the ACL 'nocache' for the bypass list for the caching policy 'webserv1':

```
xp(config)# web-cache webserv1 create bypass-list acl nocache
```

# web-cache create server-list

## Purpose

Defines the list of servers to be used for caching.

## Format

**web-cache** <cache-name> **create server-list** <server-list-name> **range** <ipaddr-range> |  
**list** <ipaddr-list>

## Mode

Configure.

## Description

The **web-cache create server-list** command allows you to create a group of servers that are used for the specified caching policy. If there are multiple cache servers, load balancing is done based on the destination IP address. If any cache server fails, traffic is redirected to other active servers. You can specify either a range of IP addresses or a list of up to four IP addresses. Note that traffic that is sent from a server in the server list is not redirected.

## Parameters

|                                |  |
|--------------------------------|--|
| <cache-name>                   | The name of the caching policy.  |
| <server-list-name>             | The name of this list of servers.  |
| <b>range</b><br><ipaddr-range> | A range of host IP addresses in the form “176.89.10.10 176.89.10.50”. This adds the hosts 176.89.10.10, 176.89.10.11, etc., through 176.89.10.50 to the server list. |
| <b>list</b> <ipaddr-list>      | A list of up to four host IP addresses in the form “176.89.10.10 176.89.10.11 176.89.10.12”.   |

## Restrictions

None.

## Example

To specify the server list ‘servers1’ for the caching policy ‘websrv1’:

```
xp(config)# web-cache websrv1 create server-list servers1 range “10.10.10.10 10.10.10.50”
```



# web-cache permit|deny hosts

## Purpose

Specifies the hosts whose HTTP requests are redirected to the cache servers.

## Format

```
web-cache <cache-name> permit|deny hosts range <ipaddr-range>|list <ipaddr-list> |  
acl <acl-name>
```

## Mode

Configure.

## Description

The **web-cache permit** command lets you specify the hosts (users) whose HTTP requests are redirected to the cache servers, while the **web-cache deny** command lets you specify the hosts whose HTTP requests are not redirected to the cache servers. If no **permit** command is specified, all HTTP requests are redirected to the cache servers. You can specify a range of IP addresses, a list of up to four IP addresses, or an ACL that qualifies these hosts.

## Parameters

|                                |   |
|--------------------------------|---|
| <cache-name>                   | The name of the cache.  |
| <b>range</b><br><ipaddr-range> | A range of host IP addresses in the form “176.89.10.10 176.89.10.50”.   |
| <b>list</b> <ipaddr-list>      | A list of up to four host IP addresses in the form “176.89.10.10 176.89.10.11 176.89.10.12”.  |
| <b>acl</b> <acl-name>          | Name of the ACL profile to be used. This defines the profile of the packets to be permitted or denied. The <b>web-cache permit/deny</b> command only looks at the following ACL rule parameter values: protocol, source IP address, destination IP address, source port, destination port, and TOS. |

## Restrictions

None.

## Examples

To allow the HTTP requests of certain hosts to be redirected to the cache servers:

```
xp(config)# web-cache webserv1 permit hosts range "10.10.20.10 10.10.20.50"
```

To specify that the HTTP requests of certain hosts not be redirected to the cache servers:

```
xp(config)# web-cache webserv1 deny hosts list "10.10.20.61 10.10.20.75"
```

# web-cache set

## Format

```
web-cache <cache-name> set [maximum-connections <number>]| [http-port <port number>]|
[round-robin {range <ipaddr-range>| list <ipaddr-list>}] |
[server-options {ping-interval <number>| ping-attempts <number>| app-interval <number>|
app-attempts <number> | no-application-check}]
```

## Mode

Configure.

## Description

Web caching provides a way to store frequently accessed Web objects on a cache of local servers. Each HTTP request is transparently redirected by the X-Pedition router to a configured cache server. The first time a user accesses a Web object, the object is stored on a cache server—each subsequent request for the object uses this cached object. Web caching allows multiple users to access Web objects stored on local servers with a much faster response time than accessing the same objects over a WAN connection. This can also result in substantial cost savings by reducing the WAN bandwidth usage.

**Note:** The X-Pedition router itself does not act as cache for web objects. It redirects HTTP requests to local servers on which the web objects are cached. One or more local servers are needed to work as cache servers with the RS.s web caching function.

The **web-cache set** command allows users to specify the behavior of a web caching server group.

## Parameters

|  |   |
|--|---|
| <b>maximum-connections</b><br><number> | The limit of connections to support for a web caching server group. This number is the maximum number of connections allowed for each server in a list of web caching servers. (This list must already have been created with the <b>web-cache create server-list</b> command.) |
| <b>http-port</b><br><port number>      | Some networks use proxy servers that listen for HTTP requests on a non-standard port number. The <b>http-port</b> parameter lets you specify the port number used by the proxy server for HTTP requests. Specify a value between 1 and 65535 (the default is 80).               |

|                       |  |  |
|-----------------------|--|--|
| <b>round-robin</b>    | If a certain web site is accessed very frequently, the cache server that services HTTP requests to this web site can become overloaded with user requests. The <b>round-robin</b> parameter allows users to distribute destination IP addresses for HTTP requests across cache servers in a round-robin manner. If a cache server fails, the address range associated with that server is redistributed among the remaining servers. |  |
|                       | <b>range</b> <i>&lt;ipaddr-range&gt;</i>   | A range of host IP addresses in the form “176.89.10.10 176.89.10.50”.                                |
|                       | <b>list</b> <i>&lt;ipaddr-list&gt;</i>   | A list of up to four destination IP addresses in the form “176.89.10.10 176.89.10.11 176.89.10.12”.  |
| <b>server-options</b> | Use the server-options command to set various parameters for a group of web cache servers.   |  |
|                       | <b>ping-interval</b> <i>&lt;number&gt;</i>   | Set interval (in seconds, from 1 to 3600) for ping checks to this server-list.                       |
|                       | <b>ping-attempts</b> <i>&lt;number&gt;</i>   | Set number (from 1 to 255) of failed ping attempts before server is considered down.                 |
|                       | <b>app-interval</b> <i>&lt;number&gt;</i>  | Set interval (in seconds, from 1 to 3600) for application checks to this server-list.                |
|                       | <b>app-attempts</b> <i>&lt;number&gt;</i>  | Set the number (from 1 to 255) of failed application attempts before application is considered down. |
|                       | <b>no-application-check</b>  | Disable TCP application health checking for this server-list.  |

## Restrictions

None.

## Examples

To limit the number of connections for servers in the server list *servers1* to 1000 connections:

```
xp(config)# web-cache set maximum-connections servers1 1000
```

To set the port number for HTTP requests:

```
xp(config)# web-cache websvr1 set http-port 100
```

To specify destination IP addresses to be distributed across the caching policy 'websvr1' servers:

```
xp(config)# web-cache set round-robin list "176.20.20.10 176.20.50.60"
```

To ping the servers in the list *service2* in the cache group *websvr1* every 10 seconds:

```
xp(config)# web-cache websvr1 set server-options service2 ping-int 10
```

## web-cache show

### Purpose

Displays information about caching policies.

### Format

**web-cache show** [**all**] [**cache-name** <cache-name>|**all**] [**servers cache** <cache-name>|**all**]

### Mode

Enable.

### Description

The **web-cache show** command allows you to display web caching information for specific caching policies or server lists.

### Parameters

|  |   |
|--|---|
| <b>all</b>                                       | Displays all web cache information for all caching policies and all server lists.   |
| <b>cache-name</b><br><cache-name>  <b>all</b>    | Displays web cache information for the specified caching policy. <b>all</b> displays all caching policies.                          |
| <b>servers cache</b><br><cache-name>  <b>all</b> | Displays information for the servers configured for the specified caching policy. <b>all</b> displays all configured cache servers. |

### Restrictions

None.

