XENYA

XS26GS

Managed Optical Ethernet Switch

User Manual

June 15 , 2011

Version: 1.01

Copyright © 2010-2011, XENYA d.o.o.

All Rights Reserved

This document contains proprietary information that is protected by copyright. No part of this document may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language, in any form or by any means, electronic, mechanical, magnetic, optical, chemical, manual or otherwise without the prior written permission of Xenya d.o.o.

Disclaimer Notice:

No license is granted, implied or otherwise, under any patent or patent rights of XENYA d.o.o. makes no warranties, implied or otherwise, in regard to this document and to the products described in this document. The information provided by this document is believed to be accurate and reliable to the publication date of this document. However, Xenya d.o.o. assumes no responsibility for any errors in this document. Furthermore, Xenya d.o.o. assumes no responsibility for the use or misuse of the information in this document and for any patent infringements that may arise from the use of this document. The information and product specifications within this document are subject to change at any time, without notice and without obligation to notify any person of such change.

Table of Contents

1. Introduction 5

1.1 Features 5
1.2 Face Panel 2
1.3 SFP Based Optical Interface Options 2
1.4 Power Supply Options 2
1.5 Physical and Environmental 2
1.6 Default Configuration 3
1.7 Management Software Specification 4

2. Web Management Function 5

2.1 Conventions 5
2.2 System Information 5
2.3 Advanced Configuration 6
2.4 Port Management 6
2.4.1 Port Configuration 7
2.4.2 Port Aggregation 7
2.4.3 Port Bandwidth 9
2.4.4 Port Mirroring 10
2.5 VLAN 11
2.5.1 Advanced 11
2.5.2 Port-based VLAN 11
2.5.3 802.1Q VLAN 11
2.5.4 Protocol VLAN 13
2.5.5 MAC-based VLAN 13
2.5.6 VLAN VPN 14
2.5.7 GARP 16
2.6 QoS 16
2.6.1 QoS Configuration 17
2.6.2 Scheduling Mechanism 17
2.6.3 Transmit Queues 18
2.6.4 DSCP Map 18
2.7 Forwarding 19
2.7.1 Unicast MAC Address 19
2.7.2 Multicast MAC Address 20
2.7.3 IGMP Snooping 21
2.7.4 MVR 22
2.7.5 Unknown Multicast 23
2.8 Security 24
2.8.1 Management Security 24
2.8.2 Port Authentication 24
2.8.3 MAC Authentication 27
2.8.4 IP Binding 28
2.8.5 Storm Control 28
2.9 ACL 28
2.9.1 Management ACL 29
2.9.2 ACL Rule 29
2.9.3 Port Binding 32
2.10 LLDP 32
2.10.1 Management LLDP 32
2.10.2 Neighbor Information 34
2.10.3 LLDP Statistics 34
2.11 Statistics 36
2.11.1 Port Status 36
2.11.2 Port Statistics 36
2.11.3 VLAN List 37
2.11.4 MAC Address Table 37

2.11.5 IGMP Snooping Group 38
2.11.6 Link Aggregation 38
2.12 Spanning Tree 39
2.12.1 Global 39
2.12.2 STP&RSTP 40
2.12.3 MSTP Region 43
2.12.4 MSTP Ports 45
2.12.5 MSTP State 46
2.13 SNMP Manager 46
2.13.1 SNMP Account 46
2.13.2 SNMP Trap 48
2.14 Administration 49
2.14.1 IP Configuration 49
2.14.2 Ping Diagnosis 50
2.14.3 Account 50
2.14.4 TFTP Services 51
2.14.5 Reboot 52
2.14.6 Reset 52
2.14.7 Save Configuration 53
2.14.8 System Logs 53
2.15 Logout 54

3. Command Line Interface (CLI) 55

3.1 ERROR Message 55
3.2 CLI Conventions 55
3.3 Shortcuts Introduction 55
3.4 CLI Command Modes 56
3.5 Global Commands 57
3.6 User Level 57
3.7 System Management Commands 58
3.8 Port Basic Configuration Commands 70
3.9 Link Aggregation Commands 78
3.10 Mirroring Commands 85
3.11 VLAN Commands 87
3.11.1 VLAN Configuration Commands 87
3.11.2 Port-Based VLAN Configuration Commands 98
3.12 VLAN VPN 101
3.13 GVRP Commands 103
3.14 QoS Commands 107
3.15 MAC Address Table Management Commands 113
3.16 Multicast Commands 118
3.17 IGMP Snooping Configuration Commands 120
3.18 802.1x Configuration Commands 126
3.19 STP Commands 133
3.20 SNMP Configuration Commands 149
3.21 System Log Commands 157
3.22 LLDP Configuration Commands 158
3.23 ACL Configuration Commands 164
3.24 Port Binding Configuration Commands 166
3.25 MVR configuration commands 168
3.26 Loopback-detection 172

4. Ordering Information 176

5. Appendix A: Command Index 177

6. Appendix B: Supported MIBs 184

REVISION HISTORY

Date	Version	Description
Jan 28, 2011	V1.00	Initial release
Jun 15, 2011	V1.01	Graphics update

1. Introduction

XS26GS Managed SFP Based Optical Ethernet Switch is a high-performance managed Layer 2+ Gigabit Ethernet switch for service providers. It offers up to twenty-six SFP based Gigabit Ethernet fiber optic ports.

XS26GS is targeted at the emerging market of Ethernet based FTTx. It comes with a rich feature set to meet the requirements of a wide range of applications, especially the access network and the small-to-medium-scale customized network. The design of dual power supply provides the power redundancy for applications requiring high reliability. XS26GS is low-profile with a standard rack-mount size. It achieves the highest fiber port density within a single rack, providing users with the best performance/price ratio.

1.1 Features

- A range of configurable copper and fiber ports to meet the requirement of various applications, such as FTTH, optical LAN, Ethernet-based DCS and security surveillance system.
- 8K address table for auto-learned unicast or static unicast/multicast addresses.
- Jumbo frame of up to 9216 bytes
- 802.1p, Port, and DiffServ based QoS package classification with 4 priority queues. Support queue mapping and DSCP mapping.
- 4K 802.1Q based VLAN
- Port based VLAN
- 16 Protocol based VLAN
- MAC based VLAN
- Guest VLAN
- VLAN VPN, QinQ
- GARP/GVRP
- 16 trunk groups of up to 8 member ports with flexible load distribution control and fail-over functions.
- Manual, static, and dynamic port aggregation
- 802.1d Spanning Tree Protocol, 802.1w Rapid Spanning Tree Protocol, and 802.1s Multiple Spanning Tree Protocol.
- By-port egress, ingress, and bi-direction rate control
- Multi combination of MAC address, VID, and port binding
- Static and dynamic MAC addressing
- Blackhole MAC address filtering
- IGMP Snooping
- Multicast VLAN Registration (MVR)
- Link Layer Discovery Protocol (LLDP)
- Storm Control for any combination of multicast, broadcast, and DLF traffic
- Access Control Lists (ACL)
- Secure Shell (SSH) v2.0
- 802.1x Port-based access control and MAC authentication
- User configurable port mirroring supports ingress/egress/both data flow monitoring on one or more ports.
- SNMP v1/v2c/v3
- Web page management
- Command Line Interface (CLI)
- Telnet and RS232 console management

- User account assignable to one of the three access privilege levels
- On-line firmware upgrade
- Configuration file backup and restore
- Dual power supply modules provide power redundancy with status monitoring features.

1.2 Face Panel

The face panel of the XS26GS optical Ethernet switch is shown in the following figure.

1.3 SFP Based Optical Interface Options

- 1000Base-X
  - Dual multimode fiber(50/125μm), single wavelength 850nm, dual LC connector, 550m reach.
  - Dual multimode fiber(62.5/125μm), single wavelength 850nm, dual LC connector, 275m reach.
  - Dual single-mode fiber, single wavelength 1310nm or 1550nm, dual LC connector, 15/40 km reach.

1.4 Power Supply Options

- AC90~264V/1.2A max, 50/60Hz, or
- DC18~36V/2A, or
- DC36~72V/1.5A
- Power Consumption: no more than 45W

1.5 Physical and Environmental

- Dimensions: 19-inch rack-mount width, 1.0U height
- Weight: ~5Kg
- Operating temperature: 0℃ ~ 50℃
- Storage temperature: -25℃ ~ 85℃
- Humidity: 5% ~ 95% RH Non-condensing

1.6 Default Configuration

(1) Administration

IP:

IP Address:	192.168.0.253
IP Sub network:	255.255.255.0
IP Gateway:	192.168.0.201

Accounts:

User Level:	Visitor	User	Administrator
User Name:	guest	manager	superuser
Password:	(none)	123	123

(2) Port

State:	enabled
Flow Control:	disabled
Learning:	enabled
Rate limit:	disabled
Negotiation:	enabled

(3) VLAN

VLAN mode:	none
Static VLAN:	1, including all ports
Port VID:	1
Port link type:	hybrid
Frame type:	admit all

(4) SNMP

Version:	v1
Community:	public
Privilege :	RO
User:	(none)
SNMP trap:	enabled
Trap host IP:	(none)

(5) Protocols

IGMP Snooping:	Disabled
GARP/GVRP:	Disabled
STP:	Disabled
LACP:	Disabled
802.1x:	Disabled
LLDP:	Disabled

1.7 Management Software Specification

The following table summarizes the protocols supported by the managed optical Ethernet switch in the current software release.

TCP/IP	ARP, ICMP, IP, TCP, UDP
SNMP	SNMP v2(1,2,3,9), FMC private MIBS, MIB counters of groups 1,2,4,9
Web management server	Http Server. Support goahead-2.1.8.Java scripts, Java Applet, CGI
Telnet server	Telnet 1.0
Console	Standard UART
Spanning tree protocol	IEEE 802.1d/1w/1s
Four-level priority queuing	IEEE 802.1p
Port-based VLAN	SVL
Tag-based VLAN	IEEE 802.1q (IVL and SVL), GVRP
Protocol-based VLAN	IEEE 802.1v
Trunking	IEEE 802.3ad, LACP
Authentication	IEEE 802.1x
IGMP Snooping	RFC2236

2. Web Management Function

A Web browser has been provided to manage and monitor the switch. The default values are set in section 1.6 of this manual. When logging to the switch, you can browse http://192.168.0.253 and type the user name and password as shown in section 1.6 above.

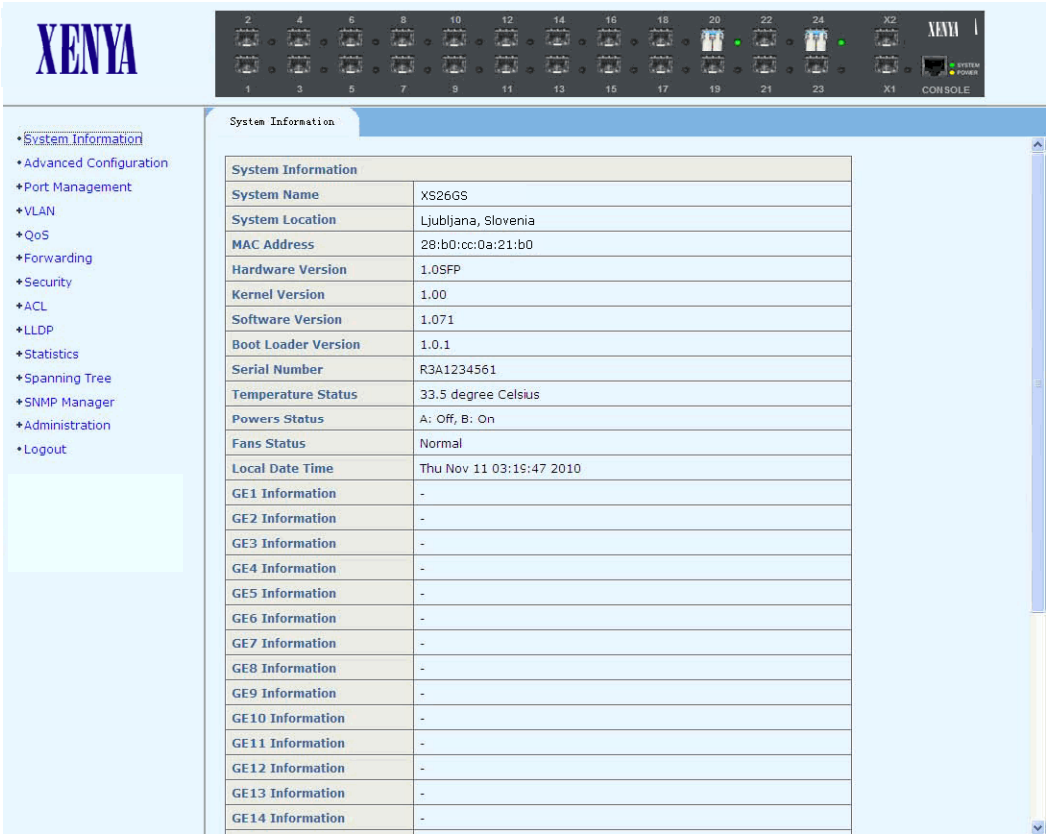
If you need to change IP address at the first time, you can modify it through RS232 console, or using telnet to login.

2.1 Conventions

Convention	Description
Boldface	Keywords on web management page is in **Boldface**
italic	Tag page name is in *italic*
<>	Button on web management page is in <>

2.2 System Information

At login, the web is on System Information page, which shows the basic information of the switch as below.

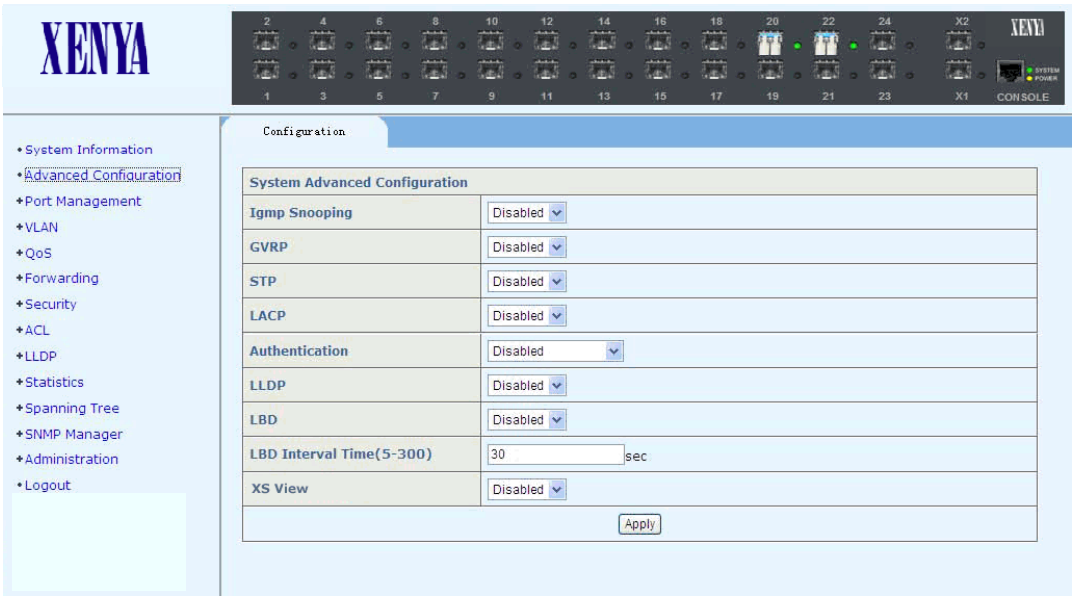


2.3 Advanced Configuration

This page configures whether to globally enable or disable the following protocols:

- IGMP Snooping
- GVRP
- STP
- LACP
- Authentication
- LLDP
- LBD
- LBD Interval Time
- XS View

IGMP Snooping: globally enable or disable the protocol.
GVRP: globally enable or disable the protocol.
STP: globally enable or disable the protocol.
LACP: globally enable or disable the protocol.
Authentication: select authentication between 802.1x or MAC based, or disable the authentication.
LLDP: globally enable or disable the protocol.
LBD: used to globally enable loopback detection function on this switch. It will check whether there is a loop on the switch on any VLAN. If there is one on a VLAN, it will shut down the port or will send out a trap.
LBD Interval Time: time interval for loopback detection, in the range of 5 to 300 (seconds). The default value is 30.
XS View: enable or disable the XS View management software.



2.4 Port Management

This page configures port related management functions as below:

- Port Configuration
- Port Aggregation
- Port Bandwidth
- Port Mirroring

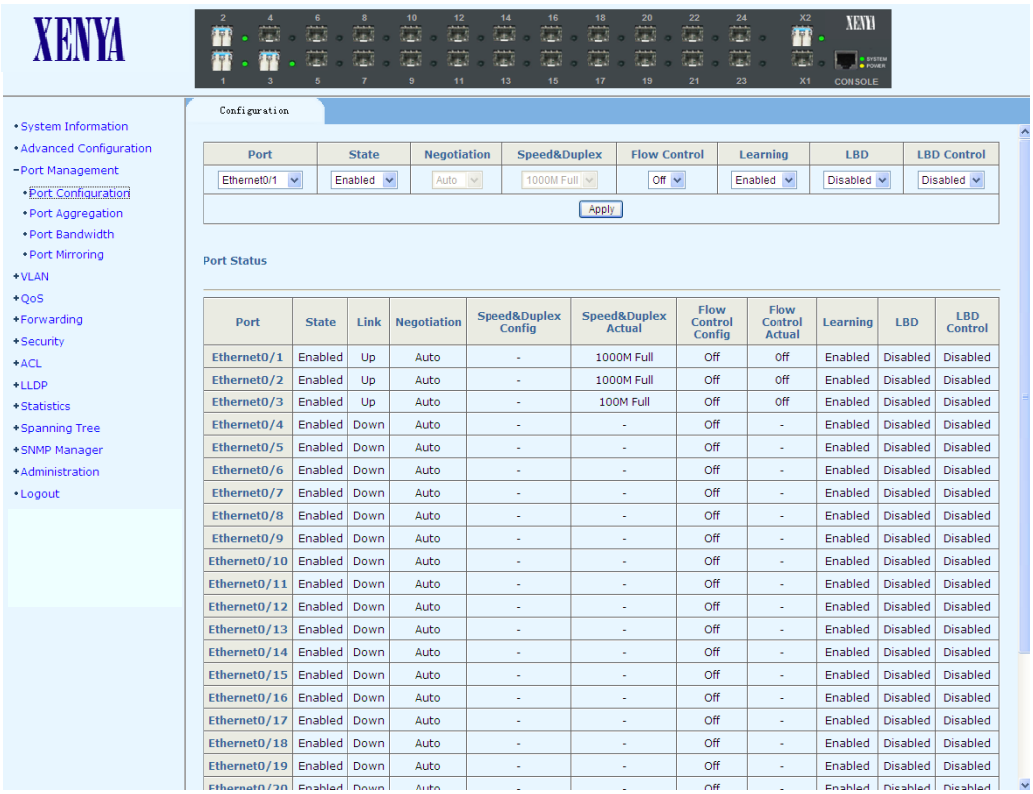
2.4.1 Port Configuration

This page configures a port. When the setup is completed, click <Apply> to take effect.

LBD: enables loopback detection for the specific port.
LBD Control: enable or disable LBD Control for the specific port. If the loopback port control function is enabled on a trunk or hybrid port when a loop is found, the switch will disable the port, and remove the corresponding MAC forwarding entries. On the other hand, if the loopback port control function is disabled on a trunk or hybrid port when a loop is found, the port will not be disabled. For an access port, the switch will disable the port if a loop is found, as far as LBD is enabled, no matter LBD Control is enabled or disabled.

By default, the loopback port control function is disabled on a trunk or hybrid port.

A list of the port status is also provided. See the following figure for more details.



2.4.2 Port Aggregation

XS26GS switch supports up to 16 link aggregation groups, and each group can have up to 8 ports.

This page sets link aggregation. There are three types of aggregation: manual, static, and dynamic. The following is a detailed description of each type of aggregation:

Manual aggregation: a manual trunk can only be manually set or deleted; any port in a manual trunk shall have this port's Link Aggregation Control Protocol (LACP) disabled, while the global LACP can be either enabled or disabled.

Static LACP aggregation: a static LACP trunk can only be manually set or deleted; any

port in a static LACP trunk shall have this port's Link LACP enabled. When a static LACP trunk is (manually) deleted, all ports of this trunk with "up" status will generate one or more dynamic LACP trunks automatically.

Dynamic LACP aggregation: a dynamic LACP trunk can only be set or deleted automatically by the protocol; any port in a dynamic LACP trunk shall have this port's LACP enabled.

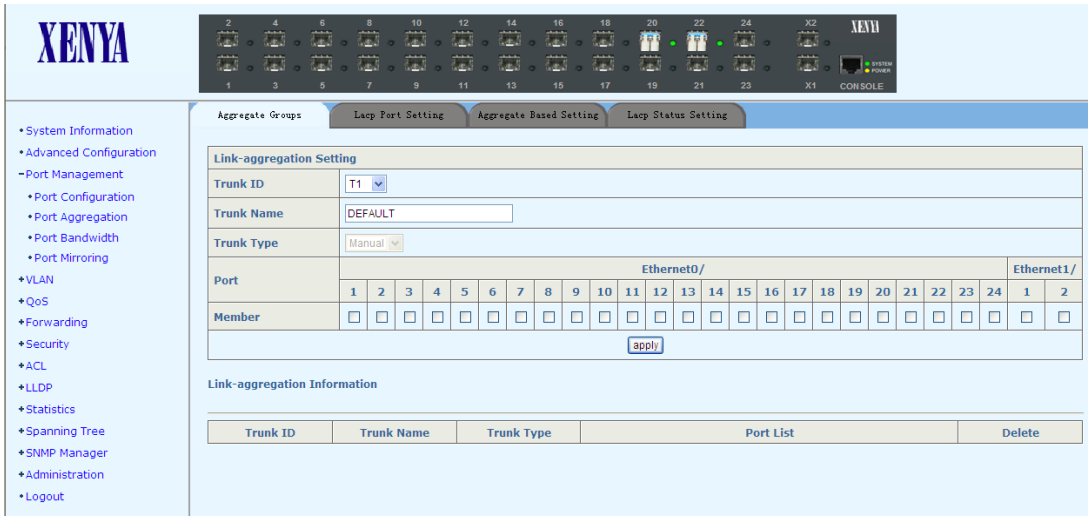
A trunk may be configured as a mirror port, but it is not allowed to configure a trunk as a monitoring port.

There are four tag pages on this webpage to configure various parameters:

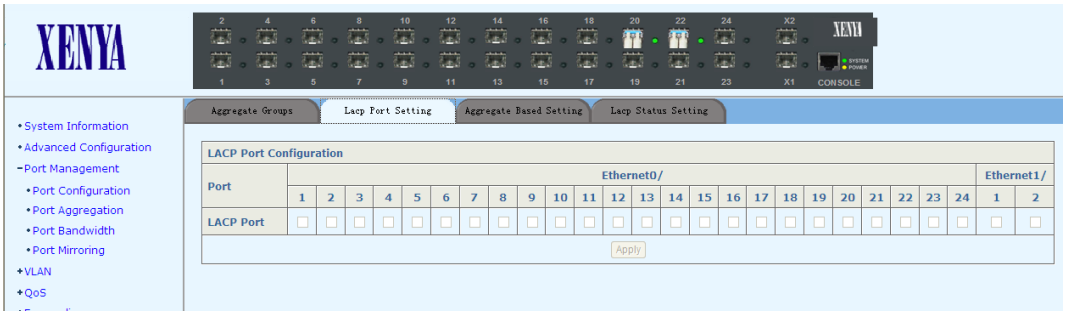
Aggregate Groups – create and configure a trunk. The switch can have up to 13 trunks.
Trunk ID: one of the 13 trunk IDs (from T1 to T13) for the user to choose from.
Trunk Name: give a name for the selected trunk.
Trunk Type: select the trunk to be a manual trunk, or static LACP trunk.
Port: choose up to 8 ports to form the trunk.

The bottom part of this tag page lists all existing trunks.

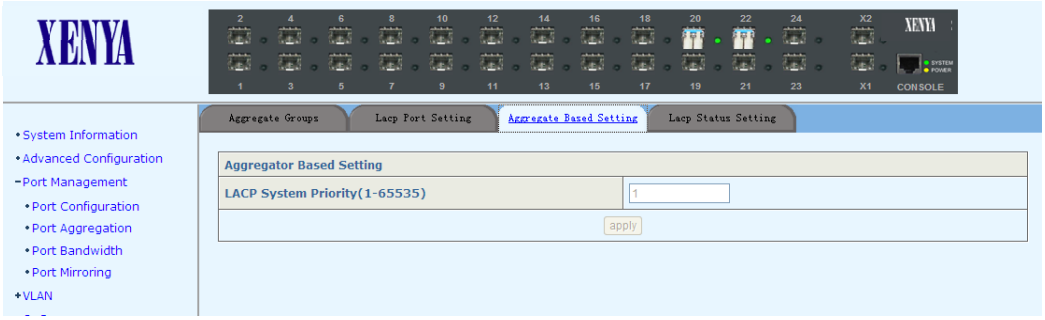
Note: Only when **LACP** in *Advanced Configuration* page is enabled, **Trunk Type** can be selected; otherwise, the **Trunk Type** is **Manual**.