## Examples

To display web cache information for all caching policies and server lists:

```
xp# web-cache show all

web-cache show all" sample output:

-----
Cache Name       : cachename
Applied Interfaces : none
HTTP Port        : 80
Bypass list      : none

ACL      Source IP/Mask  Dest. IP/Mask  SrcPort  DstPort  TOS  TOS-MASK  Prot
-----
-----

PI: Ping Check Interval
PA: Ping Check Attempts before server is considered down
AC: Application Checking Admin Status
AI: Application Check Interval
AA: Application Check Attempts before application is considered down

Server List  PI      PA      AC      AI      AA      Max con  IP address(es)
-----
group1       5       4       On      15      4       2000     10.10.10.1, 10.10.10.2
group2       10      4       Off     n/a     n/a     2000     10.10.20.1

Access       Users
-----
Permit       All Users
```

To display web cache information for a specific caching policy:

|                                      |                 |                             |         |         |       |       |
|--------------------------------------|-----------------|-----------------------------|---------|---------|-------|-------|
| xp# web-cache show cache-name cache1 |                 |                             |         |         |       |       |
| Cache Name : cache1 ❶                |                 |                             |         |         |       |       |
| Applied Interfaces : ip1 ❷           |                 |                             |         |         |       |       |
| Bypass list : none ❸                 |                 |                             |         |         |       |       |
| HTTP Port : 80 ❹                     |                 |                             |         |         |       |       |
| ❺                                    | ❻               | ❼                           | ❽       | ❾       | ❿     | ⓫     |
| ACL                                  | Source IP/Mask  | Dest. IP/Mask               | SrcPort | DstPort | TOS   | Port  |
| -----                                | -----           | -----                       | -----   | -----   | ----- | ----- |
| deny207                              | 172.89.1.1/32   | 207.135.0.0/16              | any     | http    | 0     | IP    |
| ❿                                    | ⓬               | ⓭                           |         |         |       |       |
| Server                               | Max con         | IP address                  |         |         |       |       |
| -----                                | -----           | -----                       |         |         |       |       |
| s1                                   | 2000            | 176.89.10.50 - 176.89.10.60 |         |         |       |       |
| Access                               | Users ⓮         |                             |         |         |       |       |
| -----                                | -----           |                             |         |         |       |       |
| Permit                               | All Users       |                             |         |         |       |       |
| Deny                                 | profile deny207 |                             |         |         |       |       |

#### Legend:

1. The name of the cache policy.
2. The outbound interface where the cache policy was applied, typically an interface that connects to the Internet.
3. Destination sites for which HTTP requests are *not* redirected to cache servers and are sent direct.
4. The HTTP port used by a proxy server. A port number other than 80 can be specified with the **web-cache set http-port** command.
5. The names of the profiles (created with an **acl** statement) associated with this cache policy.
6. The source address and filtering mask.
7. The destination address and filtering mask.
8. The source port.
9. The destination port.
10. The TOS value in the packet.
11. The protocol.
12. The server list name.
13. The maximum number of connections that can be handled by each server in the server list.
14. The list or range of IP addresses of the servers in the server list.



15. The hosts (users) whose HTTP requests *are* redirected to the cache servers and the hosts whose HTTP requests are *not* redirected to the cache servers. If no **permit** command is specified, all HTTP requests are redirected to the cache servers.

To display information for a specific web cache servers:

```

xp# web-cache show servers cache cache1
Cache name : cache1 ❶

```

| ❷<br>Block | ❸<br>IP address | ❹<br>Max Conn | ❺<br>Used Cnt | ❻<br>Status |
|------------|-----------------|---------------|---------------|-------------|
| -----      | -----           | -----         | -----         | -----       |
| s1         | 176.89.10.50    | 2000          | 0             | Down        |
| s1         | 176.89.10.51    | 2000          | 0             | Down        |
| s1         | 176.89.10.52    | 2000          | 0             | Down        |
| s1         | 176.89.10.53    | 2000          | 0             | Down        |
| s1         | 176.89.10.54    | 2000          | 0             | Down        |
| s1         | 176.89.10.55    | 2000          | 0             | Down        |
| s1         | 176.89.10.56    | 2000          | 0             | Down        |
| s1         | 176.89.10.57    | 2000          | 0             | Down        |
| s1         | 176.89.10.58    | 2000          | 0             | Down        |
| s1         | 176.89.10.59    | 2000          | 0             | Down        |
| s1         | 176.89.10.60    | 2000          | 0             | Down        |

#### Legend:

1. The name of the cache policy.
2. The server list name.
3. The IP address of a server in the server list.
4. The maximum number of connections that can be handled by the server.
5. The number of connections currently being handled by the server.
6. The current status of the server.

To display information for all configured web cache servers:

```

xp# web-cache show servers cache all
Cache name : cachename

```

| Block  | IP address | Max Conn | Used Cnt | Server | Application |
|--------|------------|----------|----------|--------|-------------|
| -----  | -----      | -----    | -----    | -----  | -----       |
| group1 | 10.10.10.1 | 2000     | 0        | Up     | Up          |
| group1 | 10.10.10.2 | 2000     | 0        | Up     | Down        |
| group2 | 10.10.20.1 | 2000     | 0        | Up     | n/a         |



# Appendix A

## RMON 2 Protocol Directory

This appendix lists the protocol encapsulations that can be managed with the RMON 2 Protocol Directory group on the X-Pedition router. You can specify protocol encapsulations with the **rmon set protocol-directory** or **rmon show protocol-directory** commands. For example, `ether2.ipx` specifies IPX over Ethernet II, while `*ether2.ipx` specifies IPX over any link layer protocol. The protocol object IDs are defined in RFC 2074.

The protocols are listed in the following order:

- [\*Ethernet Applications on page 1468\*](#)
- [\*IP \(version 4\) Applications on page 1469\*](#)
- [\*IPX Applications on page 1472\*](#)
- [\*TCP Applications on page 1473\*](#)
- [\*UDP Applications on page 1480\*](#)

---

| Protocol Encapsulation       | Protocol Identifier (Object ID) |
|------------------------------|---------------------------------|
| <b>Ethernet Applications</b> |                                 |
| ether2.idp                   | 8.0.0.0.1.0.0.6.0.2.0.0         |
| ether2.ip-v4                 | 8.0.0.0.1.0.0.8.0.2.0.0         |
| ether2.chaosnet              | 8.0.0.0.1.0.0.8.4.2.0.0         |
| ether2.arp                   | 8.0.0.0.1.0.0.8.6.2.0.0         |
| ether2.vip                   | 8.0.0.0.1.0.0.11.173.2.0.0      |
| ether2.vloop                 | 8.0.0.0.1.0.0.11.174.2.0.0      |
| ether2.vecho                 | 8.0.0.0.1.0.0.11.175.2.0.0      |
| ether2.netbios-3com          | 8.0.0.0.1.0.0.60.0.2.0.0        |
| ether2.dec                   | 8.0.0.0.1.0.0.96.0.2.0.0        |
| ether2.mop                   | 8.0.0.0.1.0.0.96.1.2.0.0        |
| ether2.mop2                  | 8.0.0.0.1.0.0.96.2.2.0.0        |
| ether2.drp                   | 8.0.0.0.1.0.0.96.3.2.0.0        |
| ether2.lat                   | 8.0.0.0.1.0.0.96.4.2.0.0        |
| ether2.dec-dia               | 8.0.0.0.1.0.0.96.5.2.0.0        |
| ether2.lavc                  | 8.0.0.0.1.0.0.96.7.2.0.0        |
| ether2.rarp                  | 8.0.0.0.1.0.0.128.53.2.0.0      |
| ether2.atalk                 | 8.0.0.0.1.0.0.128.155.2.0.0     |
| ether2.vloop2                | 8.0.0.0.1.0.0.128.196.2.0.0     |
| ether2.vecho2                | 8.0.0.0.1.0.0.128.197.2.0.0     |
| ether2.sna-th                | 8.0.0.0.1.0.0.128.213.2.0.0     |
| ether2.aarp                  | 8.0.0.0.1.0.0.128.243.2.0.0     |
| ether2.ipx                   | 8.0.0.0.1.0.0.129.55.2.0.0      |
| ether2.snmp                  | 8.0.0.0.1.0.0.129.76.2.0.0      |
| ether2.ip-v6                 | 8.0.0.0.1.0.0.134.221.2.0.0     |
| ether2.loopback              | 8.0.0.0.1.0.0.144.0.2.0.0       |
| *ether2.ip-v4                | 8.1.0.0.1.0.0.8.0.2.0.1         |
| *ether2.ipx                  | 8.1.0.0.1.0.0.129.55.2.0.0      |

| Protocol Encapsulation             | Protocol Identifier (Object ID)     |
|------------------------------------|-------------------------------------|
| <b>IP (version 4) Applications</b> |                                     |
| *ether2.ip-v4.icmp                 | 12.1.0.0.1.0.0.8.0.0.0.0.1.3.0.1.0  |
| *ether2.ip-v4.igmp                 | 12.1.0.0.1.0.0.8.0.0.0.0.2.3.0.1.0  |
| *ether2.ip-v4.ggp                  | 12.1.0.0.1.0.0.8.0.0.0.0.3.3.0.1.0  |
| *ether2.ip-v4.ipip4                | 12.1.0.0.1.0.0.8.0.0.0.0.4.3.0.1.0  |
| *ether2.ip-v4.st                   | 12.1.0.0.1.0.0.8.0.0.0.0.5.3.0.1.0  |
| *ether2.ip-v4.tcp                  | 12.1.0.0.1.0.0.8.0.0.0.0.6.3.0.1.0  |
| *ether2.ip-v4.ucl                  | 12.1.0.0.1.0.0.8.0.0.0.0.7.3.0.1.0  |
| *ether2.ip-v4.egp                  | 12.1.0.0.1.0.0.8.0.0.0.0.8.3.0.1.0  |
| *ether2.ip-v4.igp                  | 12.1.0.0.1.0.0.8.0.0.0.0.9.3.0.1.0  |
| *ether2.ip-v4.bbn-rcc-mon          | 12.1.0.0.1.0.0.8.0.0.0.0.10.3.0.1.0 |
| *ether2.ip-v4.nvp2                 | 12.1.0.0.1.0.0.8.0.0.0.0.11.3.0.1.0 |
| *ether2.ip-v4.pup                  | 12.1.0.0.1.0.0.8.0.0.0.0.12.3.0.1.0 |
| *ether2.ip-v4.argus                | 12.1.0.0.1.0.0.8.0.0.0.0.13.3.0.1.0 |
| *ether2.ip-v4.emcon                | 12.1.0.0.1.0.0.8.0.0.0.0.14.3.0.1.0 |
| *ether2.ip-v4.xnet                 | 12.1.0.0.1.0.0.8.0.0.0.0.15.3.0.1.0 |
| *ether2.ip-v4.chaos                | 12.1.0.0.1.0.0.8.0.0.0.0.16.3.0.1.0 |
| *ether2.ip-v4.udp                  | 12.1.0.0.1.0.0.8.0.0.0.0.17.3.0.1.0 |
| *ether2.ip-v4.mux                  | 12.1.0.0.1.0.0.8.0.0.0.0.18.3.0.1.0 |
| *ether2.ip-v4.dcn-meas             | 12.1.0.0.1.0.0.8.0.0.0.0.19.3.0.1.0 |
| *ether2.ip-v4.hmp                  | 12.1.0.0.1.0.0.8.0.0.0.0.20.3.0.1.0 |
| *ether2.ip-v4.prm                  | 12.1.0.0.1.0.0.8.0.0.0.0.21.3.0.1.0 |
| *ether2.ip-v4.xns-idp              | 12.1.0.0.1.0.0.8.0.0.0.0.22.3.0.1.0 |
| *ether2.ip-v4.trunk-1              | 12.1.0.0.1.0.0.8.0.0.0.0.23.3.0.1.0 |
| *ether2.ip-v4.trunk-2              | 12.1.0.0.1.0.0.8.0.0.0.0.24.3.0.1.0 |
| *ether2.ip-v4.leaf-1               | 12.1.0.0.1.0.0.8.0.0.0.0.25.3.0.1.0 |
| *ether2.ip-v4.leaf-2               | 12.1.0.0.1.0.0.8.0.0.0.0.26.3.0.1.0 |
| *ether2.ip-v4.rdp                  | 12.1.0.0.1.0.0.8.0.0.0.0.27.3.0.1.0 |
| *ether2.ip-v4.irtp                 | 12.1.0.0.1.0.0.8.0.0.0.0.28.3.0.1.0 |
| *ether2.ip-v4.iso-tp4              | 12.1.0.0.1.0.0.8.0.0.0.0.29.3.0.1.0 |

---

| Protocol Encapsulation     | Protocol Identifier (Object ID)     |
|----------------------------|-------------------------------------|
| *ether2.ip-v4.netbit       | 12.1.0.0.1.0.0.8.0.0.0.0.30.3.0.1.0 |
| *ether2.ip-v4.mfe-nsp      | 12.1.0.0.1.0.0.8.0.0.0.0.31.3.0.1.0 |
| *ether2.ip-v4.merit-inp    | 12.1.0.0.1.0.0.8.0.0.0.0.32.3.0.1.0 |
| *ether2.ip-v4.sep          | 12.1.0.0.1.0.0.8.0.0.0.0.33.3.0.1.0 |
| *ether2.ip-v4.third-pc     | 12.1.0.0.1.0.0.8.0.0.0.0.34.3.0.1.0 |
| *ether2.ip-v4.idpr         | 12.1.0.0.1.0.0.8.0.0.0.0.35.3.0.1.0 |
| *ether2.ip-v4.xtp          | 12.1.0.0.1.0.0.8.0.0.0.0.36.3.0.1.0 |
| *ether2.ip-v4.ddp          | 12.1.0.0.1.0.0.8.0.0.0.0.37.3.0.1.0 |
| *ether2.ip-v4.idpr-cmtp    | 12.1.0.0.1.0.0.8.0.0.0.0.38.3.0.1.0 |
| *ether2.ip-v4.tp-plus-plus | 12.1.0.0.1.0.0.8.0.0.0.0.39.3.0.1.0 |
| *ether2.ip-v4.il           | 12.1.0.0.1.0.0.8.0.0.0.0.40.3.0.1.0 |
| *ether2.ip-v4.sip          | 12.1.0.0.1.0.0.8.0.0.0.0.41.3.0.1.0 |
| *ether2.ip-v4.sdrp         | 12.1.0.0.1.0.0.8.0.0.0.0.42.3.0.1.0 |
| *ether2.ip-v4.sip-sr       | 12.1.0.0.1.0.0.8.0.0.0.0.43.3.0.1.0 |
| *ether2.ip-v4.sip-frag     | 12.1.0.0.1.0.0.8.0.0.0.0.44.3.0.1.0 |
| *ether2.ip-v4.idrp         | 12.1.0.0.1.0.0.8.0.0.0.0.45.3.0.1.0 |
| *ether2.ip-v4.rsvp         | 12.1.0.0.1.0.0.8.0.0.0.0.46.3.0.1.0 |
| *ether2.ip-v4.gre          | 12.1.0.0.1.0.0.8.0.0.0.0.47.3.0.1.0 |
| *ether2.ip-v4.mhrp         | 12.1.0.0.1.0.0.8.0.0.0.0.48.3.0.1.0 |
| *ether2.ip-v4.bna          | 12.1.0.0.1.0.0.8.0.0.0.0.49.3.0.1.0 |
| *ether2.ip-v4.sipp-esp     | 12.1.0.0.1.0.0.8.0.0.0.0.50.3.0.1.0 |
| *ether2.ip-v4.sipp-ah      | 12.1.0.0.1.0.0.8.0.0.0.0.51.3.0.1.0 |
| *ether2.ip-v4.i-nlsp       | 12.1.0.0.1.0.0.8.0.0.0.0.52.3.0.1.0 |
| *ether2.ip-v4.swipe        | 12.1.0.0.1.0.0.8.0.0.0.0.53.3.0.1.0 |
| *ether2.ip-v4.nhrp         | 12.1.0.0.1.0.0.8.0.0.0.0.54.3.0.1.0 |
| *ether2.ip-v4.priv-host    | 12.1.0.0.1.0.0.8.0.0.0.0.61.3.0.1.0 |
| *ether2.ip-v4.cftp         | 12.1.0.0.1.0.0.8.0.0.0.0.62.3.0.1.0 |
| *ether2.ip-v4.priv-net     | 12.1.0.0.1.0.0.8.0.0.0.0.63.3.0.1.0 |
| *ether2.ip-v4.sat-expak    | 12.1.0.0.1.0.0.8.0.0.0.0.64.3.0.1.0 |
| *ether2.ip-v4.kryptolan    | 12.1.0.0.1.0.0.8.0.0.0.0.65.3.0.1.0 |