Lacp Port Setting – configures LACP ports



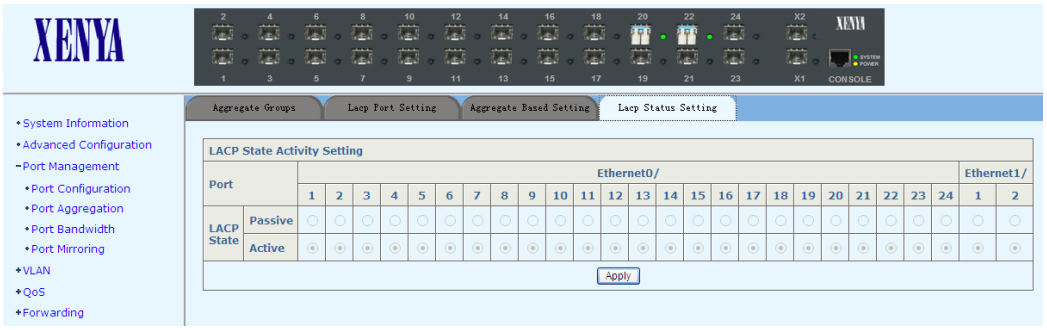
Aggregate Based Setting – sets LACP system priority, between 1 and 65535



Lacp Status Setting – sets LACP active or passive for each port

Active: The port automatically sends LACP protocol packets.
Passive: The port does not automatically send LACP protocol packets; it responds only if it receives a LACP protocol packet from the opposite device.

A link having either one or two active LACP ports can perform dynamic LACP trunking. A link has two passive LACP ports that will not perform dynamic LACP trunking as both ports are waiting for LACP protocol packet from the opposite device.



2.4.3 Port Bandwidth

This page sets the ingress and/or egress rate limit for each port.

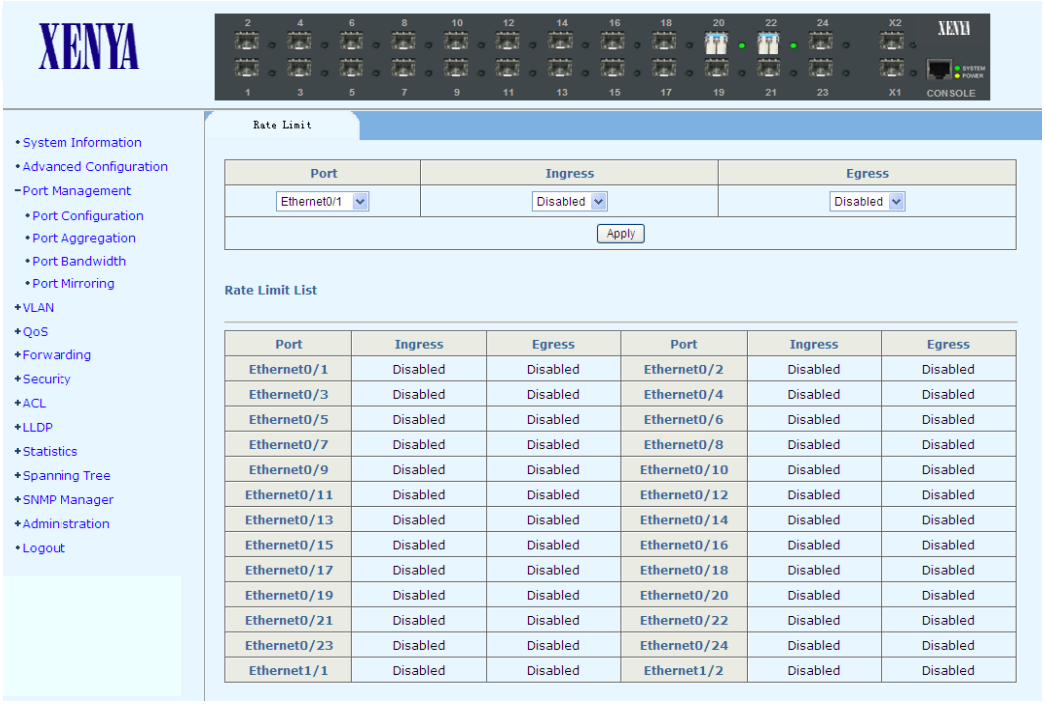
Port: the port for which the rate limit is configured.

Ingress: the desired ingress rate limit to be configured. Choose "disabled" to set the port with no ingress rate limit, which means the port will run in full speed for ingress traffic.

Egress: the desired egress rate limit to be configured. Choose "disabled" to set the port with no egress rate limit, which means the port will run in full speed for egress traffic.

When completing a configuration, click <apply> to take effect.

The bottom part of this page shows a full list of rate limit for each port.



2.4.4 Port Mirroring

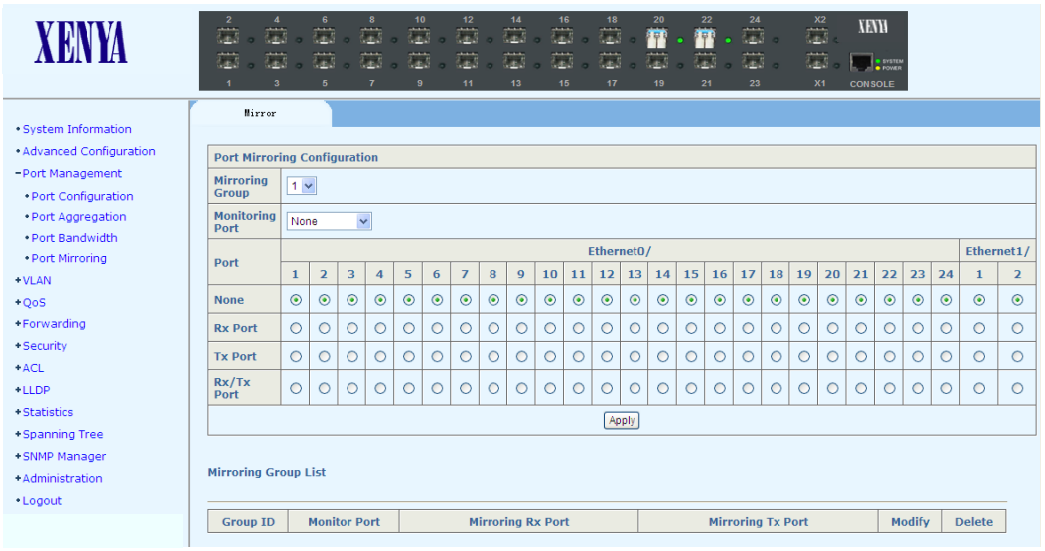
This page configures the port mirroring function. You can set up 1 to 4 Mirroring Groups,each group can select one Monitotring Port, but more than one Morroring.

Monitoring Port: the port or ports to which the traffic is mirrored

Rx Port: all ingress traffic of this port will be mirrored to each of the Monitoring Port(s)

Tx Port: all egress traffic of this port will be mirrored to each of the Monitoring Port(s)

Rx/Tx Port: all ingress and egress traffic of this port will be mirrored to each of the Monitoring Port(s)



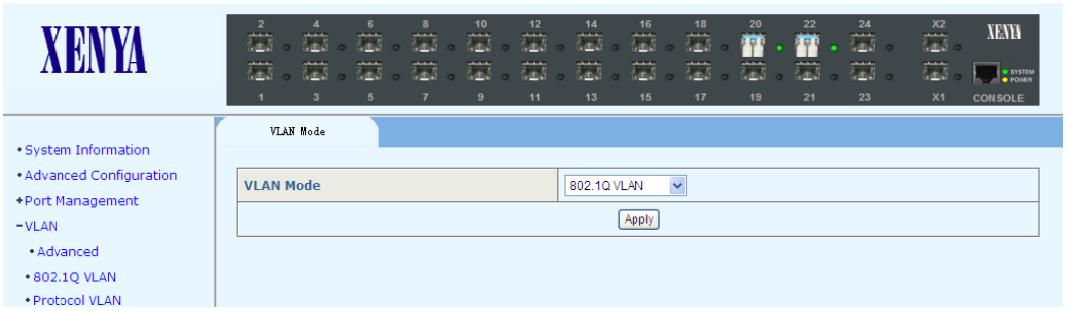
2.5 VLAN

This managed switch supports 802.1Q, port-based, mac-based vlan, vlan-vpn and protocol-based VLAN.

VLAN is disabled in default configuration.

2.5.1 Advanced

This page globally sets the VLAN mode from the following: no VLAN, 802.1Q VLAN, and port-based VLAN.

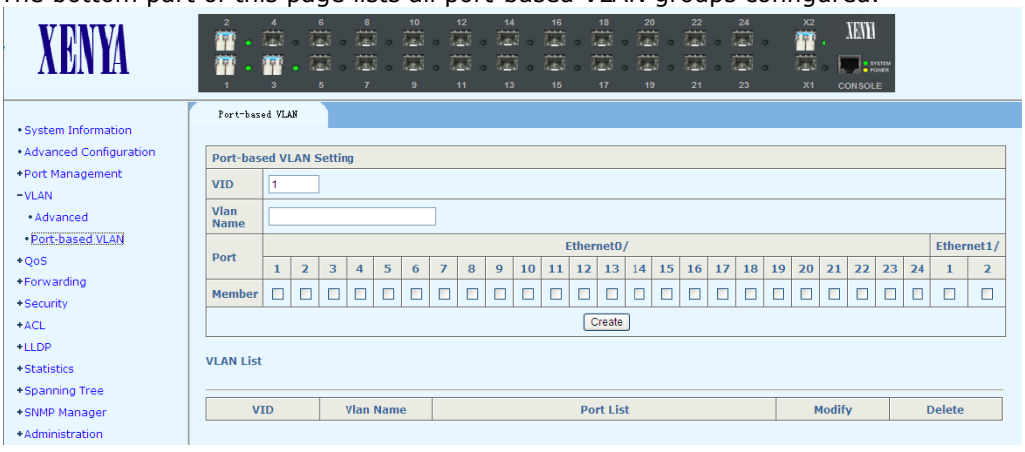


2.5.2 Port-based VLAN

On this page, the user can create a new VLAN group with specific VID and VLAN group name. Up to 256 VLAN groups can be created; each VLAN group can have an ID number from 1 to 4094.

Member: checks to indicate the port is a member of the VLAN group.

The bottom part of this page lists all port-based VLAN groups configured.



2.5.3 802.1Q VLAN

There is a default VLAN group with VLAN identifier (VID) of 1, each port is a member of this group in default, and remains as a member before it is removed from the group.

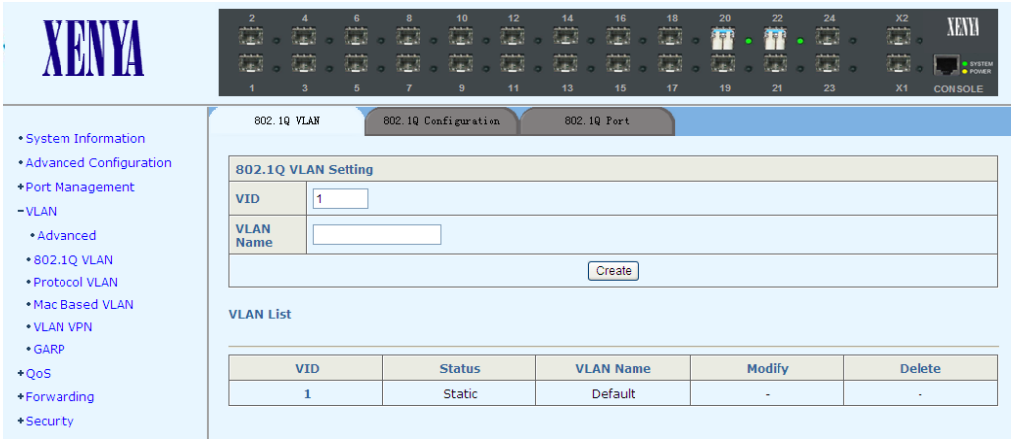
There are three tag pages on this webpage for the user to configure various parameters:

2.5.3.1 802.1Q VLAN

On this tag page, the user can create a new VLAN group with specific VID and VLAN group name. Up to 256 VLAN groups can be created; each VLAN group can have an ID number from 1 to 4094.

The bottom part of this page lists all existing VLAN groups, as well as the information on each VLAN group. Users can also modify or delete an existing VLAN group.

Note: It is not allowed to delete VLAN group 1.



2.5.3.2 802.1Q Configuration

This tag page configures a VLAN group; each port can be configured as a specific state for this VLAN group:

Tagged: indicates the port is a tagged member of the VLAN group. All packets forwarded by the port are tagged. The packets contain VLAN information.

Untagged: indicates the port is an untagged VLAN member of the VLAN group. Packets forwarded by the port are untagged.

Exclude*:* excludes the port from the VLAN group. However, the port can be added to the VLAN group through GARP.

Forbidden: does not allow the port to be added to the VLAN group, even if GARP indicates so.

2.5.3.3 802.1Q Port

This tag page configures 802.1Q VLAN port parameters:

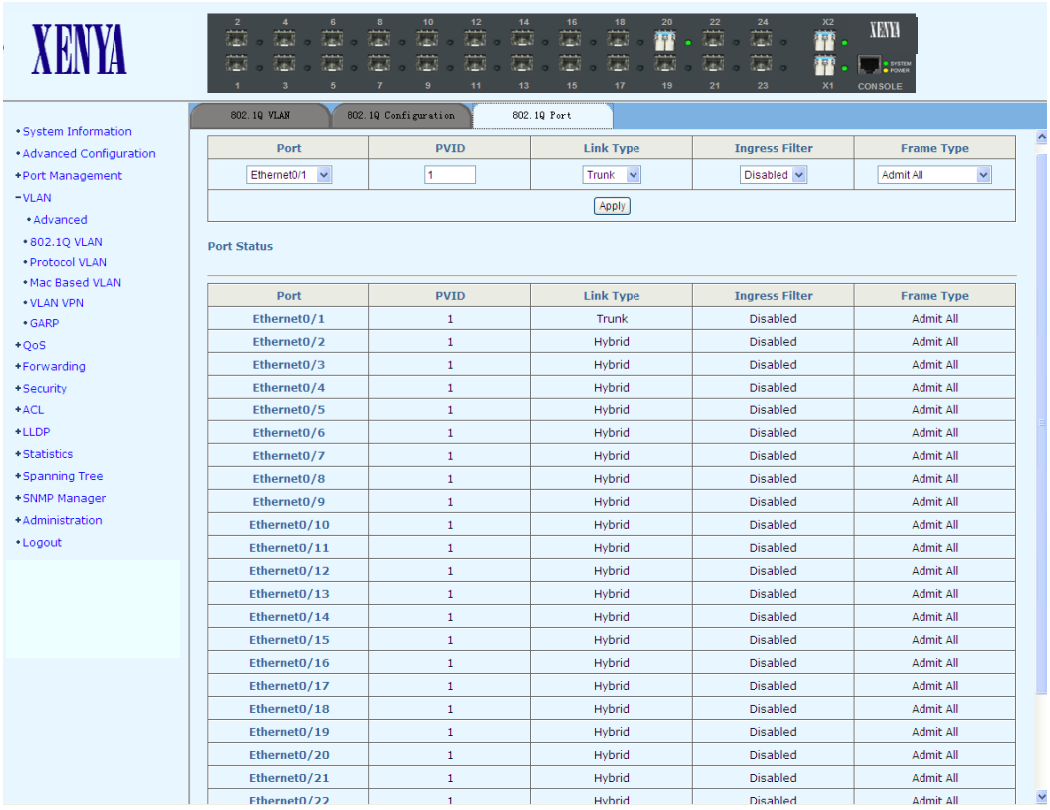
PVID: each port can have only one Port VLAN ID (PVID), an untagged Ethernet package will be tagged a VID of PVID when arriving at the port. The default PVID is 1 for each port.

Link Type: can choose **Access**, **Trunk**, or **Hybrid** (by default) from this pull-down block. An **Access** port has only one VLAN and the tag is removed when egress (i.e. **Untagged**); a **Trunk** port can have multiple VLANs, and all packages are tagged, except when an egress package is in a VLAN group with VID the same as PVID; a **Hybrid** port is similar to a **Trunk** port, except it leaves the user a flexibility of configuring each port's **Tagged** or **Untagged**.

Ingress Fliter:When enabled, an Ethernet package is discarded if this port is not a member of the VLAN with which this package is associated. When disabled(by default), all packages are forwarded in accordance with the 802.1Q VLAN bridge specification.

Frame Type: chooses how the port accepts Ethernet package. When **Admit All** is selected, the port accepts all ingress packages; while **Admit Only Tagged** accepts tagged packages, and discards untagged ones.

The bottom part of this tag page lists the status of all ports.



2.5.4 Protocol VLAN

This page configures protocol VLAN. The pull down **VID** block lists all existing VLAN groups for users to choose a group to configure. For a selected VLAN group, the **Frame Type** lists all protocols for which users can choose. **Ethernet Type** is bundled with the **Frame Type** chosen, except for **Ethernet II**, for which users can type in an **Ethernet Type**.Coressponding **Port** is selected when setting **Protocol VLAN** group.
The bottom part of this page lists all protocol VLAN groups configured.

2.5.5 MAC-based VLAN

This page configures mac-based VLAN. The pull down **VID** block lists all existing VLAN groups for the user to choose a group to configure. For a selected VLAN group, the **MAC Address** is the source MAC address of incoming packets, and the **Priority** is the added VLAN tag priority.

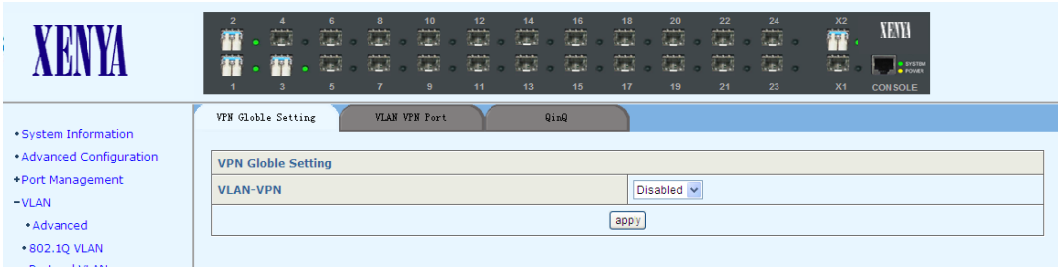
The bottom part of this page lists all mac-based VLAN groups configured.

2.5.6 VLAN VPN

2.5.6.1 VPN Global Setting

This page enables or disables global VLAN VPN.

VLAN VPN: enable or disable the global VLAN VPN.

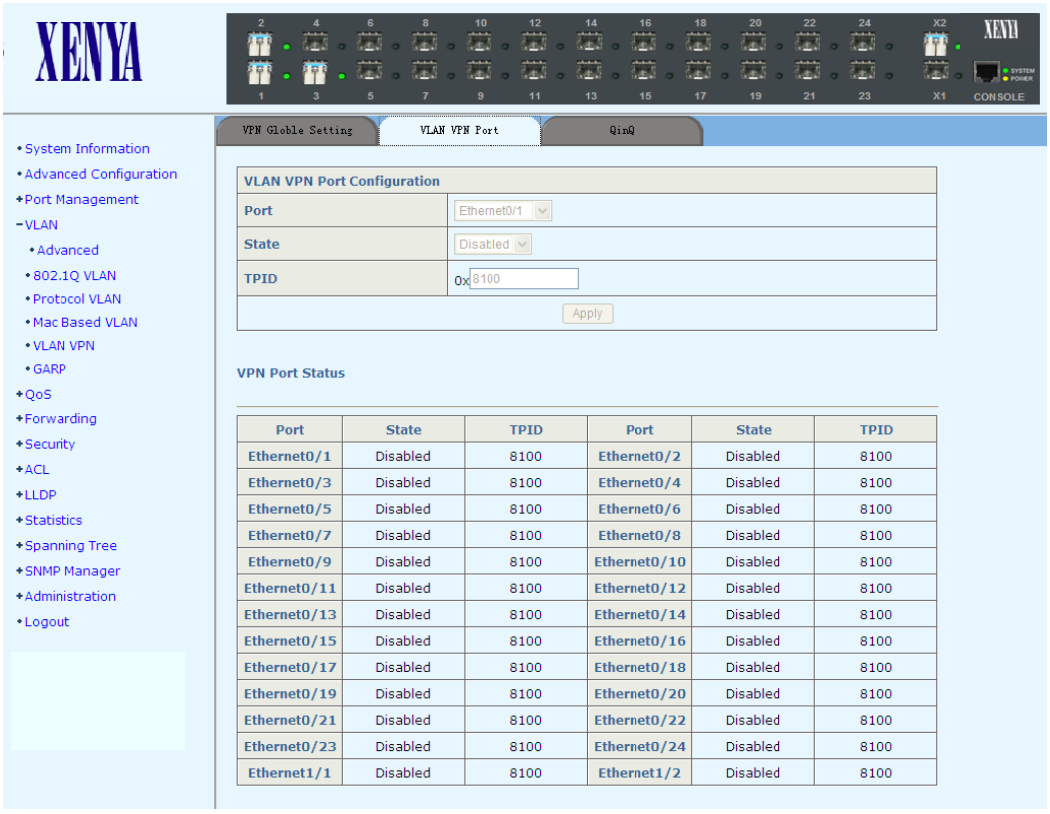


2.5.6.2 VLAN VPN Port

This page enables or disables VLAN VPN and sets TPID (Tag Protocol Identifier) value for a specific port. The default TPID value is 0x8100. Be aware that some other vendors' switches may set this value to be 0x9100.

Port: select a specific port for setting.
State: To enale or disable a specific port.
TPID: To set TPID value, 0x8100 by default. TPID is used to identify whether the packets carry specific VLAN Tag. Note that the location of the TPID field in an Ethernet packet is the same as the protocol type field in a packet without VLAN Tag. Thus, to prevent confusion from happening, the following protocol type values should not be configured as a TPID value.

- ARP: 0x0806
- IP: 0x0800
- MPLS: 0x8847/0x8848
- IPX: 0x8137
- IS-IS: 0x8000
- LACP: 0x8809
- 802.1x: 0x888E



Port	State	TPID	Port	State	TPID
Ethernet0/1	Disabled	8100	Ethernet0/2	Disabled	8100
Ethernet0/3	Disabled	8100	Ethernet0/4	Disabled	8100
Ethernet0/5	Disabled	8100	Ethernet0/6	Disabled	8100
Ethernet0/7	Disabled	8100	Ethernet0/8	Disabled	8100
Ethernet0/9	Disabled	8100	Ethernet0/10	Disabled	8100
Ethernet0/11	Disabled	8100	Ethernet0/12	Disabled	8100
Ethernet0/13	Disabled	8100	Ethernet0/14	Disabled	8100
Ethernet0/15	Disabled	8100	Ethernet0/16	Disabled	8100
Ethernet0/17	Disabled	8100	Ethernet0/18	Disabled	8100
Ethernet0/19	Disabled	8100	Ethernet0/20	Disabled	8100
Ethernet0/21	Disabled	8100	Ethernet0/22	Disabled	8100
Ethernet0/23	Disabled	8100	Ethernet0/24	Disabled	8100
Ethernet1/1	Disabled	8100	Ethernet1/2	Disabled	8100

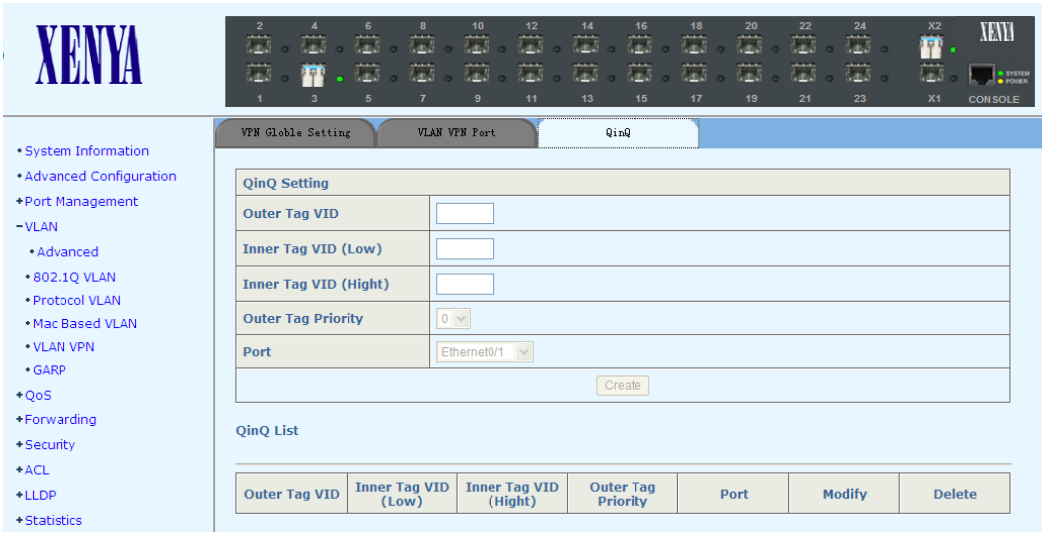
2.5.6.3 QinQ

QinQ is an enhanced feature of VLAN-VPN. An Outer Tag can be added, which is based on the inner Tag. In this page, you can set QinQ parameters as **Outer Tag VID**, **Inner Tag VID**, **Outer Tag Priority** and **Port**.