---

| Protocol Encapsulation      | Protocol Identifier (Object ID)     |
|-----------------------------|-------------------------------------|
| *ether2.ip-v4.rvd           | 12.1.0.0.1.0.0.8.0.0.0.0.66.3.0.1.0 |
| *ether2.ip-v4.ippc          | 12.1.0.0.1.0.0.8.0.0.0.0.67.3.0.1.0 |
| *ether2.ip-v4.priv-distfile | 12.1.0.0.1.0.0.8.0.0.0.0.68.3.0.1.0 |
| *ether2.ip-v4.sat-mon       | 12.1.0.0.1.0.0.8.0.0.0.0.69.3.0.1.0 |
| *ether2.ip-v4.visa          | 12.1.0.0.1.0.0.8.0.0.0.0.70.3.0.1.0 |
| *ether2.ip-v4.ipcv          | 12.1.0.0.1.0.0.8.0.0.0.0.71.3.0.1.0 |
| *ether2.ip-v4.cpnx          | 12.1.0.0.1.0.0.8.0.0.0.0.72.3.0.1.0 |
| *ether2.ip-v4.cphb          | 12.1.0.0.1.0.0.8.0.0.0.0.73.3.0.1.0 |
| *ether2.ip-v4.wsn           | 12.1.0.0.1.0.0.8.0.0.0.0.74.3.0.1.0 |
| *ether2.ip-v4.pvp           | 12.1.0.0.1.0.0.8.0.0.0.0.75.3.0.1.0 |
| *ether2.ip-v4.br-sat-mon    | 12.1.0.0.1.0.0.8.0.0.0.0.76.3.0.1.0 |
| *ether2.ip-v4.sun-nd        | 12.1.0.0.1.0.0.8.0.0.0.0.77.3.0.1.0 |
| *ether2.ip-v4.wb-mon        | 12.1.0.0.1.0.0.8.0.0.0.0.78.3.0.1.0 |
| *ether2.ip-v4.wb-expak      | 12.1.0.0.1.0.0.8.0.0.0.0.79.3.0.1.0 |
| *ether2.ip-v4.iso-ip        | 12.1.0.0.1.0.0.8.0.0.0.0.80.3.0.1.0 |
| *ether2.ip-v4.vmtip         | 12.1.0.0.1.0.0.8.0.0.0.0.81.3.0.1.0 |
| *ether2.ip-v4.secure-mvtp   | 12.1.0.0.1.0.0.8.0.0.0.0.82.3.0.1.0 |
| *ether2.ip-v4.vines         | 12.1.0.0.1.0.0.8.0.0.0.0.83.3.0.1.0 |
| *ether2.ip-v4.ttp           | 12.1.0.0.1.0.0.8.0.0.0.0.84.3.0.1.0 |
| *ether2.ip-v4.nfsnet-igp    | 12.1.0.0.1.0.0.8.0.0.0.0.85.3.0.1.0 |
| *ether2.ip-v4.dgp           | 12.1.0.0.1.0.0.8.0.0.0.0.86.3.0.1.0 |
| *ether2.ip-v4.tcf           | 12.1.0.0.1.0.0.8.0.0.0.0.87.3.0.1.0 |
| *ether2.ip-v4.igrp          | 12.1.0.0.1.0.0.8.0.0.0.0.88.3.0.1.0 |
| *ether2.ip-v4.ospf          | 12.1.0.0.1.0.0.8.0.0.0.0.89.3.0.1.0 |
| *ether2.ip-v4.sprite-rpc    | 12.1.0.0.1.0.0.8.0.0.0.0.90.3.0.1.0 |
| *ether2.ip-v4.larp          | 12.1.0.0.1.0.0.8.0.0.0.0.91.3.0.1.0 |
| *ether2.ip-v4.mtp           | 12.1.0.0.1.0.0.8.0.0.0.0.92.3.0.1.0 |
| *ether2.ip-v4.ax-25         | 12.1.0.0.1.0.0.8.0.0.0.0.93.3.0.1.0 |
| *ether2.ip-v4.ipip          | 12.1.0.0.1.0.0.8.0.0.0.0.94.3.0.1.0 |
| *ether2.ip-v4.micp          | 12.1.0.0.1.0.0.8.0.0.0.0.95.3.0.1.0 |

| Protocol Encapsulation           | Protocol Identifier (Object ID)                    |
|----------------------------------|--|
| *ether2.ip-v4.scc-sp             | 12.1.0.0.1.0.0.8.0.0.0.0.96.3.0.1.0                |
| *ether2.ip-v4.etherip            | 12.1.0.0.1.0.0.8.0.0.0.0.97.3.0.1.0                |
| *ether2.ip-v4.encap              | 12.1.0.0.1.0.0.8.0.0.0.0.98.3.0.1.0                |
| *ether2.ip-v4.priv-encrypt       | 12.1.0.0.1.0.0.8.0.0.0.0.99.3.0.1.0                |
| *ether2.ip-v4.gmtp               | 12.1.0.0.1.0.0.8.0.0.0.0.100.3.0.1.0               |
| <b>IPX Applications</b>          |  |
| *ether2.ipx.nov-pep              | 12.1.0.0.1.0.0.129.55.0.0.0.0.3.0.0.0              |
| *ether2.ipx.nov-pep.ncp          | 16.1.0.0.1.0.0.129.55.0.0.0.0.0.0.4.81.4.0.0.0.0   |
| *ether2.ipx.nov-pep.nov-sap      | 16.1.0.0.1.0.0.129.55.0.0.0.0.0.0.4.82.4.0.0.0.0   |
| *ether2.ipx.nov-pep.nov-rip      | 16.1.0.0.1.0.0.129.55.0.0.0.0.0.0.4.83.4.0.0.0.0   |
| *ether2.ipx.nov-pep.nov-netbios  | 16.1.0.0.1.0.0.129.55.0.0.0.0.0.0.4.85.4.0.0.0.0   |
| *ether2.ipx.nov-pep.nov-diag     | 16.1.0.0.1.0.0.129.55.0.0.0.0.0.0.4.86.4.0.0.0.0   |
| *ether2.ipx.nov-pep.nov-sec      | 16.1.0.0.1.0.0.129.55.0.0.0.0.0.0.4.87.4.0.0.0.0   |
| *ether2.ipx.nov-pep.smb          | 16.1.0.0.1.0.0.129.55.0.0.0.0.0.0.5.80.4.0.0.0.0   |
| *ether2.ipx.nov-pep.smb2         | 16.1.0.0.1.0.0.129.55.0.0.0.0.0.0.5.82.4.0.0.0.0   |
| *ether2.ipx.nov-pep.burst        | 16.1.0.0.1.0.0.129.55.0.0.0.0.0.0.13.5.4.0.0.0.0   |
| *ether2.ipx.nov-pep.nov-watchdog | 16.1.0.0.1.0.0.129.55.0.0.0.0.0.0.64.4.4.0.0.0.0   |
| *ether2.ipx.nov-pep.nov-bcast    | 16.1.0.0.1.0.0.129.55.0.0.0.0.0.0.64.5.4.0.0.0.0   |
| *ether2.ipx.nov-pep.nlsp         | 16.1.0.0.1.0.0.129.55.0.0.0.0.0.0.144.1.4.0.0.0.0  |
| *ether2.ipx.nov-pep.snmp         | 16.1.0.0.1.0.0.129.55.0.0.0.0.0.0.144.15.4.0.0.0.0 |
| *ether2.ipx.nov-pep.snmptrap     | 16.1.0.0.1.0.0.129.55.0.0.0.0.0.0.144.16.4.0.0.0.0 |
| *ether2.ipx.nov-rip              | 12.1.0.0.1.0.0.129.55.0.0.0.1.3.0.0.0              |
| *ether2.ipx.nov-echo             | 12.1.0.0.1.0.0.129.55.0.0.0.2.3.0.0.0              |
| *ether2.ipx.nov-error            | 12.1.0.0.1.0.0.129.55.0.0.0.3.3.0.0.0              |
| *ether2.ipx.nov-pep2             | 12.1.0.0.1.0.0.129.55.0.0.0.4.3.0.0.0              |
| *ether2.ipx.nov-spx              | 12.1.0.0.1.0.0.129.55.0.0.0.5.3.0.0.0              |
| *ether2.ipx.nov-pep3             | 12.1.0.0.1.0.0.129.55.0.0.0.17.3.0.0.0             |
| *ether2.ipx.nov-netbios          | 12.1.0.0.1.0.0.129.55.0.0.0.20.3.0.0.0             |



| Protocol Encapsulation             | Protocol Identifier (Object ID)               |
|------------------------------------|---|
| <b>TCP Applications</b>            |   |
| *ether2.ip-v4.tcp.tcpmux           | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.1.4.0.1.0.0  |
| *ether2.ip-v4.tcp.compressnet-mgmt | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.2.4.0.1.0.0  |
| *ether2.ip-v4.tcp.compressnet      | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.3.4.0.1.0.0  |
| *ether2.ip-v4.tcp.rje              | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.5.4.0.1.0.0  |
| *ether2.ip-v4.tcp.echo             | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.7.4.0.1.0.0  |
| *ether2.ip-v4.tcp.discard          | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.9.4.0.1.0.0  |
| *ether2.ip-v4.tcp.systat           | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.11.4.0.1.0.0 |
| *ether2.ip-v4.tcp.daytime          | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.13.4.0.1.0.0 |
| *ether2.ip-v4.tcp.qotd             | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.17.4.0.1.0.0 |
| *ether2.ip-v4.tcp.msp              | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.18.4.0.1.0.0 |
| *ether2.ip-v4.tcp.chargen          | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.19.4.0.1.0.0 |
| *ether2.ip-v4.tcp.ftp-data         | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.20.4.0.1.0.0 |
| *ether2.ip-v4.tcp.ftp              | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.21.4.0.1.0.0 |
| *ether2.ip-v4.tcp.telnet           | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.23.4.0.1.0.0 |
| *ether2.ip-v4.tcp.priv-mail        | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.24.4.0.1.0.0 |
| *ether2.ip-v4.tcp.smtp             | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.25.4.0.1.0.0 |
| *ether2.ip-v4.tcp.nsw-fe           | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.27.4.0.1.0.0 |
| *ether2.ip-v4.tcp.msg-icp          | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.29.4.0.1.0.0 |
| *ether2.ip-v4.tcp.msg-auth         | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.31.4.0.1.0.0 |
| *ether2.ip-v4.tcp.dsp              | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.33.4.0.1.0.0 |
| *ether2.ip-v4.tcp.priv-print       | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.35.4.0.1.0.0 |
| *ether2.ip-v4.tcp.time             | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.37.4.0.1.0.0 |
| *ether2.ip-v4.tcp.rap              | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.38.4.0.1.0.0 |
| *ether2.ip-v4.tcp.graphics         | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.41.4.0.1.0.0 |
| *ether2.ip-v4.tcp.nicname          | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.43.4.0.1.0.0 |
| *ether2.ip-v4.tcp.mpm-flags        | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.44.4.0.1.0.0 |
| *ether2.ip-v4.tcp.mpm              | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.45.4.0.1.0.0 |
| *ether2.ip-v4.tcp.mpm-send         | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.46.4.0.1.0.0 |
| *ether2.ip-v4.tcp.ni-ftp           | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.47.4.0.1.0.0 |

---

| Protocol Encapsulation         | Protocol Identifier (Object ID)               |
|--------------------------------|---|
| *ether2.ip-v4.tcp.auditd       | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.48.4.0.1.0.0 |
| *ether2.ip-v4.tcp.tacacs       | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.49.4.0.1.0.0 |
| *ether2.ip-v4.tcp.xns-time     | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.52.4.0.1.0.0 |
| *ether2.ip-v4.tcp.domain       | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.53.4.0.1.0.0 |
| *ether2.ip-v4.tcp.xns-ch       | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.54.4.0.1.0.0 |
| *ether2.ip-v4.tcp.isi-gl       | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.55.4.0.1.0.0 |
| *ether2.ip-v4.tcp.xns-auth     | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.56.4.0.1.0.0 |
| *ether2.ip-v4.tcp.priv-term    | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.57.4.0.1.0.0 |
| *ether2.ip-v4.tcp.xns-mail     | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.58.4.0.1.0.0 |
| *ether2.ip-v4.tcp.priv-file    | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.59.4.0.1.0.0 |
| *ether2.ip-v4.tcp.ni-mail      | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.61.4.0.1.0.0 |
| *ether2.ip-v4.tcp.acas         | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.62.4.0.1.0.0 |
| *ether2.ip-v4.tcp.covia        | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.64.4.0.1.0.0 |
| *ether2.ip-v4.tcp.tacacs-ds    | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.65.4.0.1.0.0 |
| *ether2.ip-v4.tcp.sql*net      | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.66.4.0.1.0.0 |
| *ether2.ip-v4.tcp.gopher       | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.70.4.0.1.0.0 |
| *ether2.ip-v4.tcp.netrjs-1     | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.71.4.0.1.0.0 |
| *ether2.ip-v4.tcp.netrjs-2     | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.72.4.0.1.0.0 |
| *ether2.ip-v4.tcp.netrjs-3     | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.73.4.0.1.0.0 |
| *ether2.ip-v4.tcp.netrjs-4     | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.74.4.0.1.0.0 |
| *ether2.ip-v4.tcp.priv-dialout | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.75.4.0.1.0.0 |
| *ether2.ip-v4.tcp.deos         | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.76.4.0.1.0.0 |
| *ether2.ip-v4.tcp.priv-rje     | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.77.4.0.1.0.0 |
| *ether2.ip-v4.tcp.vettcp       | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.78.4.0.1.0.0 |
| *ether2.ip-v4.tcp.finger       | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.79.4.0.1.0.0 |
| *ether2.ip-v4.tcp.www-http     | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.80.4.0.1.0.0 |
| *ether2.ip-v4.tcp.hosts2-ns    | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.81.4.0.1.0.0 |
| *ether2.ip-v4.tcp.xfer         | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.82.4.0.1.0.0 |
| *ether2.ip-v4.tcp.mit-ml-dev   | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.83.4.0.1.0.0 |
| *ether2.ip-v4.tcp.ctf          | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.84.4.0.1.0.0 |

---

| Protocol Encapsulation          | Protocol Identifier (Object ID)                |
|---------------------------------|--|
| *ether2.ip-v4.tcp.mit-ml-dev    | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.85.4.0.1.0.0  |
| *ether2.ip-v4.tcp.mfcobol       | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.86.4.0.1.0.0  |
| *ether2.ip-v4.tcp.priv-termlink | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.87.4.0.1.0.0  |
| *ether2.ip-v4.tcp.kerberos      | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.88.4.0.1.0.0  |
| *ether2.ip-v4.tcp.su-mit-tg     | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.89.4.0.1.0.0  |
| *ether2.ip-v4.tcp.dnsix         | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.90.4.0.1.0.0  |
| *ether2.ip-v4.tcp.mit-dov       | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.91.4.0.1.0.0  |
| *ether2.ip-v4.tcp.npp           | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.92.4.0.1.0.0  |
| *ether2.ip-v4.tcp.dcp           | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.93.4.0.1.0.0  |
| *ether2.ip-v4.tcp.objcall       | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.94.4.0.1.0.0  |
| *ether2.ip-v4.tcp.supdup        | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.95.4.0.1.0.0  |
| *ether2.ip-v4.tcp.dixie         | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.96.4.0.1.0.0  |
| *ether2.ip-v4.tcp.swift-rvf     | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.97.4.0.1.0.0  |
| *ether2.ip-v4.tcp.tacnews       | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.98.4.0.1.0.0  |
| *ether2.ip-v4.tcp.metagram      | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.99.4.0.1.0.0  |
| *ether2.ip-v4.tcp.newacct       | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.100.4.0.1.0.0 |
| *ether2.ip-v4.tcp.hostname      | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.101.4.0.1.0.0 |
| *ether2.ip-v4.tcp.iso-tsap      | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.102.4.0.1.0.0 |
| *ether2.ip-v4.tcp.gppitnp       | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.103.4.0.1.0.0 |
| *ether2.ip-v4.tcp.acr-nema      | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.104.4.0.1.0.0 |
| *ether2.ip-v4.tcp.csnet-ns      | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.105.4.0.1.0.0 |
| *ether2.ip-v4.tcp.3com-tsmux    | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.106.4.0.1.0.0 |
| *ether2.ip-v4.tcp.rtelnet       | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.107.4.0.1.0.0 |
| *ether2.ip-v4.tcp.snagas        | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.108.4.0.1.0.0 |
| *ether2.ip-v4.tcp.pop2          | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.109.4.0.1.0.0 |
| *ether2.ip-v4.tcp.pop3          | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.110.4.0.1.0.0 |
| *ether2.ip-v4.tcp.sunrpc        | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.111.4.0.1.0.0 |
| *ether2.ip-v4.tcp.mcidas        | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.112.4.0.1.0.0 |
| *ether2.ip-v4.tcp.auth          | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.113.4.0.1.0.0 |
| *ether2.ip-v4.tcp.audionews     | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.114.4.0.1.0.0 |

---

| Protocol Encapsulation        | Protocol Identifier (Object ID)                |
|-------------------------------|--|
| *ether2.ip-v4.tcp.sftp        | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.115.4.0.1.0.0 |
| *ether2.ip-v4.tcp.ansanotify  | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.116.4.0.1.0.0 |
| *ether2.ip-v4.tcp.uucp-path   | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.117.4.0.1.0.0 |
| *ether2.ip-v4.tcp.sqlserv     | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.118.4.0.1.0.0 |
| *ether2.ip-v4.tcp.nntp        | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.119.4.0.1.0.0 |
| *ether2.ip-v4.tcp.erpc        | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.121.4.0.1.0.0 |
| *ether2.ip-v4.tcp.smakynet    | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.122.4.0.1.0.0 |
| *ether2.ip-v4.tcp.ansatrader  | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.124.4.0.1.0.0 |
| *ether2.ip-v4.tcp.locus-map   | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.125.4.0.1.0.0 |
| *ether2.ip-v4.tcp.unitary     | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.126.4.0.1.0.0 |
| *ether2.ip-v4.tcp.locus-con   | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.127.4.0.1.0.0 |
| *ether2.ip-v4.tcp.gss-xlicen  | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.128.4.0.1.0.0 |
| *ether2.ip-v4.tcp.pwdgen      | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.129.4.0.1.0.0 |
| *ether2.ip-v4.tcp.cisco-fna   | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.130.4.0.1.0.0 |
| *ether2.ip-v4.tcp.cisco-tna   | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.131.4.0.1.0.0 |
| *ether2.ip-v4.tcp.cisco-sys   | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.132.4.0.1.0.0 |
| *ether2.ip-v4.tcp.statsrv     | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.133.4.0.1.0.0 |
| *ether2.ip-v4.tcp.ingres-net  | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.134.4.0.1.0.0 |
| *ether2.ip-v4.tcp.loc-srv     | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.135.4.0.1.0.0 |
| *ether2.ip-v4.tcp.profile     | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.136.4.0.1.0.0 |
| *ether2.ip-v4.tcp.netbios-ns  | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.137.4.0.1.0.0 |
| *ether2.ip-v4.tcp.netbios-dgm | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.138.4.0.1.0.0 |
| *ether2.ip-v4.tcp.netbios-ssn | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.139.4.0.1.0.0 |
| *ether2.ip-v4.tcp.emfis-data  | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.140.4.0.1.0.0 |
| *ether2.ip-v4.tcp.emfis-cntl  | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.141.4.0.1.0.0 |
| *ether2.ip-v4.tcp.bl-idm      | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.142.4.0.1.0.0 |
| *ether2.ip-v4.tcp.imap2       | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.143.4.0.1.0.0 |
| *ether2.ip-v4.tcp.news        | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.144.4.0.1.0.0 |
| *ether2.ip-v4.tcp.uaac        | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.145.4.0.1.0.0 |
| *ether2.ip-v4.tcp.iso-tp0     | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.146.4.0.1.0.0 |