Outer Tag VID: A VLAN ID for the outer tag that will be added to the packet.
Inner tag VID(Low)/ Inner tag VID(High): An outer tag is added to form a double tag package, if the incoming package has a VLAN ID value between **Inner tag VID(Low)** and **Inner tag VID(High)** (all inclusive).

Outer Tag Priority: the outer tag VLAN priority, in the range of 0 to 7.
Port: the double tag port from which a package is received.

The bottom part of this page lists all configured QinQ mapping rules.

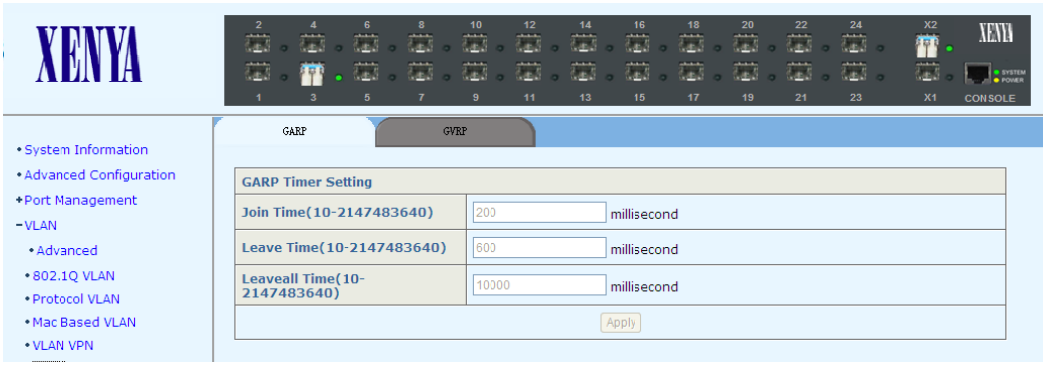


2.5.7 GARP

GARP VLAN Registration Protocol (GVRP) is based on Generic Attribute Registration Protocol (GARP). They are standard protocols described in IEEE 802.1D.

Before configuring GARP, make sure GVRP is enabled (see section 2.2 of this manual for details). There are two tag pages:

GARP: this tag page sets GARP **Join Time**, **Leave Time**, and **Leaveall Time**. **Leaveall Time** must be greater than **Leave Time**, and **Leave Time** must be greater than twice the **Join Time**.



GVRP: this tag page sets per port GVRP parameters. For a selected **Port**, enabled **GVRP**, the **Registration Type** can be set to **Normal** (default), **Fixed**, or **Forbidden**. **Normal** registration allows dynamic passing, registration, and de-registration of both dynamic and static VLANs; **Fixed** registration allows passing static VLANs, as well as manual registration, de-registration of VLANs; while **Forbidden** prohibits the port from passing, registration, or de-registration of VLANs.

The bottom part of *GVRP* tag page lists the GVRP attribute of all ports.

2.6 QoS

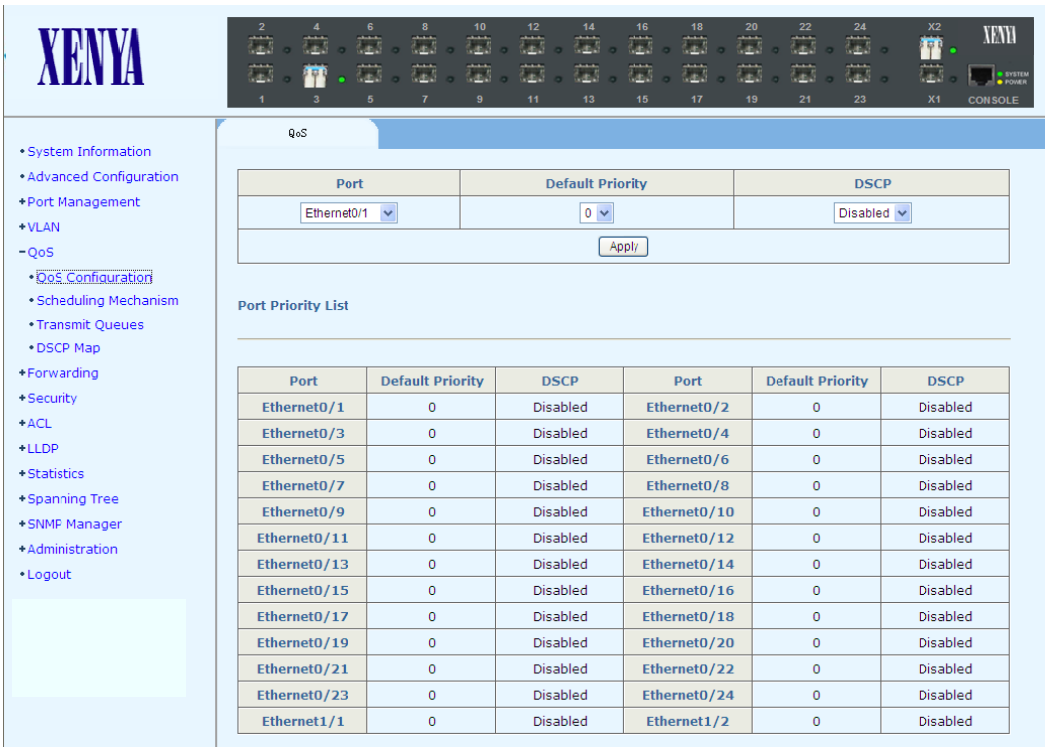
This managed switch supports Quality of Service (QoS).

QoS priority is disabled in default configuration.

2.6.1 QoS Configuration

*T*his tag page sets per port QoS parameters. For a selected **Port**, set the **Priority, with DSCP** enabled, the **Default Priority** can be set from 0-7.

The bottom part of QoS Configuration tag page lists the default priority of all ports and the state of DSCP.

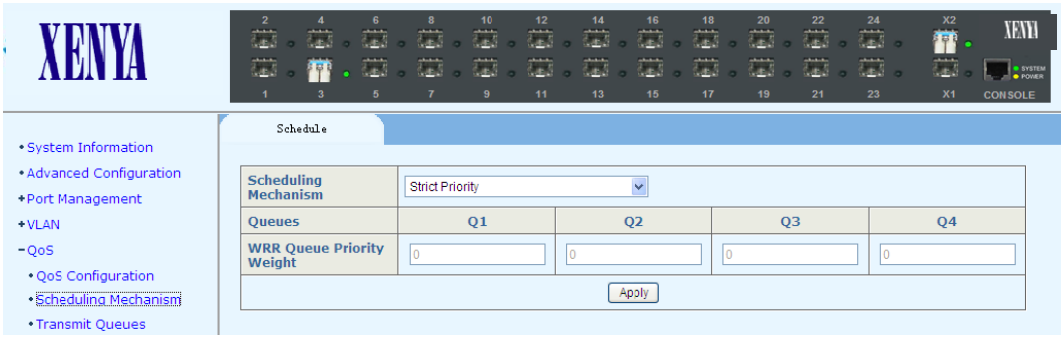


Port	Default Priority	DSCP	Port	Default Priority	DSCP
Ethernet0/1	0	Disabled	Ethernet0/2	0	Disabled
Ethernet0/3	0	Disabled	Ethernet0/4	0	Disabled
Ethernet0/5	0	Disabled	Ethernet0/6	0	Disabled
Ethernet0/7	0	Disabled	Ethernet0/8	0	Disabled
Ethernet0/9	0	Disabled	Ethernet0/10	0	Disabled
Ethernet0/11	0	Disabled	Ethernet0/12	0	Disabled
Ethernet0/13	0	Disabled	Ethernet0/14	0	Disabled
Ethernet0/15	0	Disabled	Ethernet0/16	0	Disabled
Ethernet0/17	0	Disabled	Ethernet0/18	0	Disabled
Ethernet0/19	0	Disabled	Ethernet0/20	0	Disabled
Ethernet0/21	0	Disabled	Ethernet0/22	0	Disabled
Ethernet0/23	0	Disabled	Ethernet0/24	0	Disabled
Ethernet1/1	0	Disabled	Ethernet1/2	0	Disabled

2.6.2 Scheduling Mechanism

This page sets the queue scheduling algorithm and related parameters.

Scheduling Mechanism can be set to **Strict Priority** or **Weighted Round-Robin (WRR)**.
Strict Priority: uses the strict priority (SP) algorithm for queue scheduling.
Weighted Round-Robin (WRR): uses the weighted round robin (WRR) algorithm for queue scheduling.
WRR Queue Priority Weight: customizes the weights to be assigned to queues 1 through 4. The value ranges from 1 to 55.



2.6.3 Transmit Queues

This page sets the 802.1p priority to local precedence mapping.
The following table lists the default mapping between 802.1p priority and local precedence:

802.1p priority	Local precedence
0	Q1
1	Q1
2	Q2
3	Q2
4	Q3
5	Q3
6	Q4
7	Q4

2.6.4 DSCP Map

This page sets the mapping between the DSCP value and the 802.1p priority.

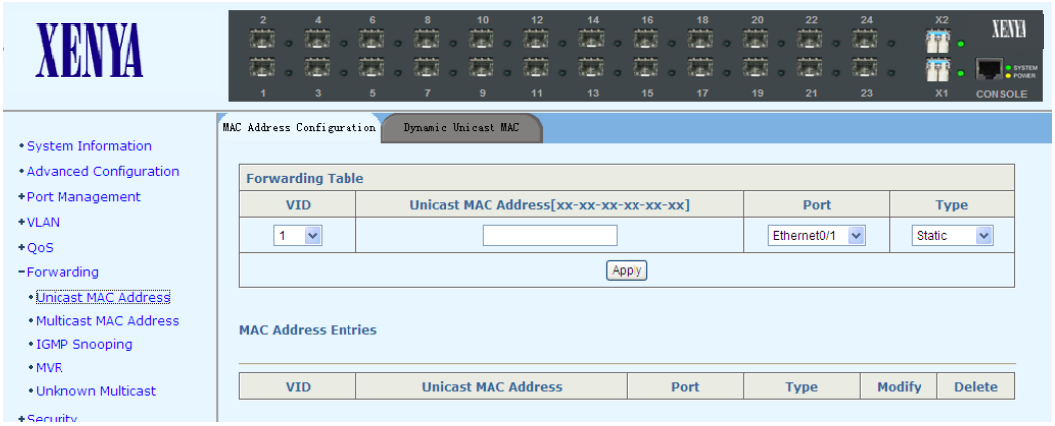
2.7 Forwarding

2.7.1 Unicast MAC Address

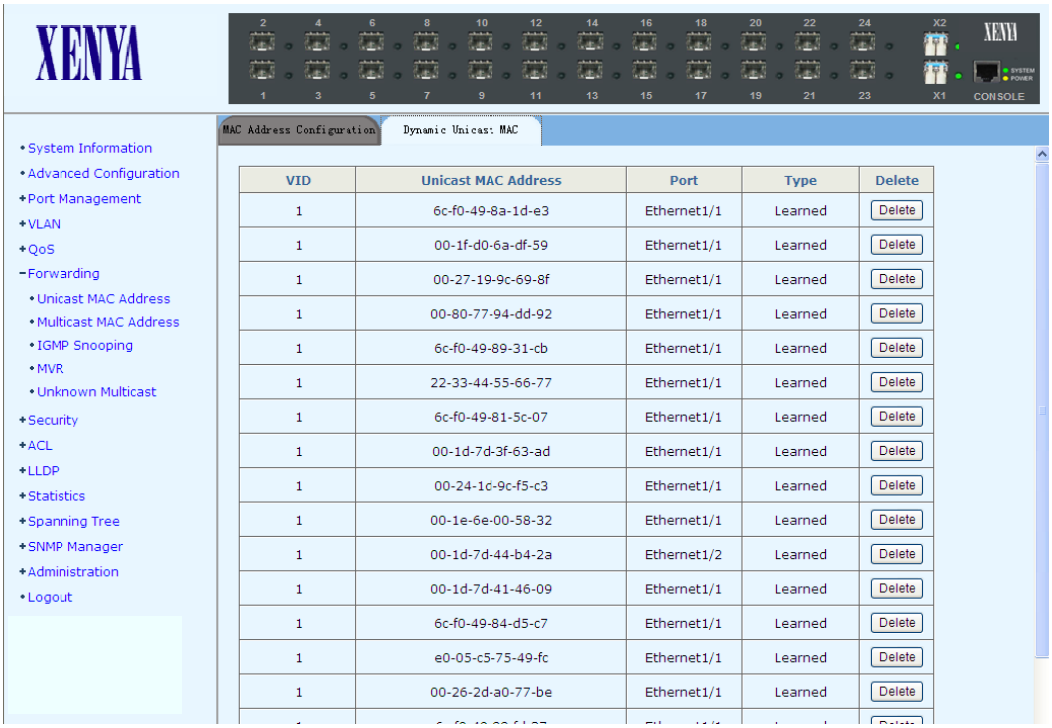
There are two tag pages:

MAC Address Configuration: To add, modify, or delete an entry in MAC table.
VID: Specifies a VLAN group to which the MAC address associated.
Unicast MAC Address: Specifies the destination MAC address.
Port: Specifies the port of the outbound interface.
Type: Choose among **Dynamic, Static and Blackhole**. **Dynamic** indicates a dynamic MAC address entry, **Static** indicates a static MAC address entry, and **Blackhole** indicates a blackhole MAC address entry.

The bottom part of *MAC Address Configuration* tag page lists all existing unicast MAC addresses, as well as the information of each unicast MAC address. The user can also modify or delete an existing unicast MAC address.



Dynamic Unicast MAC: This page lists all dynamic unicast MAC addresses. An entry can be deleted.



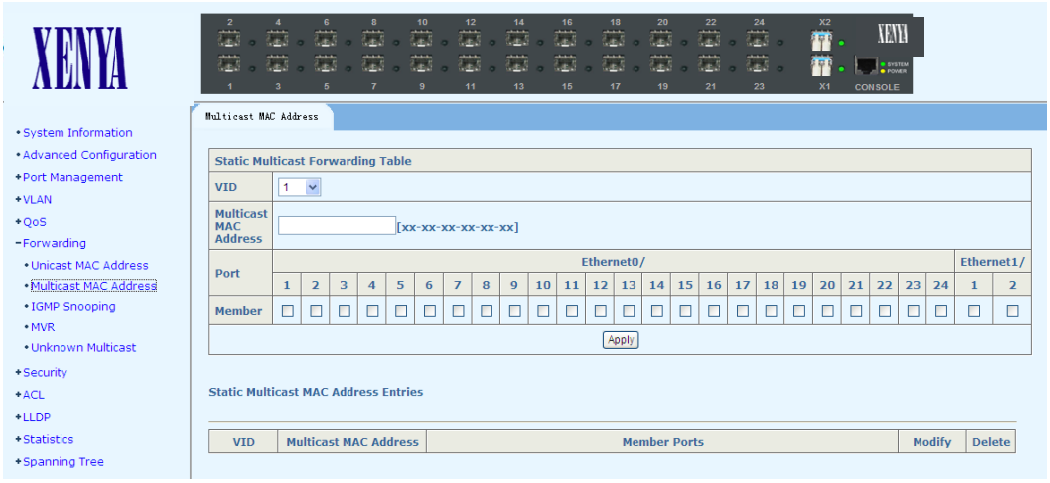
VID	Unicast MAC Address	Port	Type	Delete
1	6c-f0-49-8a-1d-e3	Ethernet1/1	Learned	Delete
1	00-1f-d0-6a-df-59	Ethernet1/1	Learned	Delete
1	00-27-19-9c-69-8f	Ethernet1/1	Learned	Delete
1	00-80-77-94-dd-92	Ethernet1/1	Learned	Delete
1	6c-f0-49-89-31-cb	Ethernet1/1	Learned	Delete
1	22-33-44-55-66-77	Ethernet1/1	Learned	Delete
1	6c-f0-49-81-5c-07	Ethernet1/1	Learned	Delete
1	00-1d-7d-3f-63-ad	Ethernet1/1	Learned	Delete
1	00-24-1c-9c-f5-c3	Ethernet1/1	Learned	Delete
1	00-1e-6e-00-58-32	Ethernet1/1	Learned	Delete
1	00-1d-7d-44-b4-2a	Ethernet1/2	Learned	Delete
1	00-1d-7d-41-46-09	Ethernet1/1	Learned	Delete
1	6c-f0-49-84-d5-c7	Ethernet1/1	Learned	Delete
1	e0-05-c5-75-49-fc	Ethernet1/1	Learned	Delete
1	00-26-2d-a0-77-be	Ethernet1/1	Learned	Delete

2.7.2 Multicast MAC Address

This page sets multicast MAC address entries. Each multicast MAC address entry contains multicast address, forward ports, and VID.
VID: Specifies the VLAN group for which the forwarding ports are members.
Multicast MAC Address: Multicast MAC address, in the form of H-H-H-H-H-H.

Member**: Specifies forwarding ports for the specified multicast MAC group address. One or more ports can be added as the member.**

The bottom part of this page lists all existing multicast MAC addresses, as well as the information of each multicast MAC address. The user can also modify or delete an existing multicast MAC address.



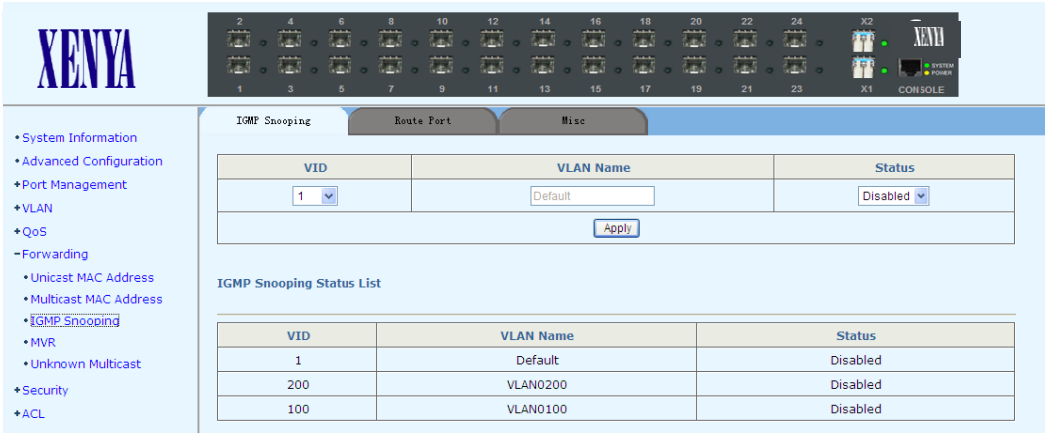
2.7.3 IGMP Snooping

There are three tag pages on this webpage for configuration:

2.7.3.1 IGMP Snooping

In this page, the user can enable IGMP Snooping feature for a VLAN group. By default, the IGMP Snooping feature is disabled.

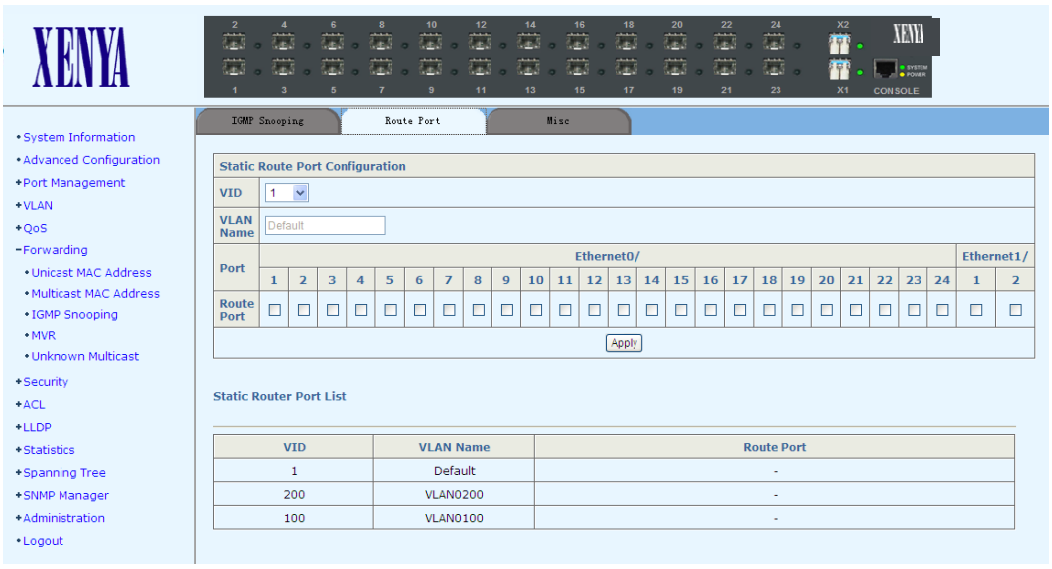
The bottom part of this page lists all VLAN IGMP Snooping feature status.



2.7.3.2 Route Port

In this page, the user can configure a port in a specified VLAN group as a static router port. By default, a port is not a static router port.

The bottom part of this page lists static router ports of all VLANs.

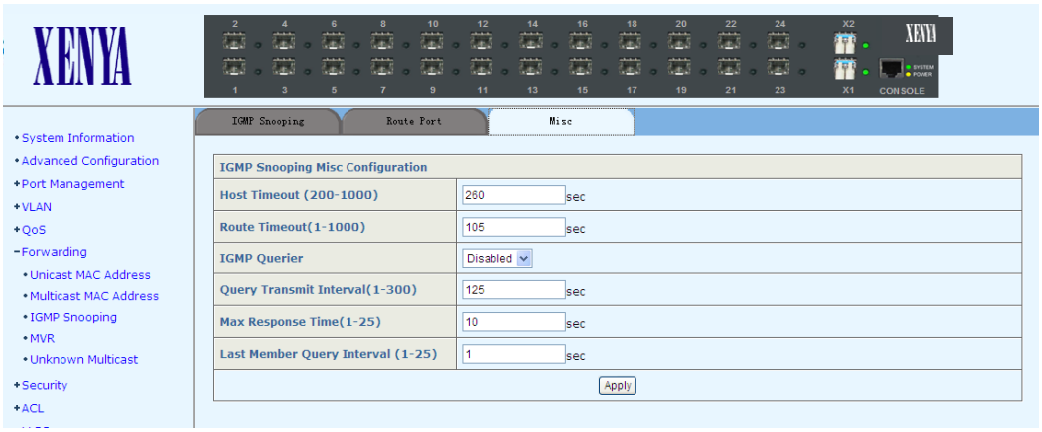


2.7.3.3 Misc

This tag page sets IGMP Snooping Misc configuration parameters: **Host Timeout, Route Timeout, IGMP Querier, Query Transmit Interval, Max Response**

Time, Last Member Query Interval, and IGMP Flood.

Host Timeout : It is in the range of 200 to 1000; by default, the value is 260 seconds.
Route Timeout :It is in the range of 1 to 1000; by default, the value is 105 seconds.
IGMP Querier : Enable/disable IGMP Querier function.
Query Transmit Interval :It is in the range of 1 to 300, by default, the value is 125 seconds.
Max Response Time : It is in the range of 1 to 25, by default, the value is 10 seconds.
Last Member Query Interval: It is in the range of 1 to 25, by default, the value is 1 second.