| Protocol Encapsulation        | Protocol Identifier (Object ID)                |
|-------------------------------|--|
| *ether2.ip-v4.tcp.iso-ip      | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.147.4.0.1.0.0 |
| *ether2.ip-v4.tcp.cronus      | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.148.4.0.1.0.0 |
| *ether2.ip-v4.tcp.aed-512     | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.149.4.0.1.0.0 |
| *ether2.ip-v4.tcp.sql-net     | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.150.4.0.1.0.0 |
| *ether2.ip-v4.tcp.hems        | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.151.4.0.1.0.0 |
| *ether2.ip-v4.tcp.bftp        | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.152.4.0.1.0.0 |
| *ether2.ip-v4.tcp.netsc-prod  | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.154.4.0.1.0.0 |
| *ether2.ip-v4.tcp.netsc-dev   | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.155.4.0.1.0.0 |
| *ether2.ip-v4.tcp.sqlsrv      | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.156.4.0.1.0.0 |
| *ether2.ip-v4.tcp.knet-cmp    | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.157.4.0.1.0.0 |
| *ether2.ip-v4.tcp.pcmail-srv  | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.158.4.0.1.0.0 |
| *ether2.ip-v4.tcp.nss-routing | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.159.4.0.1.0.0 |
| *ether2.ip-v4.tcp.snmp        | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.161.4.0.1.0.0 |
| *ether2.ip-v4.tcp.snmptrap    | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.162.4.0.1.0.0 |
| *ether2.ip-v4.tcp.cmip-man    | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.163.4.0.1.0.0 |
| *ether2.ip-v4.tcp.cmip-agent  | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.164.4.0.1.0.0 |
| *ether2.ip-v4.tcp.xns-courier | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.165.4.0.1.0.0 |
| *ether2.ip-v4.tcp.s-net       | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.166.4.0.1.0.0 |
| *ether2.ip-v4.tcp.namp        | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.167.4.0.1.0.0 |
| *ether2.ip-v4.tcp.rsvd        | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.168.4.0.1.0.0 |
| *ether2.ip-v4.tcp.send        | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.169.4.0.1.0.0 |
| *ether2.ip-v4.tcp.print-srv   | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.170.4.0.1.0.0 |
| *ether2.ip-v4.tcp.multiplex   | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.171.4.0.1.0.0 |
| *ether2.ip-v4.tcp.cl-1        | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.172.4.0.1.0.0 |
| *ether2.ip-v4.tcp.xyplex-mux  | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.173.4.0.1.0.0 |
| *ether2.ip-v4.tcp.mailq       | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.174.4.0.1.0.0 |
| *ether2.ip-v4.tcp.vynet       | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.175.4.0.1.0.0 |
| *ether2.ip-v4.tcp.genrad-mux  | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.176.4.0.1.0.0 |
| *ether2.ip-v4.tcp.nextstep    | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.178.4.0.1.0.0 |
| *ether2.ip-v4.tcp.bgp         | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.179.4.0.1.0.0 |

---

| Protocol Encapsulation        | Protocol Identifier (Object ID)                |
|-------------------------------|--|
| *ether2.ip-v4.tcp.ris         | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.180.4.0.1.0.0 |
| *ether2.ip-v4.tcp.unify       | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.181.4.0.1.0.0 |
| *ether2.ip-v4.tcp.audit       | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.182.4.0.1.0.0 |
| *ether2.ip-v4.tcp.ocbinder    | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.183.4.0.1.0.0 |
| *ether2.ip-v4.tcp.ocserver    | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.184.4.0.1.0.0 |
| *ether2.ip-v4.tcp.remote-kis  | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.185.4.0.1.0.0 |
| *ether2.ip-v4.tcp.kis         | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.186.4.0.1.0.0 |
| *ether2.ip-v4.tcp.aci         | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.187.4.0.1.0.0 |
| *ether2.ip-v4.tcp.mumps       | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.188.4.0.1.0.0 |
| *ether2.ip-v4.tcp.qft         | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.189.4.0.1.0.0 |
| *ether2.ip-v4.tcp.gacp        | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.190.4.0.1.0.0 |
| *ether2.ip-v4.tcp.prospiero   | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.191.4.0.1.0.0 |
| *ether2.ip-v4.tcp.osu-nms     | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.192.4.0.1.0.0 |
| *ether2.ip-v4.tcp.srmp        | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.193.4.0.1.0.0 |
| *ether2.ip-v4.tcp.irc         | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.194.4.0.1.0.0 |
| *ether2.ip-v4.tcp.dn6-nlm-aud | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.195.4.0.1.0.0 |
| *ether2.ip-v4.tcp.dn6-smm-red | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.196.4.0.1.0.0 |
| *ether2.ip-v4.tcp.dls         | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.197.4.0.1.0.0 |
| *ether2.ip-v4.tcp.dls-mon     | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.198.4.0.1.0.0 |
| *ether2.ip-v4.tcp.smux        | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.199.4.0.1.0.0 |
| *ether2.ip-v4.tcp.src         | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.200.4.0.1.0.0 |
| *ether2.ip-v4.tcp.at-rtmp     | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.201.4.0.1.0.0 |
| *ether2.ip-v4.tcp.at-nbp      | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.202.4.0.1.0.0 |
| *ether2.ip-v4.tcp.at-3        | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.203.4.0.1.0.0 |
| *ether2.ip-v4.tcp.at-echo     | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.204.4.0.1.0.0 |
| *ether2.ip-v4.tcp.at-5        | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.205.4.0.1.0.0 |
| *ether2.ip-v4.tcp.at-zis      | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.206.4.0.1.0.0 |
| *ether2.ip-v4.tcp.at-7        | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.207.4.0.1.0.0 |
| *ether2.ip-v4.tcp.at-8        | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.208.4.0.1.0.0 |
| *ether2.ip-v4.tcp.tam         | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.209.4.0.1.0.0 |