2.7.4 MVR

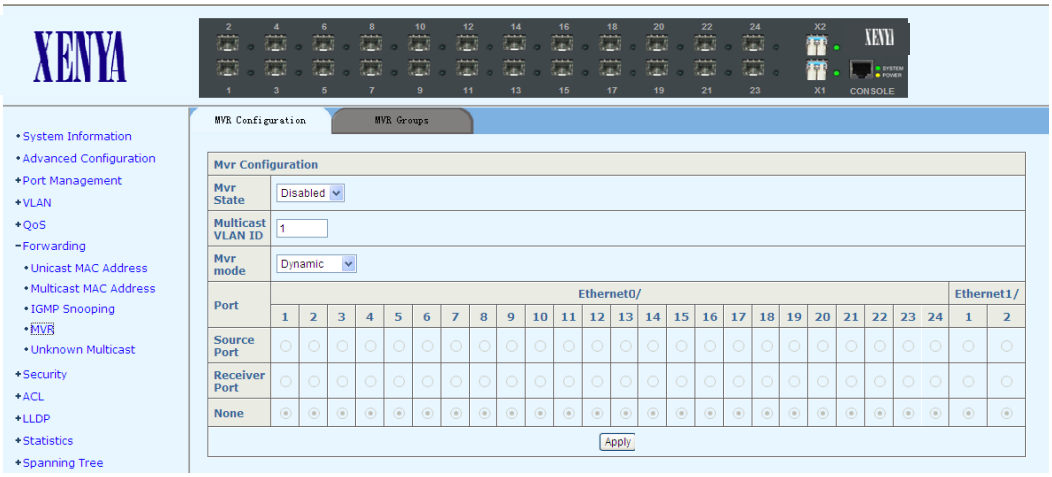
MVR(Multicast VLAN Registration) allows a subscriber on a port to subscribe and unsubscribe a multicast stream on the network-wide multicast VLAN. It allows the single multicast VLAN to be shared in the network while subscribers remain in separate VLANs. MVR provides the ability to continuously send multicast streams in the multicast VLAN, but it isolates the streams from the subscriber VLANs for bandwidth and security reasons.

2.7.4.1 MVR Configuration

This page sets MVR State, Multicast VLAN ID, Source Port and Receive Port for MVR configuration.

MVR State: globally enable or disable MVR on the switch.
Multicast VLAN ID: specify the VLAN group in which multicast data is received. All source ports must be the member of this VLAN. The default VLAN ID is 1.
MVR Mode: choose the mode between **compatible** and **dynamic**.
Compatible mode: the switch does not send out any IGMP reports to source port(s), a manual multicast forwarding configuration is needed. In the case that MVR Group is not configured, multicast data received by the switch is forwarded to all ports, regardless of the port MVR membership setting. In the case that MVR Group is successfully configured, the multicast data is forwarded only to those joined receiver ports set by MVR static configuration.
Dynamic mode: the switch sends IGMP leave and join reports through the source port(s) to the other multicast devices (such as multicast routes or servers) in the multicast VLAN. This allows the multicast devices to update the multicast forwarding

table to forward or not to forward multicast traffic to the receiver ports.
Source Port: configure uplink ports that receive and send multicast data as source ports. Subscribers cannot be directly connected to source ports. All source ports on a switch are members of the single multicast VLAN group.
Receive Port: configure a port as a receiver port if it is a subscriber port and should receive multicast data. However, it won't be able to receive the multicast data until it becomes a member of the multicast group, either statically or by using IGMP join messages. Receiver ports are untagged members of the multicast VLAN group.

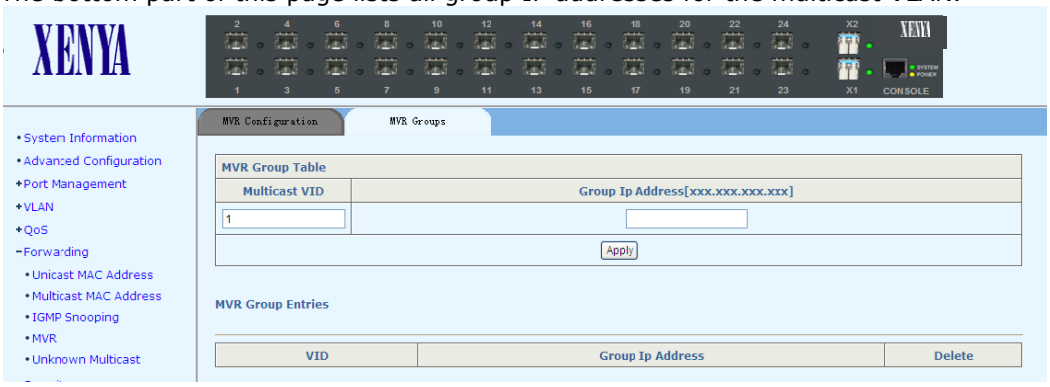


2.7.4.2 MVR Groups

This page sets specific static **Group IP Address(es)** for MVR.

Multicast VID: multicast VLAN ID
Group IP Address: static IP multicast address to be added

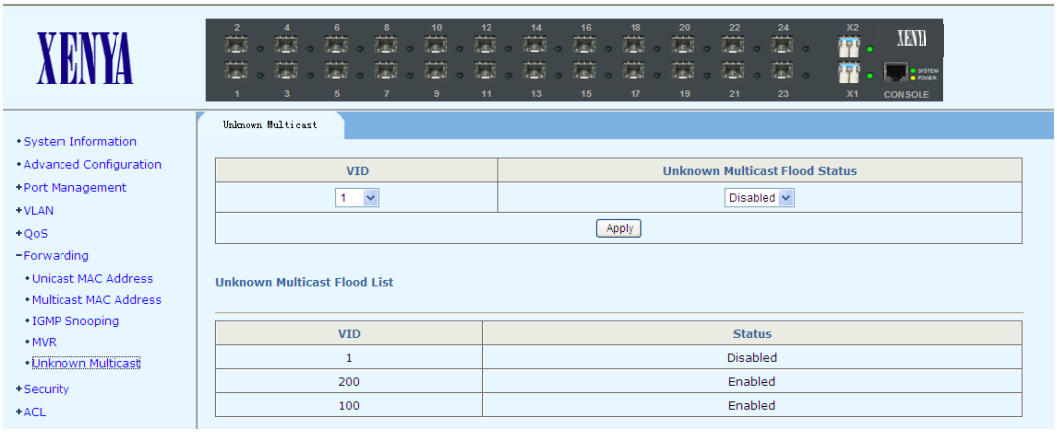
The bottom part of this page lists all group IP addresses for the multicast VLAN.



2.7.5 Unknown Multicast

Unknown Multicast Flood Status: Enable/disable Unknown Multiscast Flood Status for this VLAN group.

The bottom part of this page lists all of the unknown multicast flood

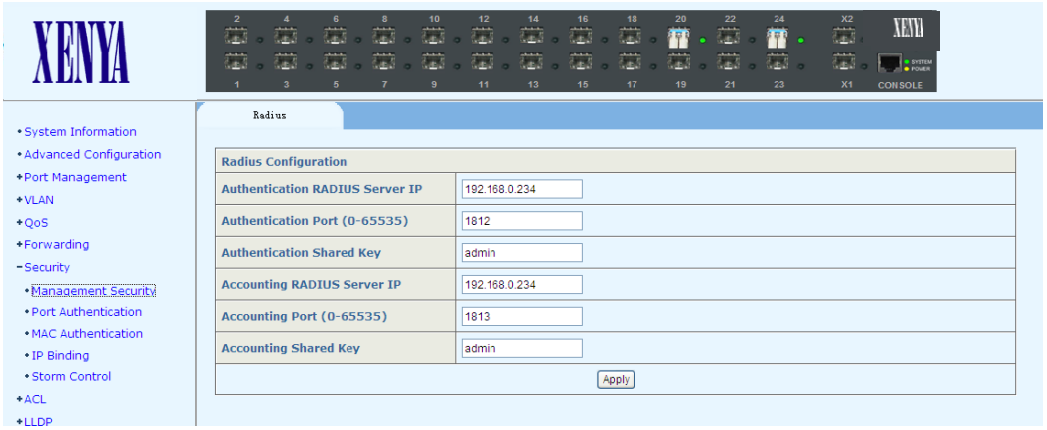


2.8 Security

2.8.1 Management Security

This page configures the 802.1x system as follows: **Authentication RADIUS Server IP**, **Authentication Port**, **Authentication Shared Key, Accounting RADIUS Server IP, Accounting Port** and **Accounting Shared Key**.

Authentication RADIUS Server IP: IP address of the radius server to be used, a valid unicast address in dotted decimal notation; the default value is 192.168.0.234.
Authentication Port: UDP port number of the radius server, ranging from 0 to 65535; the default value is 1812.
Authentication Shared Key: sets a shared key for radius messages. String length is from 1 to 15 characters.
Accounting RADIUS Server IP: IP address of accounting radius server to be used, a valid unicast address in dotted decimal notation; the default value is 192.168.0.234.
Accounting Port: UDP port number of the radius server, ranging from 0 to 65535; the default value is 1813.
Accounting Shared Key: sets a shared key for accounting radius. String length is from 1 to 15 characters.



2.8.2 Port Authentication

There are two tag pages on this webpage for the user to configure various parameters of 802.1x.

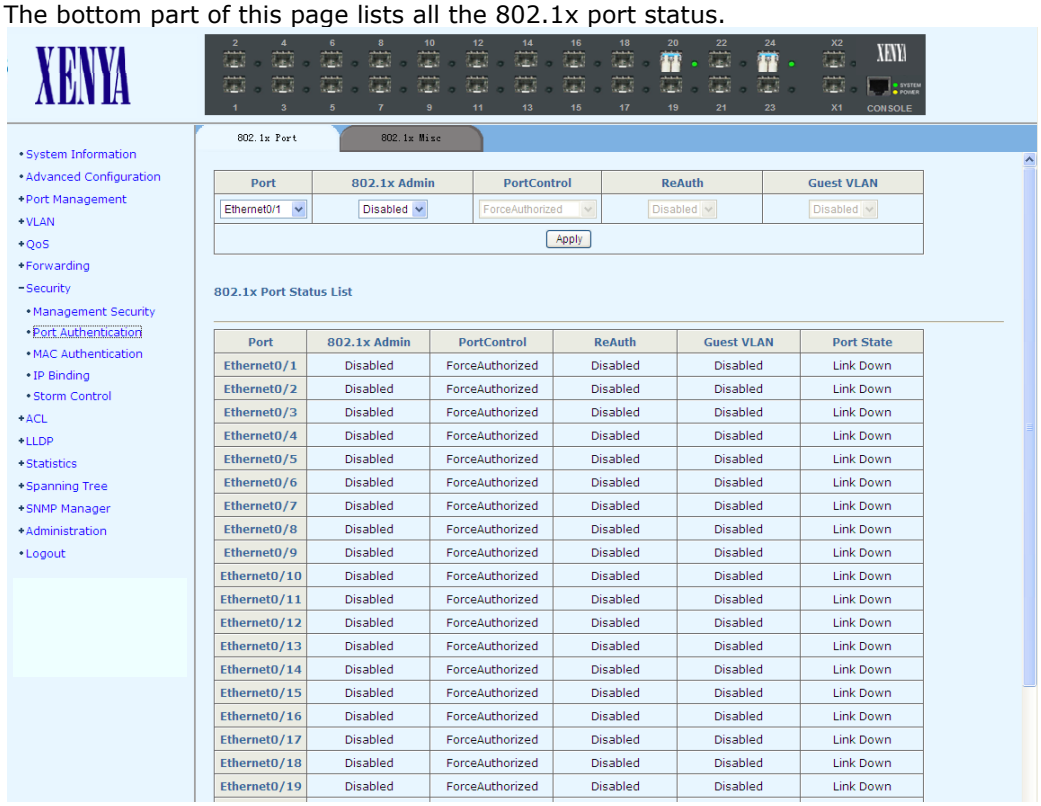
2.8.2.1 802.1x Port

This tag page sets 802.1x port enabling, re-authentication, access control, and Guest VLAN for a specified Ethernet port. There are three choices for **PortControl**: **Auto**, **ForceAuthorized**, and **ForceUnauthorized**.

Auto: specified to operate in auto access control mode. When one port operates in this mode, all the unauthenticated hosts connected to it are unauthorized. In this case, only EAPoL packets can be exchanged between the switch and the hosts. And the authenticated hosts connected to the port are authorized to access the network resources.
ForceAuthorized: specified to operate in authorized-force access control mode. When one port operates in this mode, all the hosts connected to it can access the network resources without the need of authentication.
ForceUnauthorized: specified to operate in unauthorized-force access control mode. When one port operates in this mode, the hosts connected to it cannot access the network resources.

Guest VLAN: a guest VLAN can be enabled for each IEEE 802.1x port on the switch to provide limited services to the clients.

The bottom part of this page lists all the 802.1x port status.



2.8.2.2 802.1x Misc

This tag page configures 802.1x: **Quiet Period**, **Tx Period**, **Supplicant Timeout**, **Server Timeout**, **Max Request Count**, **Reauth Period, and Guest VLAN**.

Quiet Period: this timer sets the quiet-period. When a supplicant system fails to pass the authentication, the switch quiets for the set period before it processes another authentication request re-initiated by the supplicant system. During this quiet period,

the switch does not perform any 802.1x authentication-related actions for the supplicant system. The value is in the range of 1 to 65535, and is set to 60 seconds by default.

Tx Period: sets the transmission timer. This timer sets the tx-period and is triggered in two cases. The first case is when the client requests authentication. The switch sends a unicast request/identity packet to a supplicant system and then triggers the transmission timer. The switch sends another request/identity packet to the supplicant system if it does not receive the reply packet from the supplicant system when this timer times out. The second case is when the switch authenticates the 802.1x client which cannot request for authentication actively. The switch sends multicast request/identity packets periodically through the port enabled with 802.1x function. In this case, this timer sets the interval to send the multicast request/identity packets. It is in the range of 1 to 65535; the default value is 30 seconds.

Supplicant Timeout: sets the supplicant system timer. This timer sets the supp-timeout period and is triggered by the switch after the switch sends a request/challenge packet to a supplicant system. The switch sends another request/challenge packet to the supplicant system if the switch does not receive any response from the supplicant system when this timer times out. It is in the range of 1 to 300; the default value is 30 seconds.

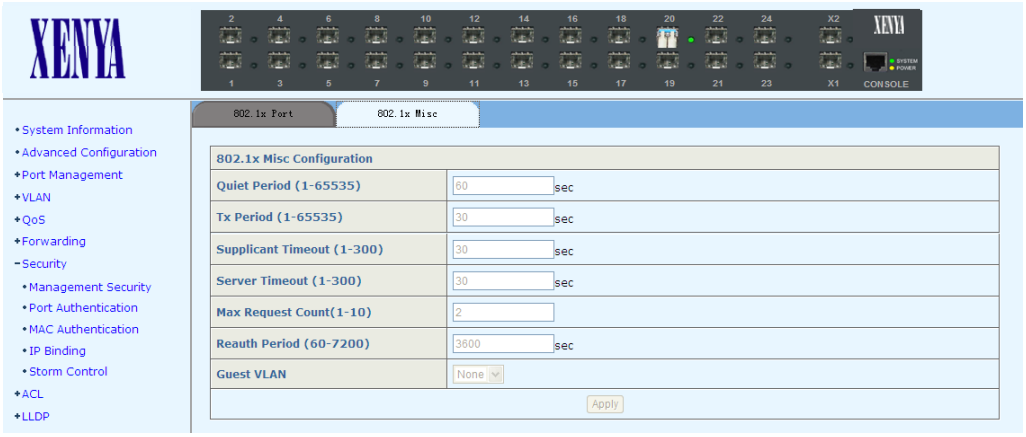
Server Timeout: sets the radius server timer. This timer sets the server-timeout period. After sending an authentication request packet to the radius server, a switch sends another authentication request packet if it does not receive any response from the radius server when this timer times out. It is in the range of 1 to 300; the default value is 30 seconds.

Max Request Count: sets the maximum number of times that a switch sends authentication request packets to a user. It is in the range of 1 to 10, and the default value is 2.

Reauth Period: sets re-authentication interval in seconds. After this timer expires, the switch indicates 802.1x re-authentication. It is in the range of 60 to 7200; the default value is 3600 seconds.

Guest VLAN: can choose a guest VLAN on the switch to provide limited services to clients, such as downloading. These clients might be upgraded for IEEE 802.1x authentication.

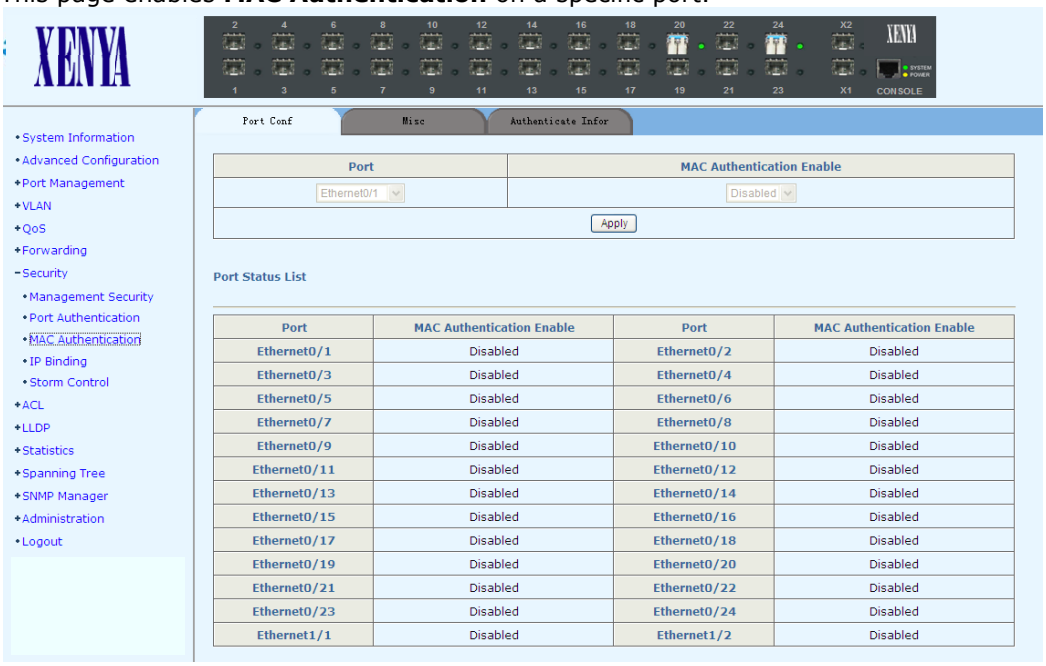
When enabling a guest VLAN on an IEEE 802.1x port, the switch assigns the client port to a guest VLAN in case that the switch does not receive any response to its EAP request/identity frame, or EAPOL packets are not sent by the client. The switch allows the client that is failed in authentication to access the guest VLAN, regardless of whether EAPOL packets have been detected. However, access to external ports out of guest VLAN still needs to be authorized.



2.8.3 MAC Authentication

2.8.3.1 Port Conf

This page enables **MAC Authentication** on a specific port.



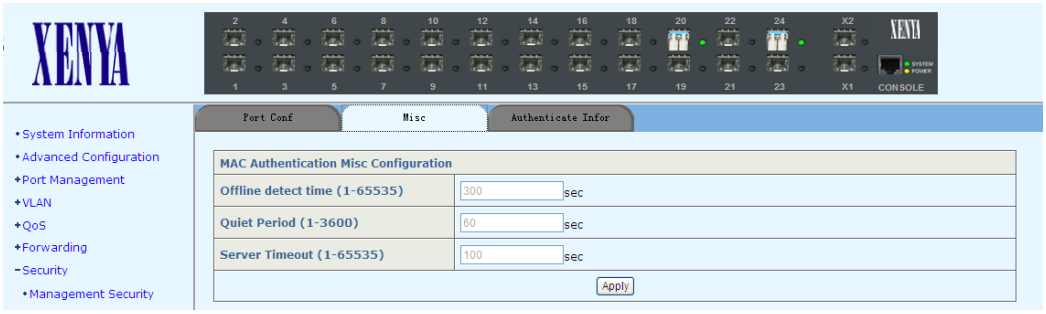
2.8.3.2 Misc

This page sets **Offine detect time**, **Quiet Period,** and **Server Timeout** for MAC Authentication.

Offline detect time: to check whether the client is offline in this time interval. The switch will immediately notify the RADIUS server to stop billing from the client when offline is detected. The value ranges from 1 to 65535, and the default value is 300 seconds.

Quiet Period: to set the time interval the client must wait after a client authentication fails. During this time interval, the switch does not perform the user authentication function. The value ranges from 1 to 3600, and the default value is 60 seconds.

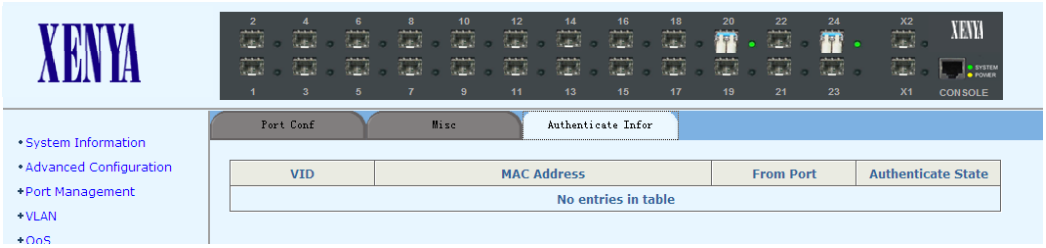
Server Timeout: to set the time interval the switch waits for a response, when there is a connection request from the authentication server to the client. The value ranges from 1 to 65535, and the default value is 100 seconds.



2.8.3.3 Authenticate Infor

This page lists all the MAC authentication information including **MAC Address**, **From**

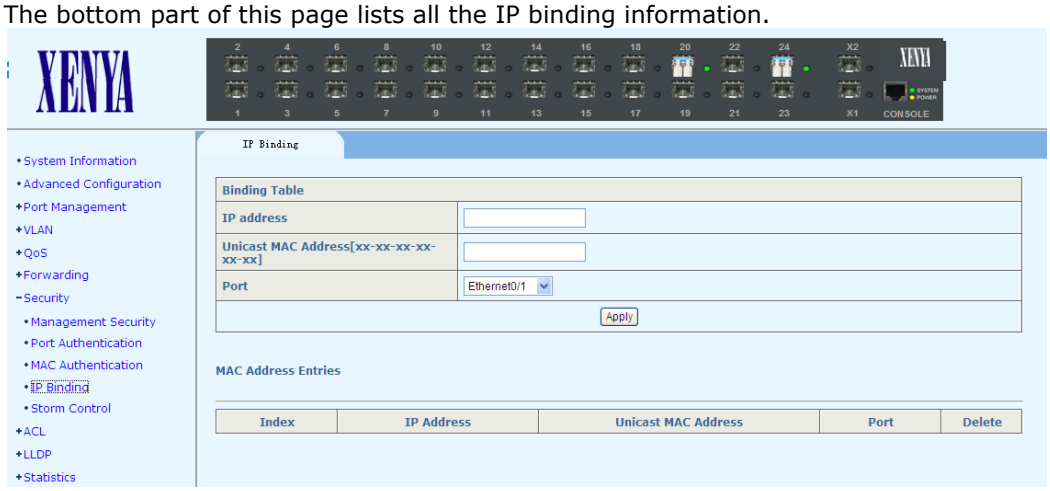
Port, and **Authenticate state**.



2.8.4 IP Binding

This page sets **IP address**, **Unicast MAC Address,** and **Port** for IP binding.

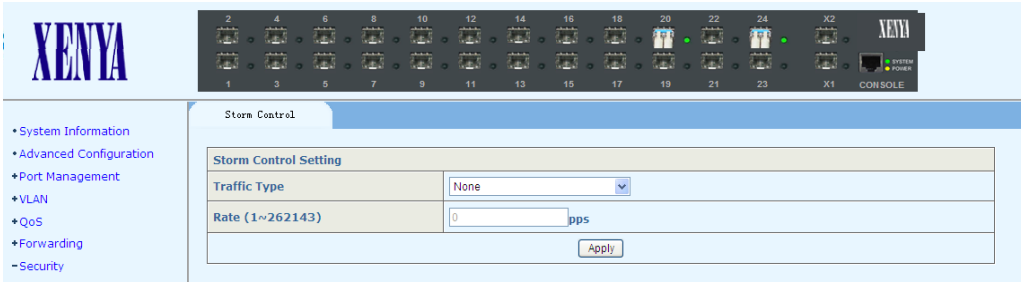
The bottom part of this page lists all the IP binding information.



2.8.5 Storm Control

This page sets thresholds of the specified **Traffic Type**.
Traffic Type can be chosen from **None**, **Broadcast**, **Multicast**, **Destination Lookup Failed (DLF)**, **Broadcast+Multicast**, **Broadcast+DLF**, **Multicast+DLF**, and **Broadcast+Multicast+DLF**.

The Rate is in the range from 1 to 262143.
By default, suppress no traffic type.



2.9 ACL

ACL(Access Control List) is used to achieve the packet filtering function by the configuration of matching rules and processing operation(s). An ACL is a sequential

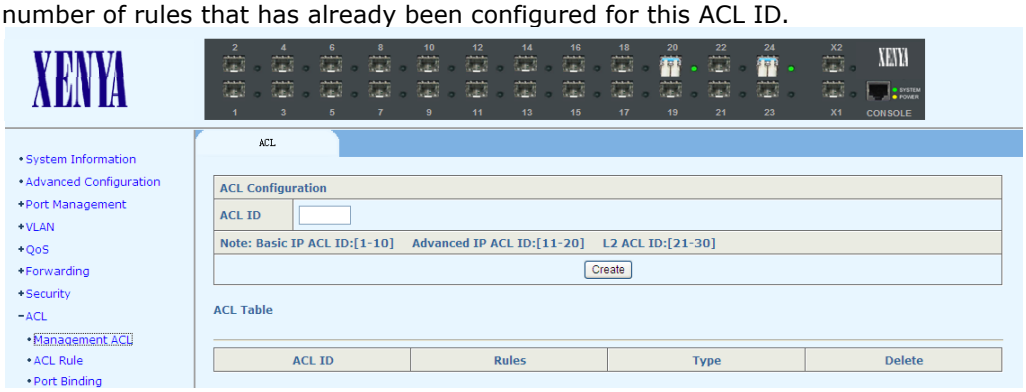
collection of permit and deny conditions that apply to packets. When a packet is received on an interface, the switch compares the fields in the packet against any applied ACLs to verify that the packet has the required permissions to be forwarded, based on the criteria specified in the access lists.

There are three types of ACL:
Basic IP ACL: filtering packets only based on source IP address.
Advance IP ACL: filtering packets based on source IP address, destination IP address, IP protocol type, and more.
L2 ACL: filtering packets based on source MAC address, destination MAC addresses, 802.1p priority, and L2 protocol type.

2.9.1 Management ACL

In order to flexibly configure ACL rule, the ACL ID is divided into three segments: 1-10 for Basic IP ACL, 11-20 for Advanced IP ACL, and 21-30 for L2 ACL. **ACL Rule** page sets different ACL rules based on the range of ACL ID.

The bottom part of this page lists all configured ACL IDs. Parameter **Rules** shows the number of rules that has already been configured for this ACL ID.



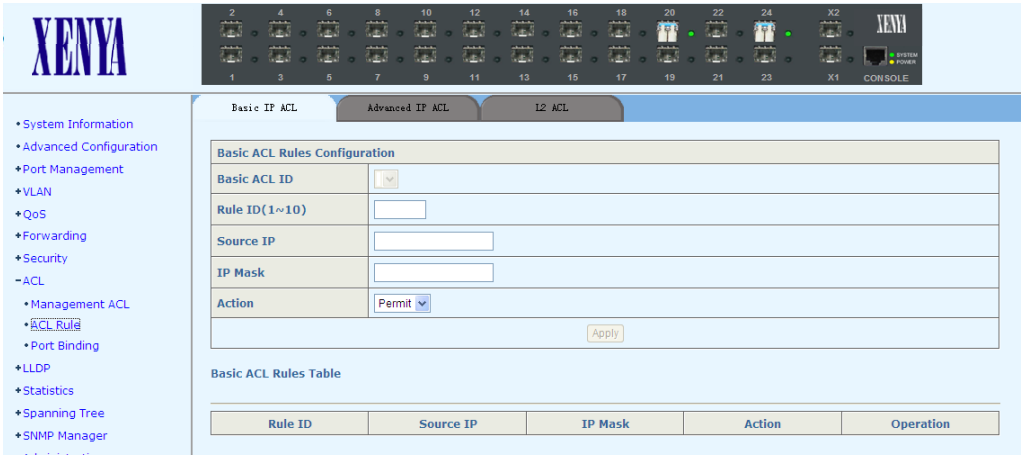
2.9.2 ACL Rule

2.9.2.1 Basic IP ACL

This page sets Basic IP ACL rule s. Up to 10 rules per ACL ID can be set; each rule ID can only be used once. All parameters, **Rule ACL ID**, **Source IP**, and **IP Mask,** must be set, and the **Action** can be **Permit** or **Deny.**

Permit: permit the access of rule matched IP**.**
Deny: Deny the access of rule matched IP**.**

The bottom part of this page lists all configured Basic IP ACL rules.

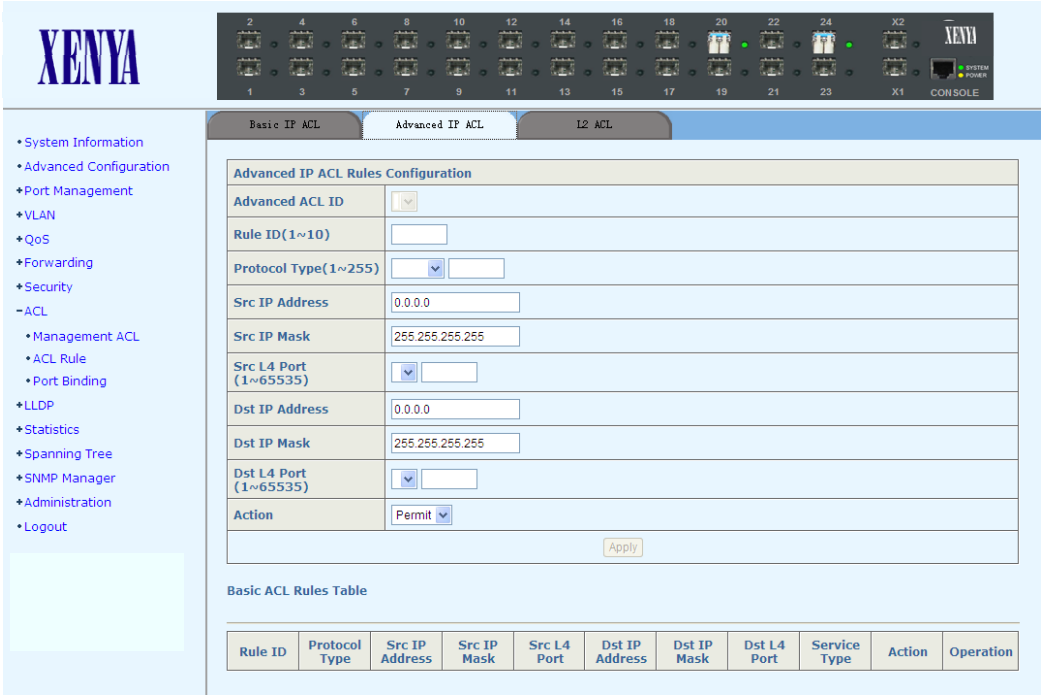


2.9.2.2 Advanced IP ACL

This page sets ACL rules based on packet Src IP Address, Dst IP Address, IP Protocol type and other protocol features, such as TCP or UDP source port, destination port, ICMP protocol message types etc.

Rule ID: identification of the ACL rule.
Protocol Type: an existing protocol type such as Icmp, igmp, Udp, Tcp, Ospf, or an interger between 1 and 255.
Src IP Address: source host IP address.
Src IP Mask: source host IP subnet mask.
Src L4 Port: TCP/UDP source port, an existing Echo, Frp, telnet, Smtp, WWW, or an integer between 1 to 65535. It can be set only when protocol type is TCP or UDP.
Note: IETF IANA defines three groups of ports: Well Known Ports (0-1023), Registered Ports (1024-49151), and Dynamic and/or Private Ports (49152-65535).
Dst IP Address: destination host IP address.
Dst IP Mask: destination host IP subnet mask
Dst L4 Port: TCP/UDP destination port, an existing Echo, Frp, telnet, Smtp, WWW, or an integer 1-65535. It can be set only when protocol type is TCP or UDP.
Action: permit or deny access of the package with matched rules**.**

The bottom part of this page lists all configured Advanced IP ACL rules.



2.9.2.3 L2 ACL

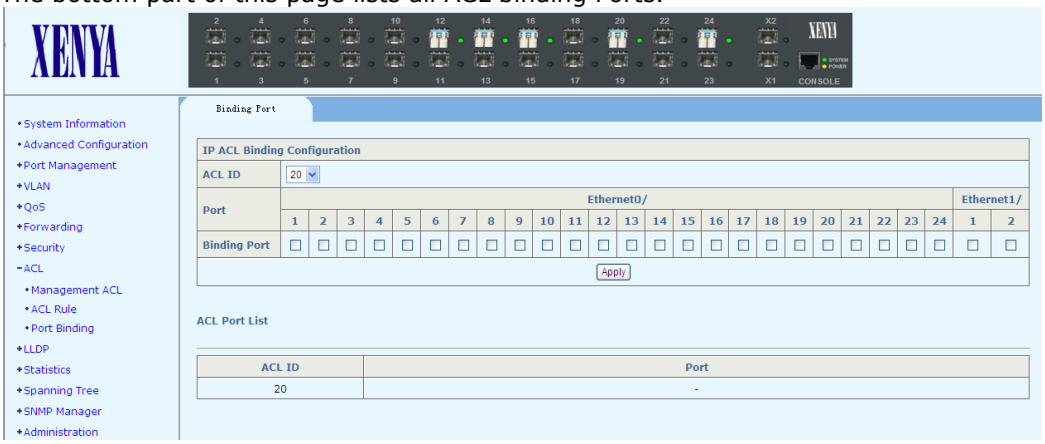
This page sets **Src MAC Address, Src MAC Address Mask, Dst Mac Address, and Dst MAC address Mask**, and the **Action that** can be selected as **Permit** or **Deny.**
Rule ID: Identification the ACL rule.
Src MAC Address: source host mac address.
Src MAC Address Mask: source host mac address mask.
Dst MAC Address: destination host mac address.
Dst MAC address Mask: destination host mac address mask.
Action: permit or deny the access for the package with matched rules**.**

The bottom part of this page lists all configured L2 ACL rules.

2.9.3 Port Binding

This page sets the binding of an Ethernet port to a specified ACL ID. If a port is bound, it will take effect on all the rules associated to this ACL ID.

The bottom part of this page lists all ACL binding Ports.



2.10 LLDP

LLDP (Link Layer Discovery Protocol) defines a standard way for an Ethernet device to advertise its information to its network neighbors and to store the information discovered from other devices, as described in IEEE 802.1AB.

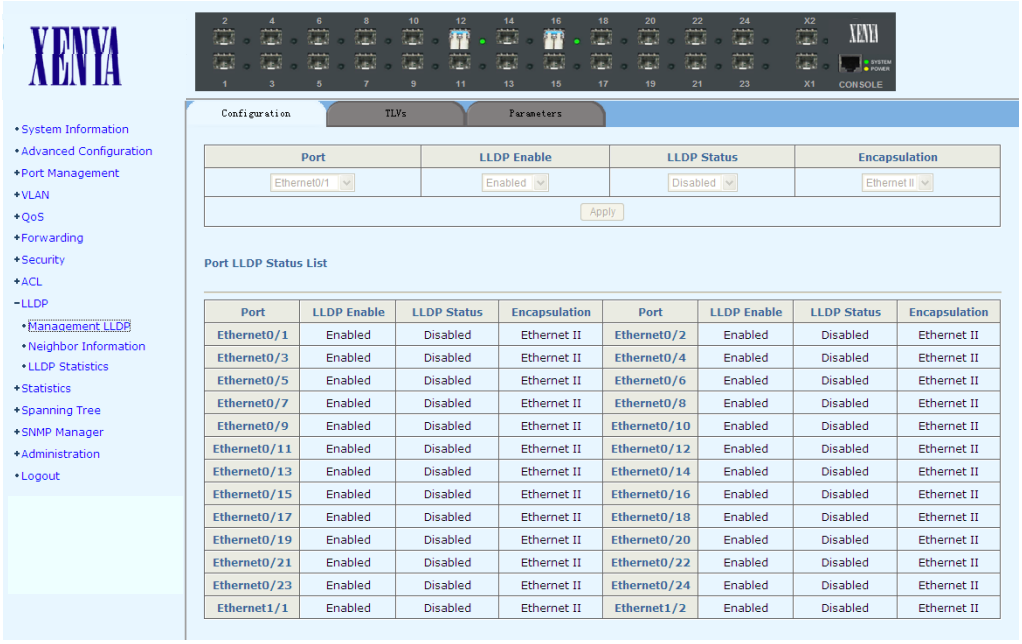
2.10.1 Management LLDP

2.10.1.1 Configuration

This page configures LLDP enabling, sets transmit LLDP information mode from **Disabled**, **Rx and Tx,Tx only, Rx only,** and also specifies the LLDP **Encapsulation** to be **ethernetII** or **SNAP** for a specified Ethernet port.

EthernetII: the Ethernet frame of type 0x88cc.
SNAP: the Ethernet frame of type 0xAAAA-0300-0000-88CC.

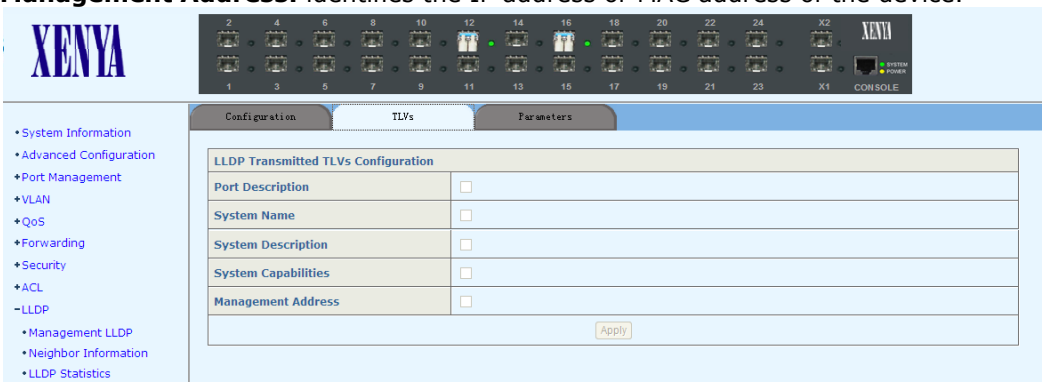
The bottom part of this page lists the LLDP status for all ports.



2.10.1.2 TLVs

This page sets the type of transmitted information: **Port Description, System Name, System Description, System Capability,** and **Management**.

Port Description: identifies information of the interface, including the name of manufacturer, product name, and the version of the interface hardware & software.
System Name: identifies the administratively-assigned name for the device.
System Description: a textual description of the device. This value typically includes the full name and version identification of the system's hardware type, software operating system, and networking software.
System Capability: identifies the capabilities of the device and its primary function (e.g. repeater, Bridge, WLAN, Access Point, Router, Telephone, DOCSIS cable device, Station only, etc.)
Management Address: identifies the IP address or MAC address of the device.

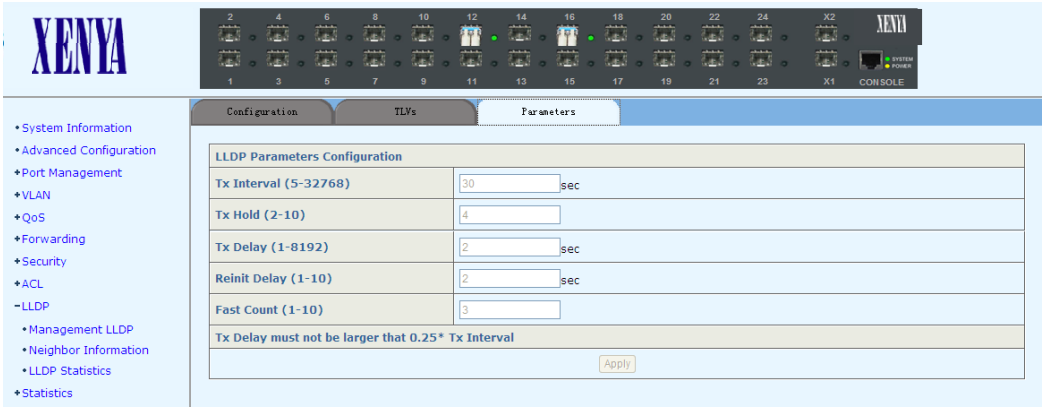


2.10.1.3 Parameters

This page sets LLDP parameters: **TX Interval**, **Tx Hold**, **Tx Delay**, **Reinit Dalay,** and **Fast Count**.

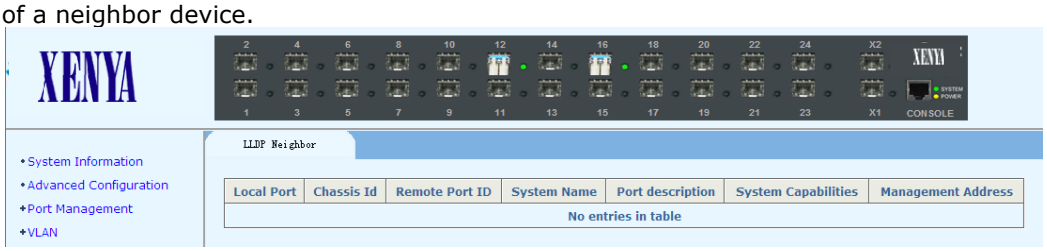
Tx Interval: the time interval between sending LLDP packets. The range is from 5 to

32768 seconds. The default value is 30 seconds.
Tx Hold: TTL multiplier. TTL of TLV carried in LLDPDU is used to set the aging time on the neighbor device. Since TTL of TLV = TTL multiplier × **Tx Interval**, the aging time on the neighbor device can be adjusted by the TTL multiplier. The range of this value is from 2 to 10, and the default value is 4.
Tx Delay: the delay between successive LLDP packets which are initiated by port parameter changes. The range is from 1 to 8192, and the default value is 2.
Reinit Delay: in the case of **LLDP Status** mode change, the port will initialize the protocol state machine, and the switch will need to wait for **Reinit Delay** to be able to start the next initialization. The range of this value is from 1 to 10 seconds, and the default value is 2.
Fast Count: number of fast sending packets. It is in the range of 1 to 10, and the default value is 3.



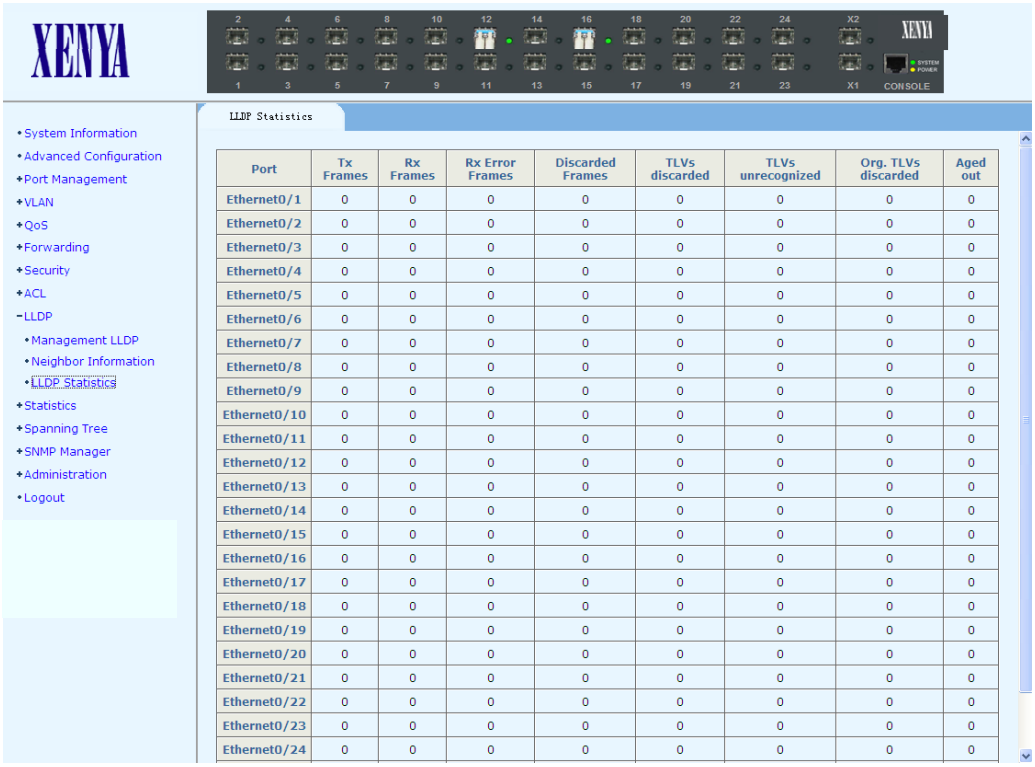
2.10.2 Neighbor Information

This page shows the **Local Port, Chassis Id** of a local device**,** and the **Remote Port ID, System name, Port description, System Capabilities**, and **Management Address** of a neighbor device.



2.10.3 LLDP Statistics

This page shows the statistics **Tx Frames, Rx Frames, Rx Error Frames, Discarded Frames, TLVs discarded, TLVs unrecongnized**, **Org.TLVs discarded,** and **Age out** packet counts of LLDP packets on each Ethernet port.



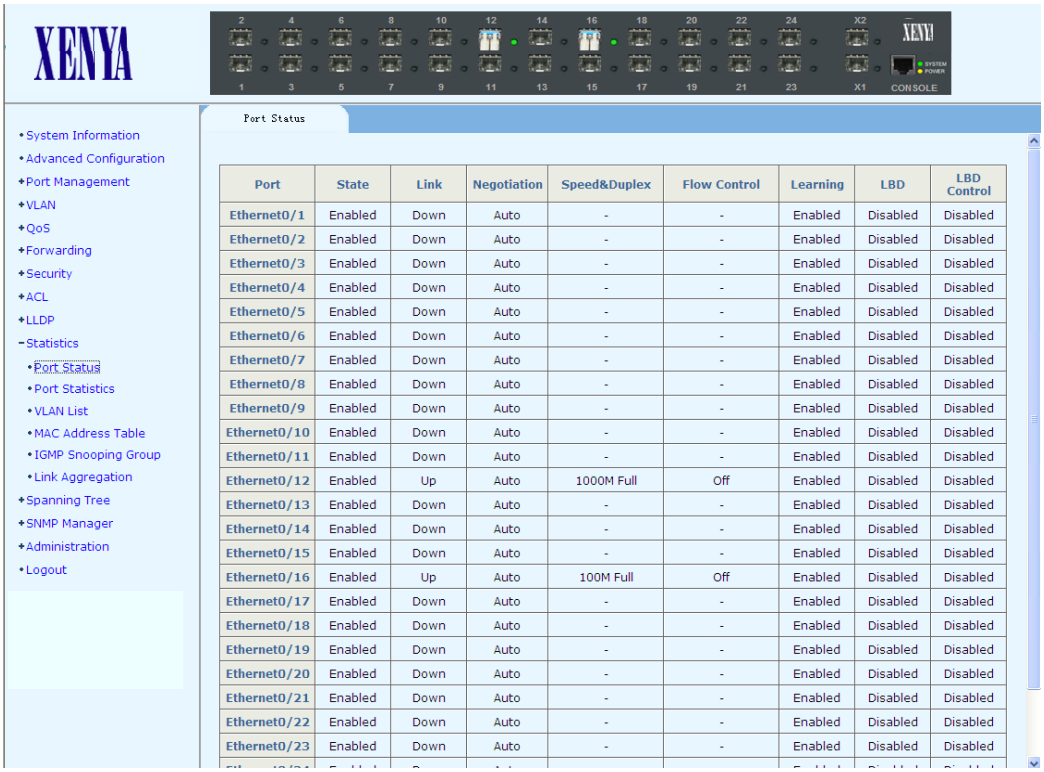
Port	Tx Frames	Rx Frames	Rx Error Frames	Discarded Frames	TLVs discarded	TLVs unrecognized	Org. TLVs discarded	Aged out
Ethernet0/1	0	0	0	0	0	0	0	0
Ethernet0/2	0	0	0	0	0	0	0	0
Ethernet0/3	0	0	0	0	0	0	0	0
Ethernet0/4	0	0	0	0	0	0	0	0
Ethernet0/5	0	0	0	0	0	0	0	0
Ethernet0/6	0	0	0	0	0	0	0	0
Ethernet0/7	0	0	0	0	0	0	0	0
Ethernet0/8	0	0	0	0	0	0	0	0
Ethernet0/9	0	0	0	0	0	0	0	0
Ethernet0/10	0	0	0	0	0	0	0	0
Ethernet0/11	0	0	0	0	0	0	0	0
Ethernet0/12	0	0	0	0	0	0	0	0
Ethernet0/13	0	0	0	0	0	0	0	0
Ethernet0/14	0	0	0	0	0	0	0	0
Ethernet0/15	0	0	0	0	0	0	0	0
Ethernet0/16	0	0	0	0	0	0	0	0
Ethernet0/17	0	0	0	0	0	0	0	0
Ethernet0/18	0	0	0	0	0	0	0	0
Ethernet0/19	0	0	0	0	0	0	0	0
Ethernet0/20	0	0	0	0	0	0	0	0
Ethernet0/21	0	0	0	0	0	0	0	0
Ethernet0/22	0	0	0	0	0	0	0	0
Ethernet0/23	0	0	0	0	0	0	0	0
Ethernet0/24	0	0	0	0	0	0	0	0

2.11 Statistics

All the pages in this menu show various statistics information of the switch.