---

| Protocol Encapsulation           | Protocol Identifier (Object ID)                |
|----------------------------------|--|
| *ether2.ip-v4.tcp.z39-50         | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.210.4.0.1.0.0 |
| *ether2.ip-v4.tcp.914c-g         | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.211.4.0.1.0.0 |
| *ether2.ip-v4.tcp.anet           | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.212.4.0.1.0.0 |
| *ether2.ip-v4.tcp.vmpwscs        | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.214.4.0.1.0.0 |
| *ether2.ip-v4.tcp.softpc         | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.215.4.0.1.0.0 |
| *ether2.ip-v4.tcp.atls           | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.216.4.0.1.0.0 |
| *ether2.ip-v4.tcp.dbase          | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.217.4.0.1.0.0 |
| *ether2.ip-v4.tcp.mpp            | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.218.4.0.1.0.0 |
| *ether2.ip-v4.tcp.uarps          | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.219.4.0.1.0.0 |
| *ether2.ip-v4.tcp.imap3          | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.220.4.0.1.0.0 |
| *ether2.ip-v4.tcp.fln-spx        | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.221.4.0.1.0.0 |
| *ether2.ip-v4.tcp.rsh-spx        | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.222.4.0.1.0.0 |
| *ether2.ip-v4.tcp.cdc            | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.223.4.0.1.0.0 |
| *ether2.ip-v4.tcp.sur-meas       | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.243.4.0.1.0.0 |
| *ether2.ip-v4.tcp.link           | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.245.4.0.1.0.0 |
| *ether2.ip-v4.tcp.dsp3270        | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.0.246.4.0.1.0.0 |
| *ether2.ip-v4.tcp.ldap           | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.1.133.4.0.1.0.0 |
| *ether2.ip-v4.tcp.https          | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.1.187.4.0.1.0.0 |
| *ether2.ip-v4.tcp.exec           | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.2.0.4.0.1.0.0   |
| *ether2.ip-v4.tcp.login          | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.2.1.4.0.1.0.0   |
| *ether2.ip-v4.tcp.cmd            | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.2.2.4.0.1.0.0   |
| *ether2.ip-v4.tcp.printer        | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.2.3.4.0.1.0.0   |
| *ether2.ip-v4.tcp.uucp           | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.2.28.4.0.1.0.0  |
| *ether2.ip-v4.tcp.banyan-vip     | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.2.61.4.0.1.0.0  |
| *ether2.ip-v4.tcp.doom           | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.2.154.4.0.1.0.0 |
| *ether2.ip-v4.tcp.notes          | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.5.72.4.0.1.0.0  |
| *ether2.ip-v4.tcp.orac1-srv      | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.5.245.4.0.1.0.0 |
| *ether2.ip-v4.tcp.orac1-tns      | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.5.246.4.0.1.0.0 |
| *ether2.ip-v4.tcp.orac1-tns-srv  | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.5.247.4.0.1.0.0 |
| *ether2.ip-v4.tcp.orac1-coauthor | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.5.249.4.0.1.0.0 |

| Protocol Encapsulation         | Protocol Identifier (Object ID)                  |
|--------------------------------|--|
| *ether2.ip-v4.tcp.oracle-remdb | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.6.35.4.0.1.0.0    |
| *ether2.ip-v4.tcp.oracle-names | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.6.39.4.0.1.0.0    |
| *ether2.ip-v4.tcp.oracle-em1   | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.6.212.4.0.1.0.0   |
| *ether2.ip-v4.tcp.oracle-em2   | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.6.218.4.0.1.0.0   |
| *ether2.ip-v4.tcp.ms-streaming | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.6.219.4.0.1.0.0   |
| *ether2.ip-v4.tcp.oracle-vp2   | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.7.16.4.0.1.0.0    |
| *ether2.ip-v4.tcp.oracle-vp1   | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.7.17.4.0.1.0.0    |
| *ether2.ip-v4.tcp.ccmail       | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.12.192.4.0.1.0.0  |
| *ether2.ip-v4.tcp.xwin         | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.23.112.4.0.1.0.0  |
| *ether2.ip-v4.tcp.quake        | 16.1.0.0.1.0.0.8.0.0.0.0.6.0.0.101.144.4.0.1.0.0 |
| <b>UDP Applications</b>        |  |
| *ether2.ip-v4.udp.echo         | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.7.4.0.1.0.0    |
| *ether2.ip-v4.udp.discard      | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.9.4.0.1.0.0    |
| *ether2.ip-v4.udp.systat       | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.11.4.0.1.0.0   |
| *ether2.ip-v4.udp.daytime      | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.13.4.0.1.0.0   |
| *ether2.ip-v4.udp.qotd         | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.17.4.0.1.0.0   |
| *ether2.ip-v4.udp.msp          | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.18.4.0.1.0.0   |
| *ether2.ip-v4.udp.chargen      | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.19.4.0.1.0.0   |
| *ether2.ip-v4.udp.priv-mail    | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.24.4.0.1.0.0   |
| *ether2.ip-v4.udp.nsw-fe       | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.27.4.0.1.0.0   |
| *ether2.ip-v4.udp.msg-icp      | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.29.4.0.1.0.0   |
| *ether2.ip-v4.udp.msg-auth     | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.31.4.0.1.0.0   |
| *ether2.ip-v4.udp.dsp          | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.33.4.0.1.0.0   |
| *ether2.ip-v4.udp.priv-print   | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.35.4.0.1.0.0   |
| *ether2.ip-v4.udp.time         | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.37.4.0.1.0.0   |
| *ether2.ip-v4.udp.rlp          | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.39.4.0.1.0.0   |
| *ether2.ip-v4.udp.graphics     | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.41.4.0.1.0.0   |
| *ether2.ip-v4.udp.nameserver   | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.42.4.0.1.0.0   |
| *ether2.ip-v4.udp.auditd       | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.48.4.0.1.0.0   |
| *ether2.ip-v4.udp.re-mail-ck   | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.50.4.0.1.0.0   |



---

| Protocol Encapsulation         | Protocol Identifier (Object ID)                 |
|--------------------------------|---|
| *ether2.ip-v4.udp.la-maint     | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.51.4.0.1.0.0  |
| *ether2.ip-v4.udp.xns-time     | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.52.4.0.1.0.0  |
| *ether2.ip-v4.udp.domain       | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.53.4.0.1.0.0  |
| *ether2.ip-v4.udp.xns-ch       | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.54.4.0.1.0.0  |
| *ether2.ip-v4.udp.isi-gl       | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.55.4.0.1.0.0  |
| *ether2.ip-v4.udp.xns-auth     | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.56.4.0.1.0.0  |
| *ether2.ip-v4.udp.priv-term    | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.57.4.0.1.0.0  |
| *ether2.ip-v4.udp.xns-mail     | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.58.4.0.1.0.0  |
| *ether2.ip-v4.udp.priv-file    | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.59.4.0.1.0.0  |
| *ether2.ip-v4.udp.ni-mail      | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.61.4.0.1.0.0  |
| *ether2.ip-v4.udp.bootps       | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.67.4.0.1.0.0  |
| *ether2.ip-v4.udp.bootpc       | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.68.4.0.1.0.0  |
| *ether2.ip-v4.udp.tftp         | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.69.4.0.1.0.0  |
| *ether2.ip-v4.udp.priv-dialout | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.75.4.0.1.0.0  |
| *ether2.ip-v4.udp.deos         | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.76.4.0.1.0.0  |
| *ether2.ip-v4.udp.priv-rje     | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.77.4.0.1.0.0  |
| *ether2.ip-v4.udp.vettpc       | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.78.4.0.1.0.0  |
| *ether2.ip-v4.udp.hosts2-ns    | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.81.4.0.1.0.0  |
| *ether2.ip-v4.udp.xfer         | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.82.4.0.1.0.0  |
| *ether2.ip-v4.udp.mit-ml-dev   | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.83.4.0.1.0.0  |
| *ether2.ip-v4.udp.ctf          | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.84.4.0.1.0.0  |
| *ether2.ip-v4.udp.mit-ml-dev   | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.85.4.0.1.0.0  |
| *ether2.ip-v4.udp.kerberos     | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.88.4.0.1.0.0  |
| *ether2.ip-v4.udp.npp          | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.92.4.0.1.0.0  |
| *ether2.ip-v4.udp.dcp          | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.93.4.0.1.0.0  |
| *ether2.ip-v4.udp.dixie        | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.96.4.0.1.0.0  |
| *ether2.ip-v4.udp.swift-rvf    | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.97.4.0.1.0.0  |
| *ether2.ip-v4.udp.tacnews      | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.98.4.0.1.0.0  |
| *ether2.ip-v4.udp.metagram     | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.99.4.0.1.0.0  |
| *ether2.ip-v4.udp.iso-tsap     | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.102.4.0.1.0.0 |