2.11.1 Port Status

This page shows the **State**, **Link**, **Negotiation**, **Speed&Duplex**, **Flow Control**, **Learning** of each Ethernet port.

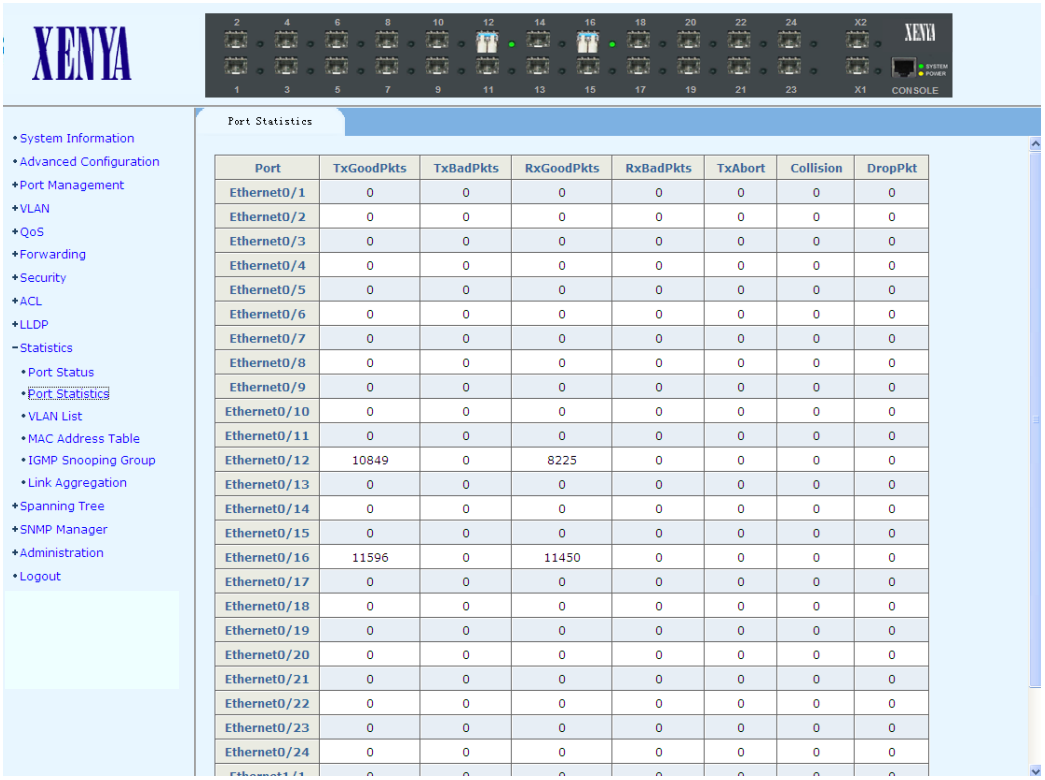


Port	State	Link	Negotiation	Speed&Duplex	Flow Control	Learning	LBD	LBD Control
Ethernet0/1	Enabled	Down	Auto	-	-	Enabled	Disabled	Disabled
Ethernet0/2	Enabled	Down	Auto	-	-	Enabled	Disabled	Disabled
Ethernet0/3	Enabled	Down	Auto	-	-	Enabled	Disabled	Disabled
Ethernet0/4	Enabled	Down	Auto	-	-	Enabled	Disabled	Disabled
Ethernet0/5	Enabled	Down	Auto	-	-	Enabled	Disabled	Disabled
Ethernet0/6	Enabled	Down	Auto	-	-	Enabled	Disabled	Disabled
Ethernet0/7	Enabled	Down	Auto	-	-	Enabled	Disabled	Disabled
Ethernet0/8	Enabled	Down	Auto	-	-	Enabled	Disabled	Disabled
Ethernet0/9	Enabled	Down	Auto	-	-	Enabled	Disabled	Disabled
Ethernet0/10	Enabled	Down	Auto	-	-	Enabled	Disabled	Disabled
Ethernet0/11	Enabled	Down	Auto	-	-	Enabled	Disabled	Disabled
Ethernet0/12	Enabled	Up	Auto	1000M Full	Off	Enabled	Disabled	Disabled
Ethernet0/13	Enabled	Down	Auto	-	-	Enabled	Disabled	Disabled
Ethernet0/14	Enabled	Down	Auto	-	-	Enabled	Disabled	Disabled
Ethernet0/15	Enabled	Down	Auto	-	-	Enabled	Disabled	Disabled
Ethernet0/16	Enabled	Up	Auto	100M Full	Off	Enabled	Disabled	Disabled
Ethernet0/17	Enabled	Down	Auto	-	-	Enabled	Disabled	Disabled
Ethernet0/18	Enabled	Down	Auto	-	-	Enabled	Disabled	Disabled
Ethernet0/19	Enabled	Down	Auto	-	-	Enabled	Disabled	Disabled
Ethernet0/20	Enabled	Down	Auto	-	-	Enabled	Disabled	Disabled
Ethernet0/21	Enabled	Down	Auto	-	-	Enabled	Disabled	Disabled
Ethernet0/22	Enabled	Down	Auto	-	-	Enabled	Disabled	Disabled
Ethernet0/23	Enabled	Down	Auto	-	-	Enabled	Disabled	Disabled

2.11.2 Port Statistics

This page shows the **TxGoodPkts**, **TxBadPkts**, **RxGoodPkts**, **RxBadPkts**, **TxAbort**, **Collision, and DropPkt** of each Ethernet port.

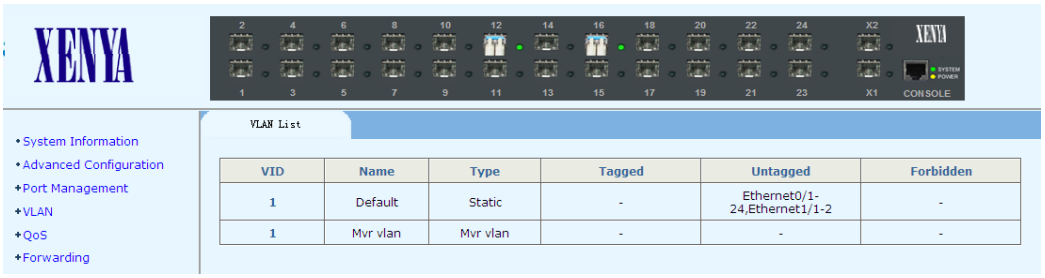
TxGoodPkts: the total number of outgoing normal packets on the port, including outgoing normal packets and normal pause frames.
TxBadPkts: the total byte number of outgoing error frames.
RxGoodPkts: the total number of incoming normal packets on the port, including incoming normal packets and normal pause frames.
RxBadPkts: the total byte number of incoming error frames.
TxAbort: the number of transmission failures due to various reasons, such as collisions.
Collision: the number of detected collisions.
DropPkt: the number of packets dropped for various reasons.



Port	TxGoodPkts	TxBadPkts	RxGoodPkts	RxBadPkts	TxAbort	Collision	DropPkt
Ethernet0/1	0	0	0	0	0	0	0
Ethernet0/2	0	0	0	0	0	0	0
Ethernet0/3	0	0	0	0	0	0	0
Ethernet0/4	0	0	0	0	0	0	0
Ethernet0/5	0	0	0	0	0	0	0
Ethernet0/6	0	0	0	0	0	0	0
Ethernet0/7	0	0	0	0	0	0	0
Ethernet0/8	0	0	0	0	0	0	0
Ethernet0/9	0	0	0	0	0	0	0
Ethernet0/10	0	0	0	0	0	0	0
Ethernet0/11	0	0	0	0	0	0	0
Ethernet0/12	10849	0	8225	0	0	0	0
Ethernet0/13	0	0	0	0	0	0	0
Ethernet0/14	0	0	0	0	0	0	0
Ethernet0/15	0	0	0	0	0	0	0
Ethernet0/16	11596	0	11450	0	0	0	0
Ethernet0/17	0	0	0	0	0	0	0
Ethernet0/18	0	0	0	0	0	0	0
Ethernet0/19	0	0	0	0	0	0	0
Ethernet0/20	0	0	0	0	0	0	0
Ethernet0/21	0	0	0	0	0	0	0
Ethernet0/22	0	0	0	0	0	0	0
Ethernet0/23	0	0	0	0	0	0	0
Ethernet0/24	0	0	0	0	0	0	0

2.11.3 VLAN List

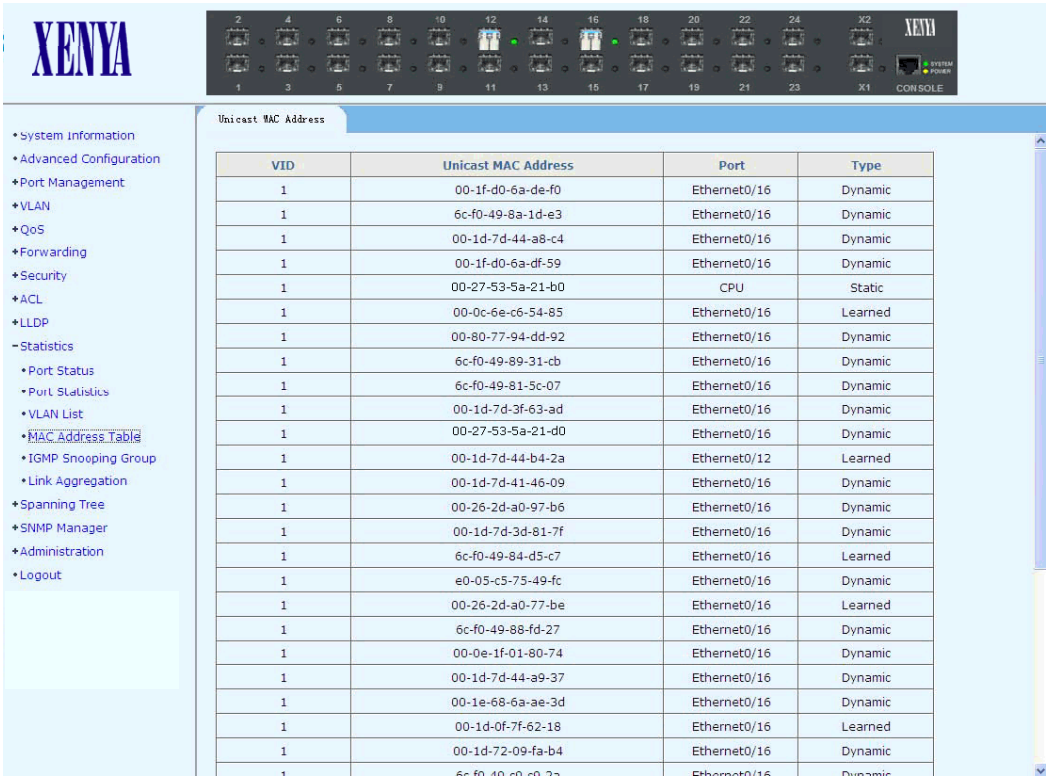
This page lists the information of all VLANs, including **VID**, **Name**, **Type**, **Tagged**, **Untagged**, and **Forbidden**. **Type** includes **Static** or **Dynamic. Tagged** lists all ports out of which packets are sent tagged， **Untagged** lists all ports out of which packets are sent untagged, and **Forbidden** lists all ports that cannot be added to the VLAN group.



VID	Name	Type	Tagged	Untagged	Forbidden
1	Default	Static	-	Ethernet0/1-24,Ethernet1/1-2	-
1	Mvr vlan	Mvr vlan	-	-	-

2.11.4 MAC Address Table

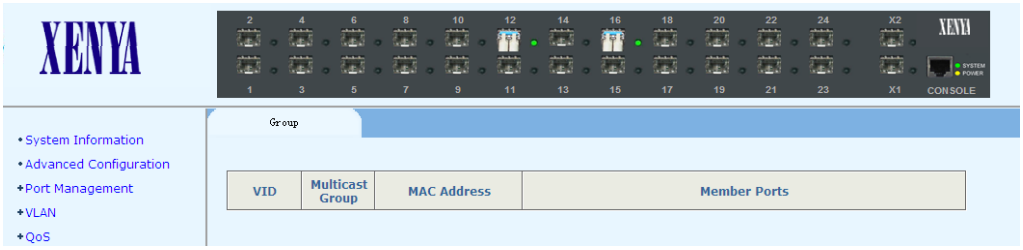
This page shows information of MAC address entries in the MAC address table, including **VID**, **Unicast MAC Address**, **Port**, and **Type**. **Type** includes **Dynamic**, **Static**, **Blackhole** or **Learned**.



VID	Unicast MAC Address	Port	Type
1	00-1f-d0-6a-de-f0	Ethernet0/16	Dynamic
1	6c-f0-49-8a-1d-e3	Ethernet0/16	Dynamic
1	00-1d-7d-44-a8-c4	Ethernet0/16	Dynamic
1	00-1f-d0-6a-df-59	Ethernet0/16	Dynamic
1	00-27-53-5a-21-b0	CPU	Static
1	00-0c-6e-c6-54-85	Ethernet0/16	Learned
1	00-80-77-94-dd-92	Ethernet0/16	Dynamic
1	6c-f0-49-89-31-cb	Ethernet0/16	Dynamic
1	6c-f0-49-81-5c-07	Ethernet0/16	Dynamic
1	00-1d-7d-3f-63-ad	Ethernet0/16	Dynamic
1	00-27-53-5a-21-d0	Ethernet0/16	Dynamic
1	00-1d-7d-44-b4-2a	Ethernet0/12	Learned
1	00-1d-7d-41-46-09	Ethernet0/16	Dynamic
1	00-26-2d-a0-97-b6	Ethernet0/16	Dynamic
1	00-1d-7d-3d-81-7f	Ethernet0/16	Dynamic
1	6c-f0-49-84-d5-c7	Ethernet0/16	Learned
1	e0-05-c5-75-49-fc	Ethernet0/16	Dynamic
1	00-26-2d-a0-77-be	Ethernet0/16	Learned
1	6c-f0-49-88-fd-27	Ethernet0/16	Dynamic
1	00-0e-1f-01-80-74	Ethernet0/16	Dynamic
1	00-1d-7d-44-a9-37	Ethernet0/16	Dynamic
1	00-1e-68-6a-ae-3d	Ethernet0/16	Dynamic
1	00-1d-0f-7f-62-18	Ethernet0/16	Learned
1	00-1d-72-09-fa-b4	Ethernet0/16	Dynamic

2.11.5 IGMP Snooping Group

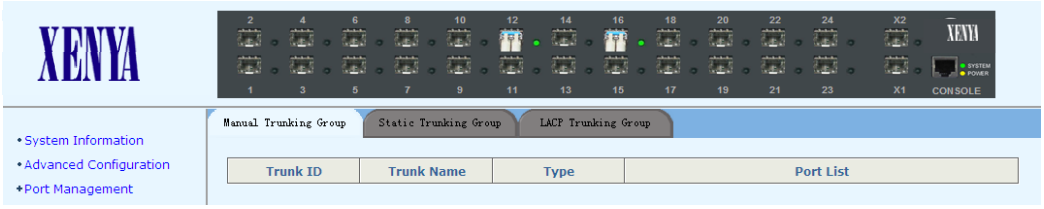
This page shows IGMP Snooping multicast group information, including **VID**, **Multicast Group**, **MAC Address**, and **Member Ports**. **Multicast Group** is the IP address of a multicast group, **MAC Address** is the address of a MAC multicast group, and **Member Ports** include all ports belonging to this IGMP Snooping group.



2.11.6 Link Aggregation

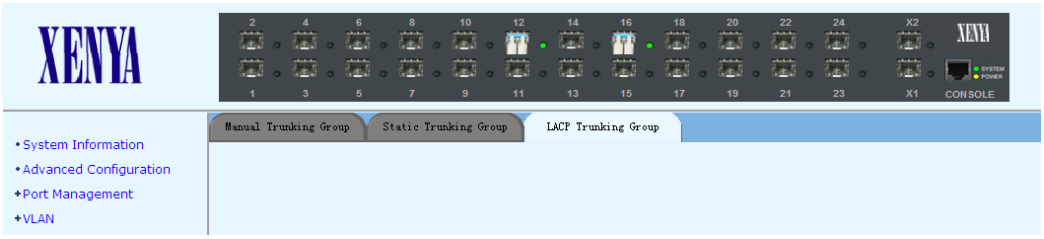
There are three tag pages on this webpage.

Manual Trunking Group: shows manual trunk information, including **Trunk ID**, **Trunk Name**, **Type**, and **Port List**. **Type** is fixed to **Manual**.



Static Trunking Group: shows static trunk information, including **Trunk ID**, **Trunk Name**, **Type**, and **Port List**. **Type** is fixed to **Static**.

LACP Trunking Group: shows LACP trunk information, including **Priority**, **MAC** of Actor and Partner. It also shows the **Key**, priority, **Active** state of member ports.



2.12 Spanning Tree

Spanning Tree Protocol (STP) is a standard protocol described in IEEE 802.1D. Rapid Spanning Tree Protocol (RSTP, IEEE 802.1w) is an evolution of the 802.1D. Multiple Spanning Tree Protocol (MSTP, IEEE 802.1s) is also an evolution of the 802.1D.

2.12.1 Global

Before configuring STP, make sure STP is enabled (see section 2.2 of this manual for details). There is one tag page:

2.12.1.1 Configuration

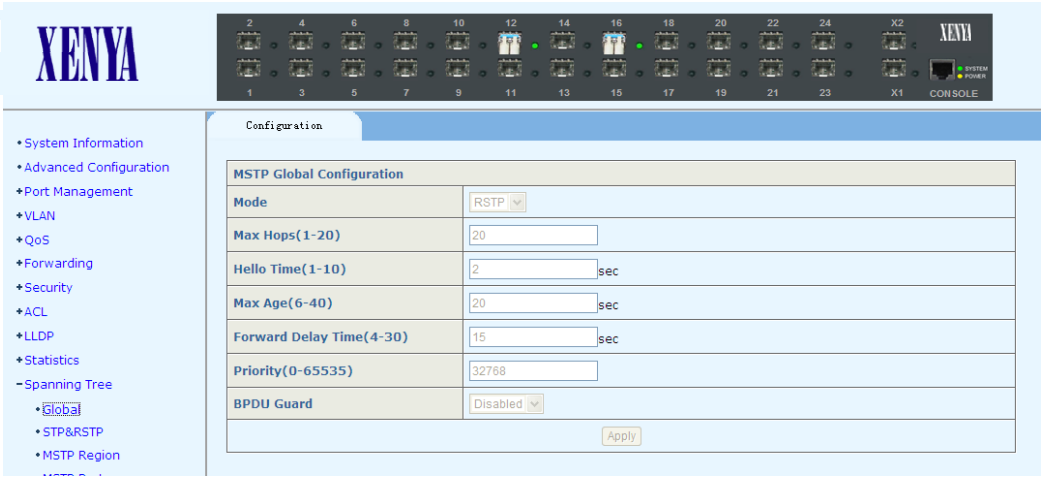
This page sets bridge configurations: **Mode**, **Max Hops**, **Hello Time**, **Max Age**, **Forward Delay Time**, **Priority, and BPDU Guard**.
Mode: Three spanning tree modes are supported: stp, rstp, and mstp.
Max Hops: this value is in the range from 1 to 20, and is 20 by default.
This parameter is used in MSTP mode only to limit the size of MST domain, and the root switch of the instance always sends a BPDU (or M-record) with a cost of 0 and the hop count of the maximum value. When a switch receives this BPDU, it decrements the received remaining hop count by one and propagates this value as the remaining hop count in the BPDUs it generates. When the count reaches zero, the switch discards the BPDU and ages the information held for the port. By default, this value is set to 20.
Hello Time: this value is in the range from 1 to 10 seconds, and is 2 seconds by default. A root bridge regularly sends out configuration BPDUs to maintain the stability of the existing spanning tree. If the switch does not receive a BPDU packet in a specified period,

the spanning tree will be recalculated at BPDU packet times out. When a switch becomes a root bridge, it regularly sends BPDUs at the interval specified by this hello time. A non-root-bridge switch adopts the interval specified by this hello time.
Max Age: this value is in the range from 6 to 40 seconds, and is 20 seconds by default. MSTP is capable of detecting link failures and automatically restoring redundant links to the forwarding state. In CIST, switches use max age parameter to determine whether a received configuration BPDU times out. Spanning trees will be recalculated if a configuration BPDU received by a port times out.
Forward Delay Time: this value is in the range from 4 to 30 seconds, and is 15 seconds by default.

To prevent the occurrence of a temporary loop, when a port changes its state from discarding to forwarding, it undergoes an intermediate state and waits for a specific period of time to synchronize with the state transition of the remote switches. This state transition period is determined by **Forward Delay Time** configured on the root bridge, and applies to all non-root bridges.

As for the configuration of **Hello Time, Forward Delay Time, and Max Age**, the following formulas must be met to prevent frequent network jitter:
2 × (**Forward Delay Time** – 1 second) >= **Max Age**, and **Max Age** >= 2 × (**Hello Time** + 1 second).
Priority: this value is in the range from 0 to 65535, and is 32768 by default. This parameter is used in STP and RSTP modes only.
BPDU Guard: some ports are usually configured as edge ports to achieve rapid transition, while they will resume non-edge ports automatically upon receiving configuration BPDUs, which may cause spanning trees regeneration and network topology jitter.

Normally, no configuration BPDU will reach edge ports, but malicious users can attack a network by sending configuration BPDUs deliberately to edge ports to cause network jitter, which can be prevented by utilizing this BPDU protection function. With this function enabled on a switch, the switch shuts down the edge ports that receive configuration BPDUs and then reports the cases to the network administrator. After a port is shut down, only the administrator can restore it.
By default, the BPDU protection function is disabled.



2.12.2 STP&RSTP

2.12.2.1 Ports Configuration

This page sets STP enabling, Edge Port, P2P, Migration, Tx Hold Count, External Cost,

Priority, and Root Guard for each port, and also can set Path Cost and Priority.

Edge Port: selects **Enabled** to configure the specified Ethernet port as an edge port. By default, all Ethernet ports are non-edge ports.
An edge port is such a port that is directly connected to a user terminal instead of another switch or network segment. Rapid transition to the forwarding state is applied to edge ports, because no loop can be incurred by network topology change on edge ports. The spanning tree protocol allows a port to enter the forwarding state rapidly by setting it to be an edge port, and it is recommended to configure the Ethernet ports connected directly to user terminals as edge ports, so that they may enter the forwarding state immediately.
Normally, configuration BPDUs cannot reach an edge port because the port is not connected to another switch. But, in case that BPDU guard function is disabled on an edge port, configuration BPDUs sent deliberately by a malicious user may reach the port. If an edge port receives a BPDU, it changes itself to be a non-edge port.
P2P: choose from **Force_True**, **Force_False**, and **Auto**.

Force_True: specifies that the link connected to the specified Ethernet port is a point-to-point link.

Force_False: specifies that the link connected to the specified Ethernet port is not a point-to-point link.

Auto: specified to automatically determine whether the link connected to the specified Ethernet port is a point-to-point link.

Protocol **Migration**: For backward compatibility with switches running 802.1d, RSTP selectively sends 802.1d configuration BPDUs and TCN BPDUs on per-port basis.

When a port is initialized, the migration-delay timer is started, and RSTP BPDUs are sent in this time interval. When this timer is active, the switch processes all BPDUs received on the port and ignores the protocol type.

If the switch receives an 802.1d BPDU after the port's migration-delay timer is expired, it assumes that it is connected to an 802.1d switch and starts using only 802.1d BPDUs. However, if the RSTP switch is using 802.1d BPDUs on a port and receives an RSTP BPDU after the timer is timed out, it restarts the timer and starts using RSTP BPDUs on that port.

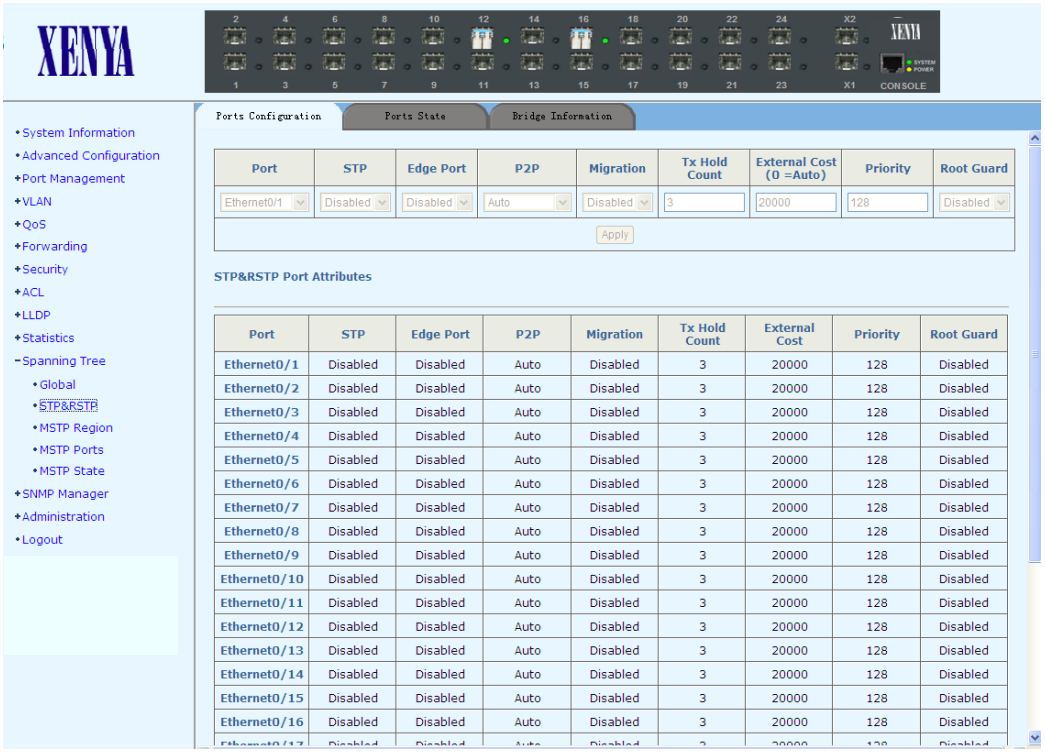
Tx Hold Count: the maximum number of configuration BPDUs a port can send in each Hello time. This argument ranges from 1 to 10 and is 3 by default.

External Cost: sets the path cost of the specified port. It is in the range of 1 to 200000000, the default value is 0 (Auto).

Priority: port priority, it is in the range of 0 to 255; the default value is 128.

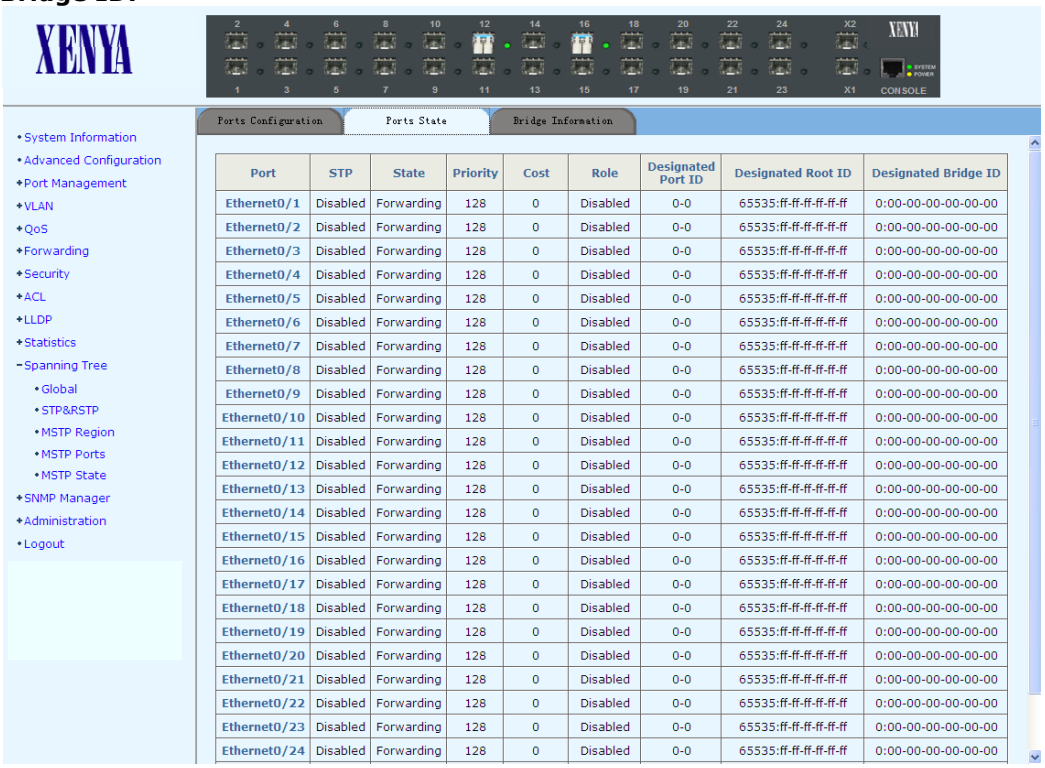
Root Guard: by default, the root protection function is disabled.
Due to configuration error or malicious attack, the root bridge in the network may receive configuration BPDUs with priorities higher than that of a root bridge, which will cause a new root bridge to be elected and network topology jitter will occur. In this case, data flows that should have been transmitted along a high-speed link may be led to a low-speed link.

This problem can be resolved by enabling the root protection function. Root-protection-enabled ports can only be kept as designated ports. When a port of this type receives configuration BPDUs with higher priorities, that is, when it is to become a non-designated port, it turns to the discarding state and stops forwarding packets (as if it were disconnected from the link).



2.12.2.2 Ports State

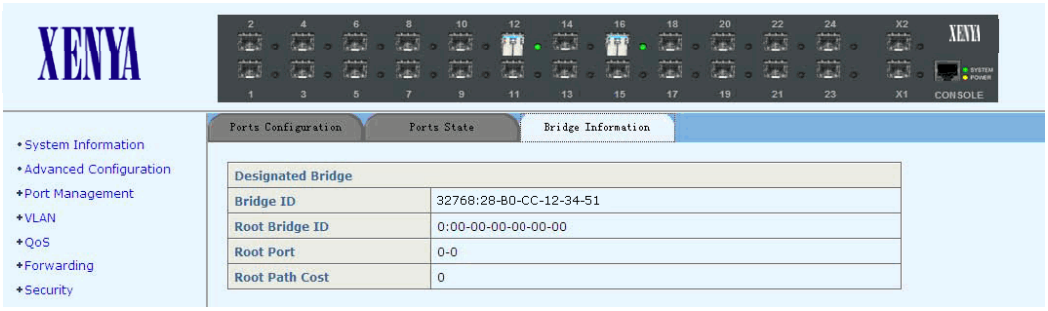
This page lists all port parameters and spanning tree information, including **STP**, **State**, **Priority**, **Cost**, **Role**, **Designated Port ID**, **Designated Root ID**, and **Designated Bridge ID.**



2.12.2.3 Bridge Information

This page lists basic information of **Designated Bridge**, including **Bridge ID**, **Root Bridge ID**, **Root Port**, and **Root Path Cost**.

Bridge ID: ID of this switch.
Root Bridge ID: ID of the root bridge.
Root Port: the spanning tree root port.
Root Path Cost: cost of the path from the switch to the root bridge.



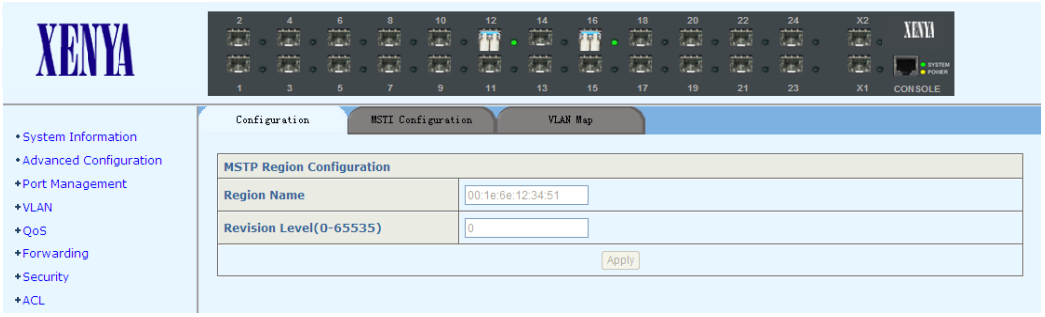
2.12.3 MSTP Region

An MSTP region comprises of one or more MST Bridges with the same MSTP configuration identifier.

2.12.3.1 Configuration

This page sets **Region Name** and **Revision level** of MST configuration Identifiers.

Region Name: a variable length text string of up to 32 octets
Revision level: a 2-octet unsigned integer. It ranges from 0 to 65535.

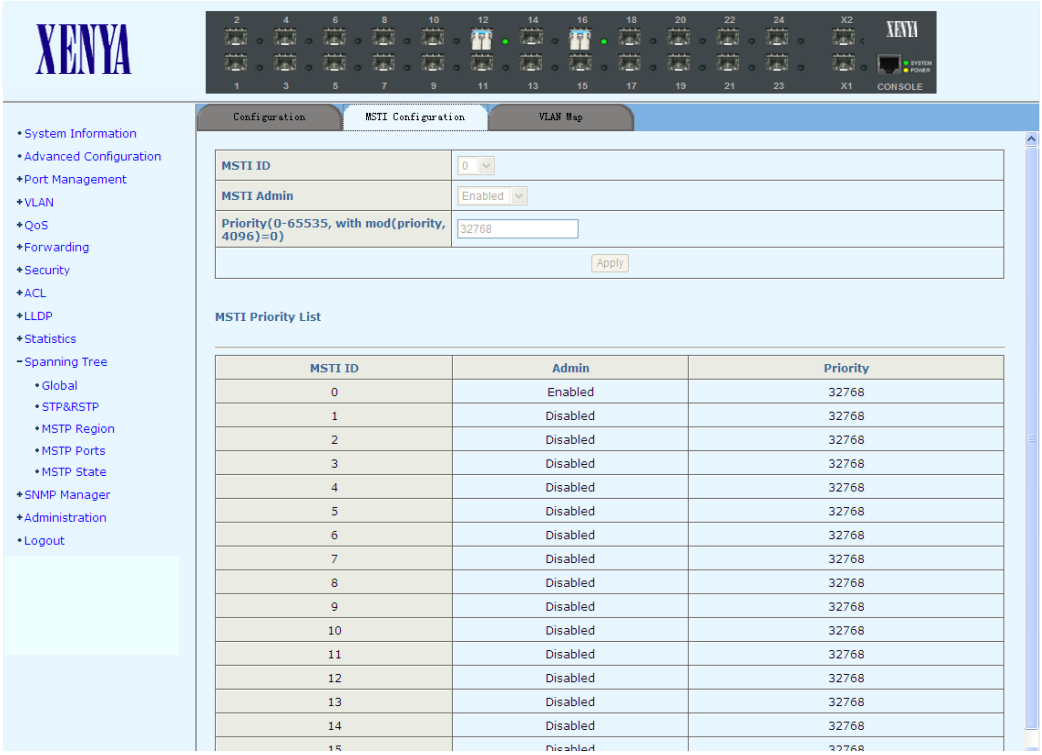


2.12.3.2 MSTI Configuration

This page sets **MSTI ID**, **MSTI Admin,** and **Priority** for each MST instance.

MSTI ID: MSTI identification, ranging from 0 to 15.
MSTI Admin: enable or disable the specified instance.
Priority: sets a priority for the specified instance. It is in the range from 0 to 65535; the default value is 32768.

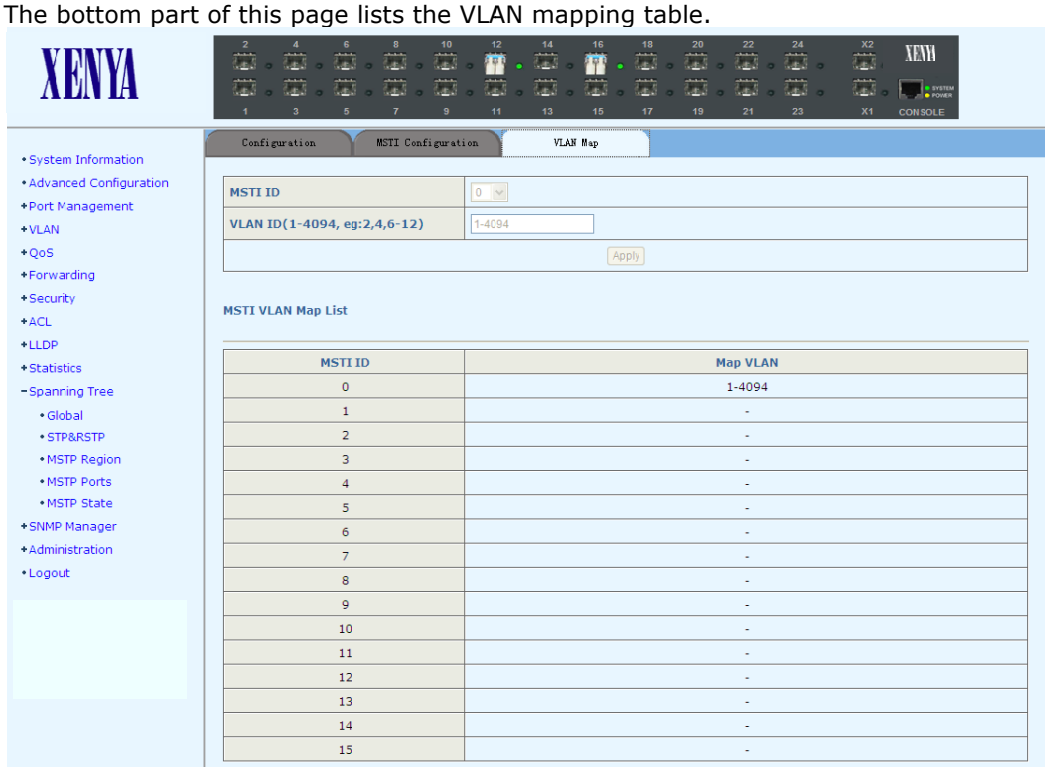
The bottom part of this page lists all MST instances information.



2.12.3.3 VLAN MAP

This page maps one or more VLANs into a specific MST instance. One or more VLANs can be assigned to a spanning-tree instance at a time.

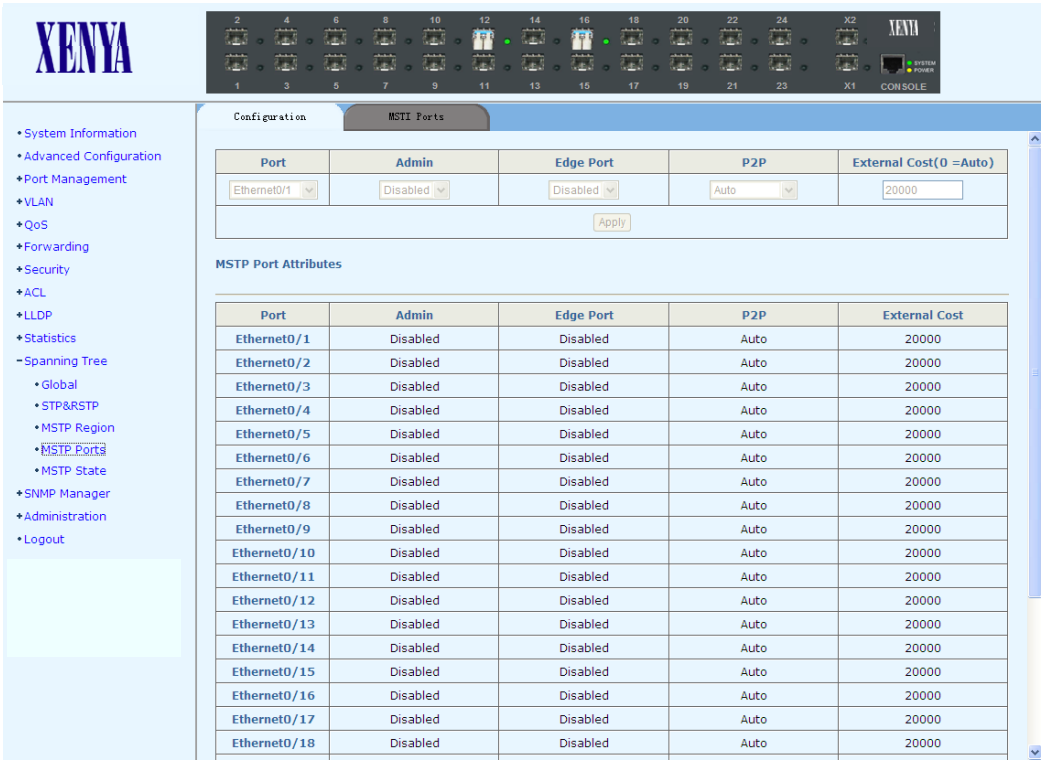
The bottom part of this page lists the VLAN mapping table.



2.12.4 MSTP Ports

2.12.4.1 Configuration

This page enables **Admin**, **Edge Port, P2P,** and **External Cost** for each port.
Similar to STP and RSTP port configuration described in section 2.12.2.1 Ports Configuration, this page sets MSTP port configuration.
The bottom part of this page lists the MSTP attributes for each port.

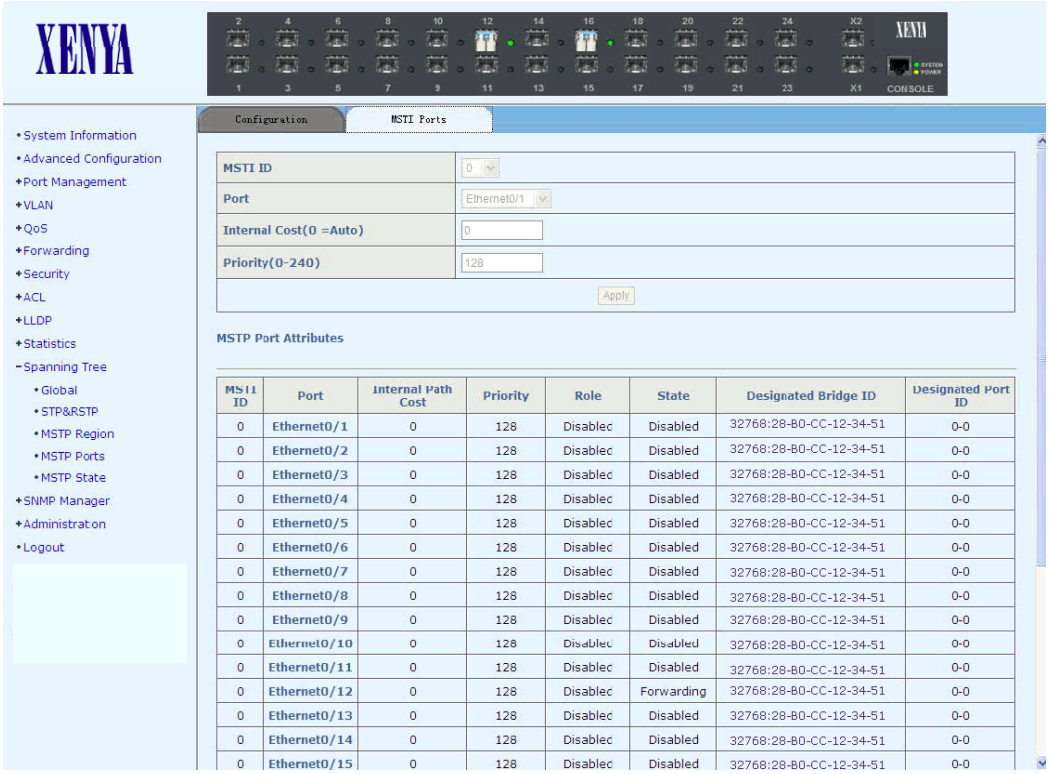


2.12.4.2 MSTI Ports

This page sets the **Internal Cost** and **Priority** for each MST instance.

Internal Cost: sets the path cost of the specified port in a specified MST instance. It is in the range from 1 to 200000000, and the default value is 0 (Auto).
Priority: sets the port priority for the specified port in a specified MST instance. It is in the range from 0 to 240, and the default value is 128.

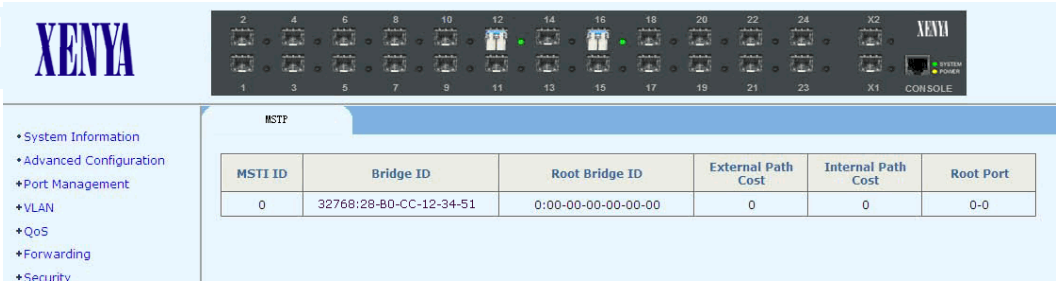
The bottom part of this page lists port parameters and spanning tree information for each MST instance.



MSTI ID	Port	Internal Path Cost	Priority	Role	State	Designated Bridge ID	Designated Port ID
0	Ethernet0/1	0	128	Disablec	Disabled	32768:28-B0-CC-12-34-51	0-0
0	Ethernet0/2	0	128	Disablec	Disabled	32768:28-B0-CC-12-34-51	0-0
0	Ethernet0/3	0	128	Disablec	Disabled	32768:28-B0-CC-12-34-51	0-0
0	Ethernet0/4	0	128	Disablec	Disabled	32768:28-B0-CC-12-34-51	0-0
0	Ethernet0/5	0	128	Disablec	Disabled	32768:28-B0-CC-12-34-51	0-0
0	Ethernet0/6	0	128	Disablec	Disabled	32768:28-B0-CC-12-34-51	0-0
0	Ethernet0/7	0	128	Disablec	Disabled	32768:28-B0-CC-12-34-51	0-0
0	Ethernet0/8	0	128	Disablec	Disabled	32768:28-B0-CC-12-34-51	0-0
0	Ethernet0/9	0	128	Disablec	Disabled	32768:28-B0-CC-12-34-51	0-0
0	Ethernet0/10	0	128	Disablec	Disabled	32768:28-B0-CC-12-34-51	0-0
0	Ethernet0/11	0	128	Disablec	Disabled	32768:28-B0-CC-12-34-51	0-0
0	Ethernet0/12	0	128	Disablec	Forwarding	32768:28-B0-CC-12-34-51	0-0
0	Ethernet0/13	0	128	Disablec	Disabled	32768:28-B0-CC-12-34-51	0-0
0	Ethernet0/14	0	128	Disablec	Disabled	32768:28-B0-CC-12-34-51	0-0
0	Ethernet0/15	0	128	Disablec	Disabled	32768:28-B0-CC-12-34-51	0-0

2.12.5 MSTP State

This page lists spanning tree information: **Bridge ID**, **Root Bridge ID, External Path Cost**, **Internal Path Cost,** and **Root Port** for each MST instance.