---

| Protocol Encapsulation        | Protocol Identifier (Object ID)                 |
|-------------------------------|---|
| *ether2.ip-v4.udp.gppitnp     | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.103.4.0.1.0.0 |
| *ether2.ip-v4.udp.csnet-ns    | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.105.4.0.1.0.0 |
| *ether2.ip-v4.udp.3com-tsmux  | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.106.4.0.1.0.0 |
| *ether2.ip-v4.udp.pop3        | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.110.4.0.1.0.0 |
| *ether2.ip-v4.udp.sunrpc      | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.111.4.0.1.0.0 |
| *ether2.ip-v4.udp.audionews   | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.114.4.0.1.0.0 |
| *ether2.ip-v4.udp.ansanotify  | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.116.4.0.1.0.0 |
| *ether2.ip-v4.udp.sqlserv     | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.118.4.0.1.0.0 |
| *ether2.ip-v4.udp.cfdpkt      | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.120.4.0.1.0.0 |
| *ether2.ip-v4.udp.erpc        | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.121.4.0.1.0.0 |
| *ether2.ip-v4.udp.smakynet    | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.122.4.0.1.0.0 |
| *ether2.ip-v4.udp.ntp         | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.123.4.0.1.0.0 |
| *ether2.ip-v4.udp.ansatrader  | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.124.4.0.1.0.0 |
| *ether2.ip-v4.udp.unitary     | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.126.4.0.1.0.0 |
| *ether2.ip-v4.udp.gss-xlicen  | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.128.4.0.1.0.0 |
| *ether2.ip-v4.udp.pwdgen      | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.129.4.0.1.0.0 |
| *ether2.ip-v4.udp.cisco-fna   | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.130.4.0.1.0.0 |
| *ether2.ip-v4.udp.cisco-tna   | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.131.4.0.1.0.0 |
| *ether2.ip-v4.udp.cisco-sys   | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.132.4.0.1.0.0 |
| *ether2.ip-v4.udp.statsrv     | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.133.4.0.1.0.0 |
| *ether2.ip-v4.udp.loc-srv     | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.135.4.0.1.0.0 |
| *ether2.ip-v4.udp.netbios-ns  | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.137.4.0.1.0.0 |
| *ether2.ip-v4.udp.netbios-dgm | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.138.4.0.1.0.0 |
| *ether2.ip-v4.udp.netbios-ssn | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.139.4.0.1.0.0 |
| *ether2.ip-v4.udp.emfis-data  | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.140.4.0.1.0.0 |
| *ether2.ip-v4.udp.emfis-cntl  | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.141.4.0.1.0.0 |
| *ether2.ip-v4.udp.bl-idm      | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.142.4.0.1.0.0 |
| *ether2.ip-v4.udp.news        | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.144.4.0.1.0.0 |
| *ether2.ip-v4.udp.uaac        | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.145.4.0.1.0.0 |
| *ether2.ip-v4.udp.iso-tp0     | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.146.4.0.1.0.0 |

---

| Protocol Encapsulation        | Protocol Identifier (Object ID)                 |
|-------------------------------|---|
| *ether2.ip-v4.udp.iso-ip      | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.147.4.0.1.0.0 |
| *ether2.ip-v4.udp.cronus      | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.148.4.0.1.0.0 |
| *ether2.ip-v4.udp.aed-512     | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.149.4.0.1.0.0 |
| *ether2.ip-v4.udp.sql-net     | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.150.4.0.1.0.0 |
| *ether2.ip-v4.udp.sgmp        | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.153.4.0.1.0.0 |
| *ether2.ip-v4.udp.netsc-prod  | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.154.4.0.1.0.0 |
| *ether2.ip-v4.udp.netsc-dev   | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.155.4.0.1.0.0 |
| *ether2.ip-v4.udp.nss-routing | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.159.4.0.1.0.0 |
| *ether2.ip-v4.udp.sgmp-traps  | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.160.4.0.1.0.0 |
| *ether2.ip-v4.udp.snmp        | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.161.4.0.1.0.0 |
| *ether2.ip-v4.udp.snmptrap    | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.162.4.0.1.0.0 |
| *ether2.ip-v4.udp.cmip-man    | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.163.4.0.1.0.0 |
| *ether2.ip-v4.udp.cmip-agent  | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.164.4.0.1.0.0 |
| *ether2.ip-v4.udp.xns-courier | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.165.4.0.1.0.0 |
| *ether2.ip-v4.udp.s-net       | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.166.4.0.1.0.0 |
| *ether2.ip-v4.udp.namp        | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.167.4.0.1.0.0 |
| *ether2.ip-v4.udp.rsvd        | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.168.4.0.1.0.0 |
| *ether2.ip-v4.udp.send        | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.169.4.0.1.0.0 |
| *ether2.ip-v4.udp.print-srv   | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.170.4.0.1.0.0 |
| *ether2.ip-v4.udp.multiplex   | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.171.4.0.1.0.0 |
| *ether2.ip-v4.udp.cl-1        | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.172.4.0.1.0.0 |
| *ether2.ip-v4.udp.xyplex-mux  | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.173.4.0.1.0.0 |
| *ether2.ip-v4.udp.mailq       | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.174.4.0.1.0.0 |
| *ether2.ip-v4.udp.vmnet       | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.175.4.0.1.0.0 |
| *ether2.ip-v4.udp.genrad-mux  | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.176.4.0.1.0.0 |
| *ether2.ip-v4.udp.xdmcp       | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.177.4.0.1.0.0 |
| *ether2.ip-v4.udp.nextstep    | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.178.4.0.1.0.0 |
| *ether2.ip-v4.udp.ris         | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.180.4.0.1.0.0 |
| *ether2.ip-v4.udp.unify       | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.181.4.0.1.0.0 |
| *ether2.ip-v4.udp.audit       | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.182.4.0.1.0.0 |

---

| Protocol Encapsulation       | Protocol Identifier (Object ID)                 |
|------------------------------|---|
| *ether2.ip-v4.udp.ocbinder   | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.183.4.0.1.0.0 |
| *ether2.ip-v4.udp.ocserver   | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.184.4.0.1.0.0 |
| *ether2.ip-v4.udp.remote-kis | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.185.4.0.1.0.0 |
| *ether2.ip-v4.udp.kis        | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.186.4.0.1.0.0 |
| *ether2.ip-v4.udp.aci        | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.187.4.0.1.0.0 |
| *ether2.ip-v4.udp.mumps      | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.188.4.0.1.0.0 |
| *ether2.ip-v4.udp.osu-nms    | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.192.4.0.1.0.0 |
| *ether2.ip-v4.udp.srmp       | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.193.4.0.1.0.0 |
| *ether2.ip-v4.udp.irc        | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.194.4.0.1.0.0 |
| *ether2.ip-v4.udp.dls        | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.197.4.0.1.0.0 |
| *ether2.ip-v4.udp.dls-mon    | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.198.4.0.1.0.0 |
| *ether2.ip-v4.udp.src        | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.200.4.0.1.0.0 |
| *ether2.ip-v4.udp.at-rtmp    | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.201.4.0.1.0.0 |
| *ether2.ip-v4.udp.at-nbp     | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.202.4.0.1.0.0 |
| *ether2.ip-v4.udp.at-3       | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.203.4.0.1.0.0 |
| *ether2.ip-v4.udp.at-echo    | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.204.4.0.1.0.0 |
| *ether2.ip-v4.udp.at-5       | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.205.4.0.1.0.0 |
| *ether2.ip-v4.udp.at-zis     | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.206.4.0.1.0.0 |
| *ether2.ip-v4.udp.at-7       | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.207.4.0.1.0.0 |
| *ether2.ip-v4.udp.at-8       | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.208.4.0.1.0.0 |
| *ether2.ip-v4.udp.tam        | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.209.4.0.1.0.0 |
| *ether2.ip-v4.udp.914c-g     | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.211.4.0.1.0.0 |
| *ether2.ip-v4.udp.anet       | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.212.4.0.1.0.0 |
| *ether2.ip-v4.udp.ipx-tunnel | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.213.4.0.1.0.0 |
| *ether2.ip-v4.udp.vmpwscs    | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.214.4.0.1.0.0 |
| *ether2.ip-v4.udp.softpc     | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.215.4.0.1.0.0 |
| *ether2.ip-v4.udp.atls       | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.216.4.0.1.0.0 |
| *ether2.ip-v4.udp.dbase      | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.217.4.0.1.0.0 |
| *ether2.ip-v4.udp.uarps      | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.219.4.0.1.0.0 |
| *ether2.ip-v4.udp.fln-spx    | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.221.4.0.1.0.0 |

---

| Protocol Encapsulation       | Protocol Identifier (Object ID)                   |
|------------------------------|---|
| *ether2.ip-v4.udp.rsh-spx    | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.222.4.0.1.0.0   |
| *ether2.ip-v4.udp.cdc        | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.223.4.0.1.0.0   |
| *ether2.ip-v4.udp.sur-meas   | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.243.4.0.1.0.0   |
| *ether2.ip-v4.udp.link       | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.245.4.0.1.0.0   |
| *ether2.ip-v4.udp.dsp3270    | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.0.246.4.0.1.0.0   |
| *ether2.ip-v4.udp.ldap       | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.1.133.4.0.1.0.0   |
| *ether2.ip-v4.udp.biff       | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.2.0.4.0.1.0.0     |
| *ether2.ip-v4.udp.who        | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.2.1.4.0.1.0.0     |
| *ether2.ip-v4.udp.syslog     | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.2.2.4.0.1.0.0     |
| *ether2.ip-v4.udp.ip-xns-rip | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.2.8.4.0.1.0.0     |
| *ether2.ip-v4.udp.banyan-vip | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.2.61.4.0.1.0.0    |
| *ether2.ip-v4.udp.notes      | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.5.72.4.0.1.0.0    |
| *ether2.ip-v4.udp.ccmil      | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.12.192.4.0.1.0.0  |
| *ether2.ip-v4.udp.quake      | 16.1.0.0.1.0.0.8.0.0.0.0.17.0.0.101.144.4.0.1.0.0 |