MSTI ID	Bridge ID	Root Bridge ID	External Path Cost	Internal Path Cost	Root Port
0	32768:28-B0-CC-12-34-51	0:00-00-00-00-00-00	0	0	0-0

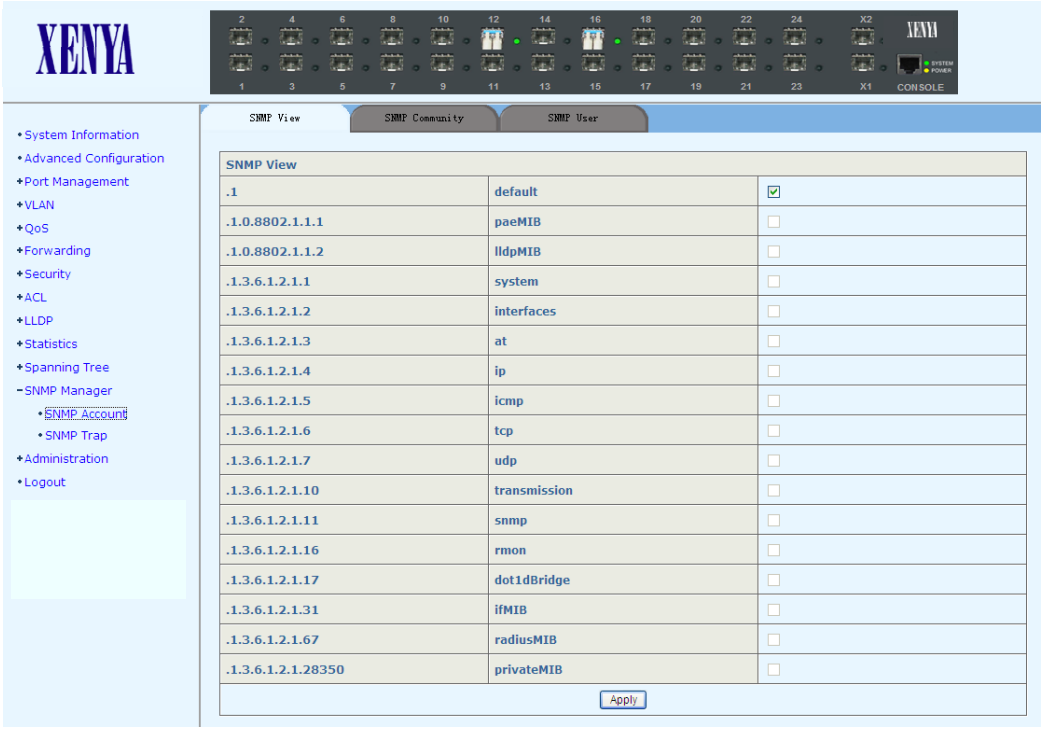
2.13 SNMP Manager

2.13.1 SNMP Account

There are three tag pages: *SNMP View*, *SNMP Community*, and *SNMP User*.

2.13.1.1 SNMP View

This page sets which tree of SNMP-OID can be managed by an SNMP agent user; the default is all of them. For details of which MIBs are supported, please check section 6 "Appendix B: Supported MIBs" of this manual.

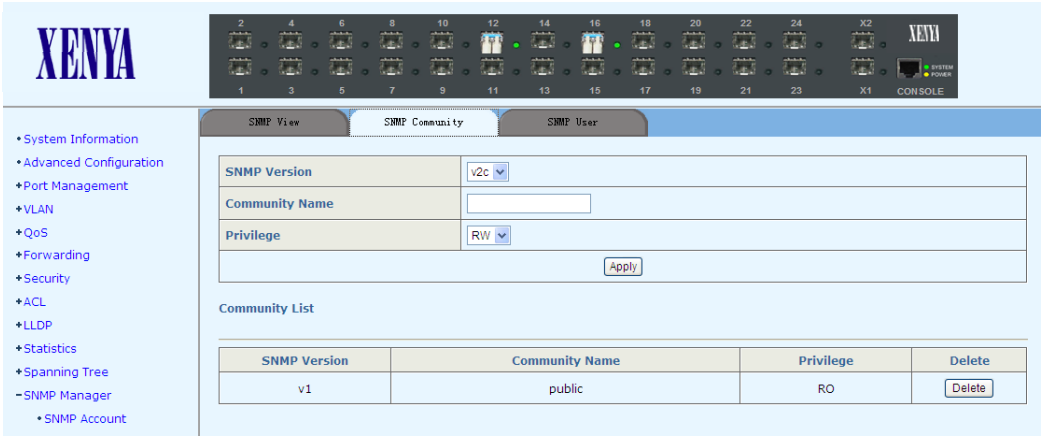


2.13.1.2 SNMP Community

This page sets **SNMP Version** between **v1** and **v2c; Community Name**, and **Privilege** between **RO** and **RW**.

v1: creates an SNMPv1 user.
v2c: creates an SNMPv2c user.
Community Name: name of the community to be created. It is a string of 3 to 16 characters.
RO: specifies that the community to be created has read-only permission to MIB objects. Communities of this type can only query MIBs for device information.
RW: specifies that the community to be created has read-write permission to MIB objects. Communities of this type are capable of configuring devices.

The bottom part of this page lists all existing SNMP v1 and v2c communities, including **SNMP Version**, **Community Name**, and **Privilege**. A community can be deleted.

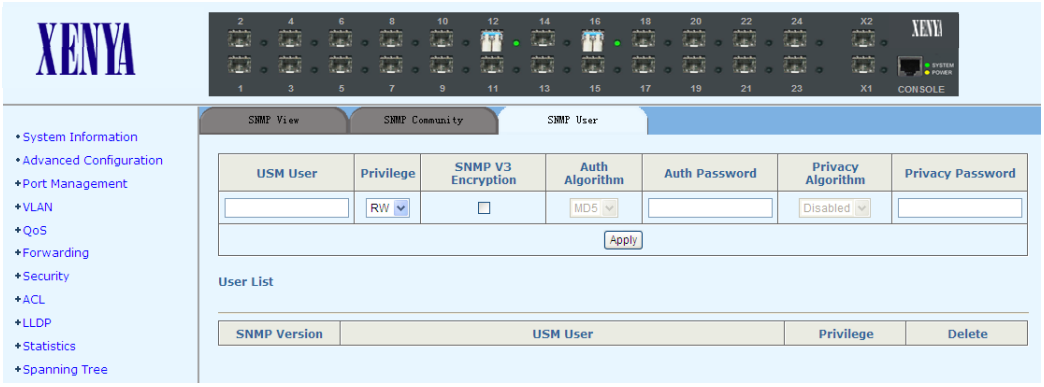


2.13.1.3 SNMP User

This page creates a SNMP v3 user, and sets **USM User**, **Privilege**, **SNMP V3 Encryption**, **Auth Algorithm**, **Auth Password**, **Privacy Algorithm**, and **Privacy Password**.

USM User: username, a string of 3 to 16 characters.
Auth Algorithm: specifies the security mode of authentication. If **SNMP V3 Encryption** is not selected, neither authentication nor encryption will be performed.
MD5: uses HMAC MD5 algorithm for authentication.
SHA: uses HMAC SHA algorithm for authentication, which is more secure than MD5.
Auth Password: Authentication password, a string of 9 to 15 characters in plain text, a 32-bit hexadecimal number in cipher text if MD5 algorithm is used, and a 40-bit hexadecimal number in cipher text if SHA algorithm is used.
Privacy Algorithm: specifies the security mode as encrypted.
DES: specifies the encryption protocol as Data Encryption Standard (DES).
AES: specifies the encryption protocol as Advanced Encryption Standard (AES), which is more secure than DES.
Privacy Password: encryption password, a string of 9 to 15 characters in plain text, a 32-bit hexadecimal number in cipher text if MD5 algorithm is used, and a 40-bit hexadecimal number in cipher text if SHA algorithm is used.

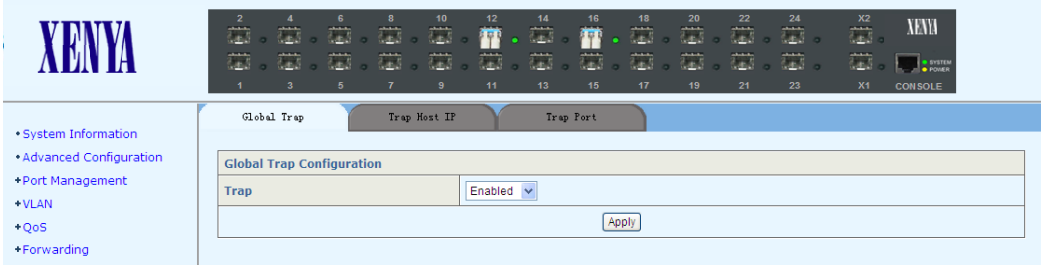
The bottom part of this page lists all existing SNMP v3 USM Users, including **SNMP Version**, **USM User**, and **Privilege**; you can delete any USM User.



2.13.2 SNMP Trap

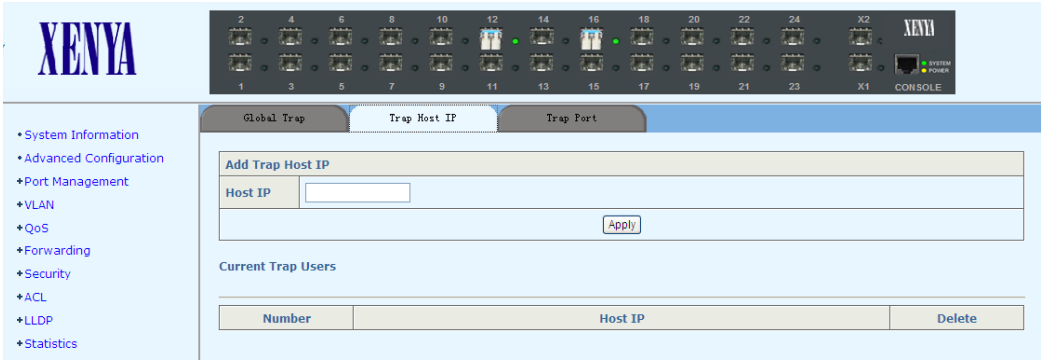
There are three tag pages.

Global Trap: globally disables or enables the trap function; by default, the trap function is enabled.

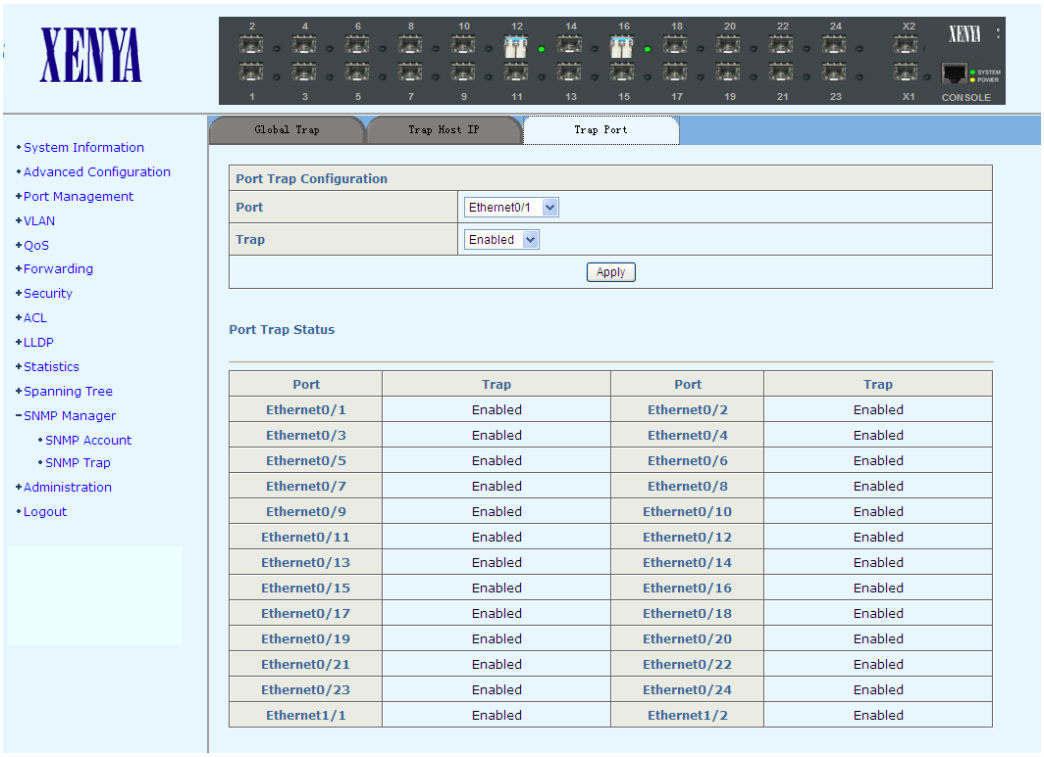


Trap Host IP: specifies SNMP trap Host IP. Host IP is the IPv4 address of the host to receive the traps.
The bottom part of this page lists all existing hosts' IP addresses. You can delete any trap

host IP address.



Trap Port: disables or enables the trap function for each port.
The bottom part of this page lists the trap status of all ports.

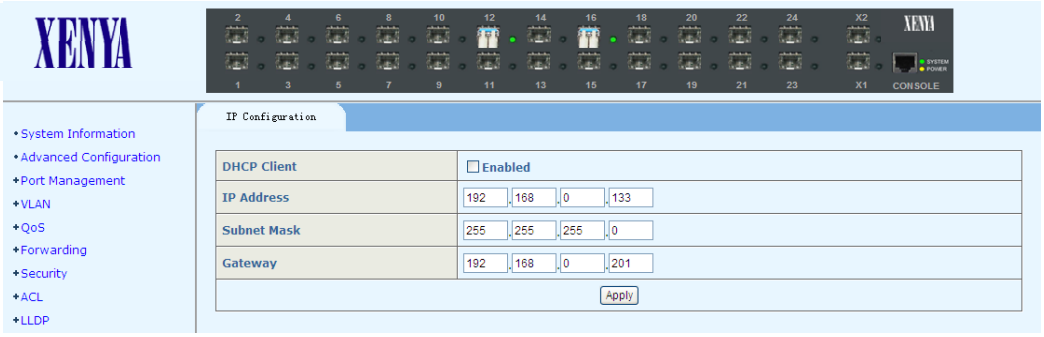


2.14 Administration

This part covers switch management and maintenance functions.

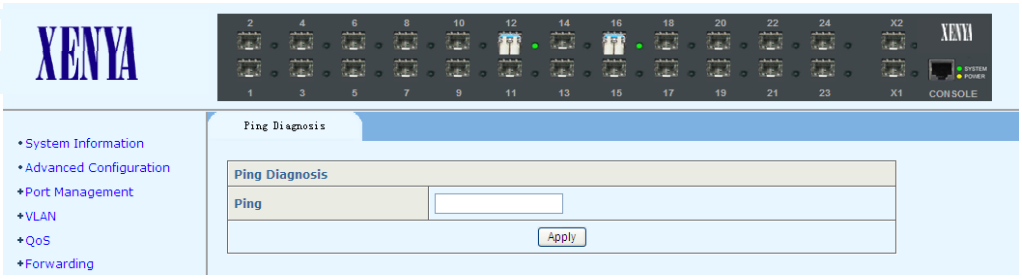
2.14.1 IP Configuration

The managed switch supports DHCP and Static IP. **DHCP Client** can be enabled by checking the **Enabled** checkbox. If static IP is used, **IP Address**, **Subnet Mask**, and **Gateway** shall be specified.



2.14.2 Ping Diagnosis

This page can be used to ping a specific IP address.

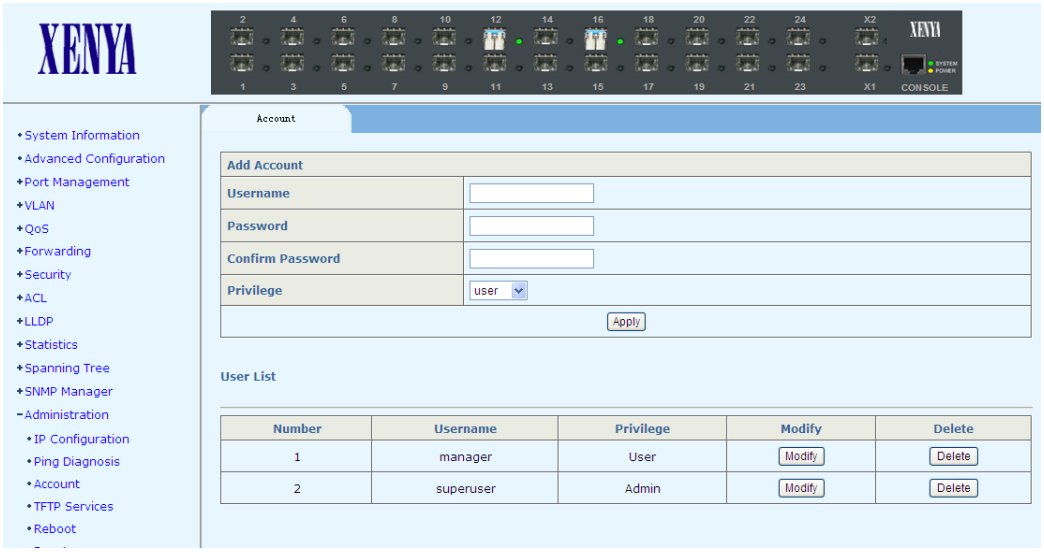


2.14.3 Account

This page can be used to add a new account. **Username**, **Password**, and **Privilege** for the new account are set on this page.
Username: username, a string of 3 to 16 characters.
Password: password, a string of 1 to 16 characters.
Privilege: choose **user** or **admin**.

The bottom part of this page lists all accounts, including **Username** and **Privilege**. An account can be deleted on this page.

Note: check section 3.6 “User Level” of this manual for privilege details of each level of users.

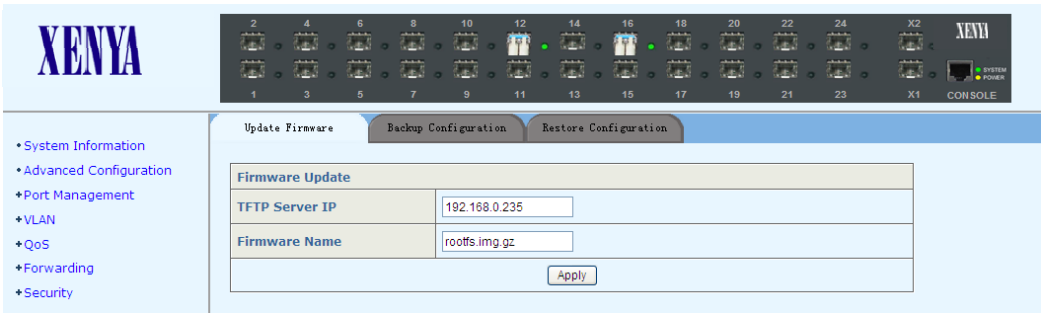


2.14.4 TFTP Services

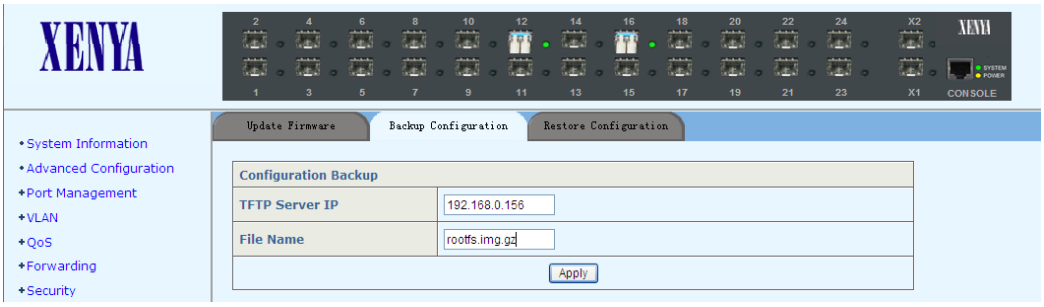
There are three tag pages.

Update Firmware: This page sets a **TFTP Server IP** and **Firmware Name**. Before doing firmware upgrade, make sure the switch is connected to the TFTP server and new firmware file exists on the server. The switch will begin to update firmware after **Apply** button is clicked.

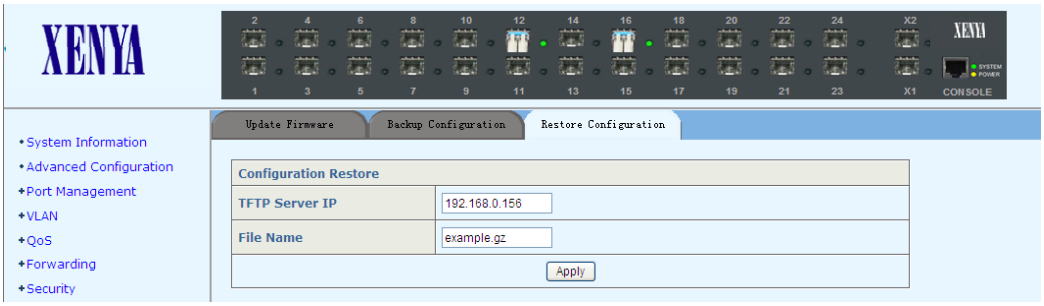
Note: please don't cut off the power supply when updating!



Backup Configuration: This page sets a **TFTP Server IP** and **File Name**. Before backing up configuration, make sure the switch is connected to the TFTP server. The switch configuration file will be uploaded to TFTP server with the specified **File Name** after **Apply** button is clicked.



Restore Configuration: This page sets a **TFTP Server IP** and **File Name**. Before restoring a configuration, make sure the switch is connected to the TFTP server. The switch will download the file with the specified **File Name** and use it as the configuration file after **Apply** button is clicked.

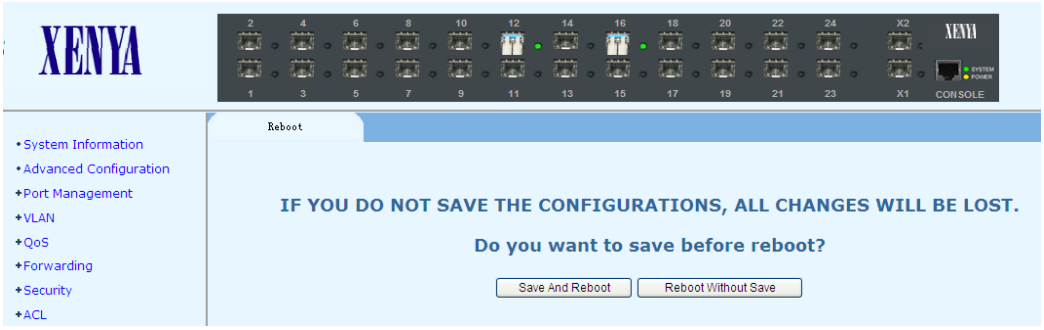


Note: During updating firmware, uploading or downloading a configuration file, make sure the power is not turned off.

2.14.5 Reboot

In this page, there are two buttons: **Save And Reboot**, and **Reboot Without Save**.

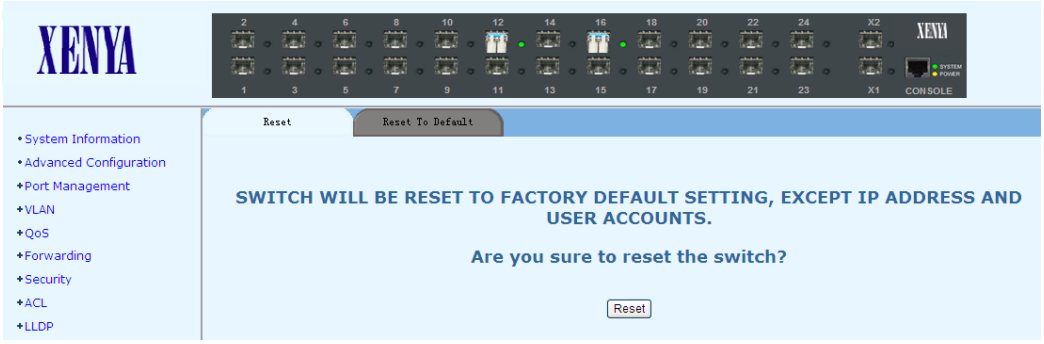
Save And Reboot: saves the current configuration and then reboot.
Reboot Without Save: directly reboots without saving the current configuration. All changes may be lost.



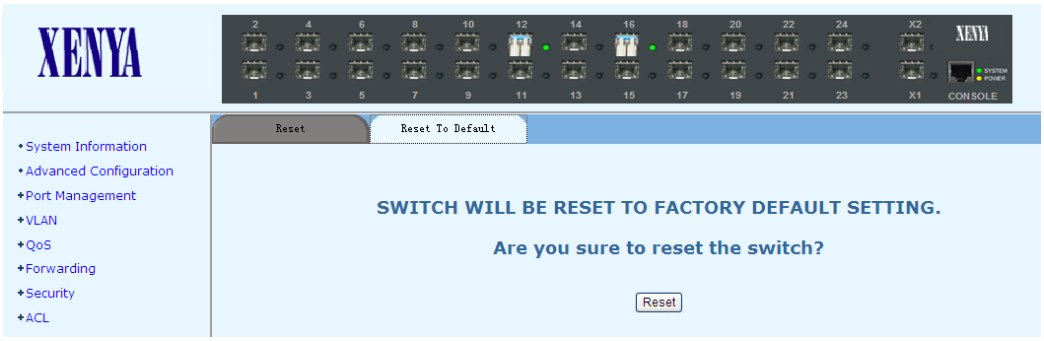
2.14.6 Reset

There are two tag pages: **Reset** and **Reset To Default.**

Reset: the switch will be reset to the factory default setting, except that the IP address and user accounts are kept unchanged.

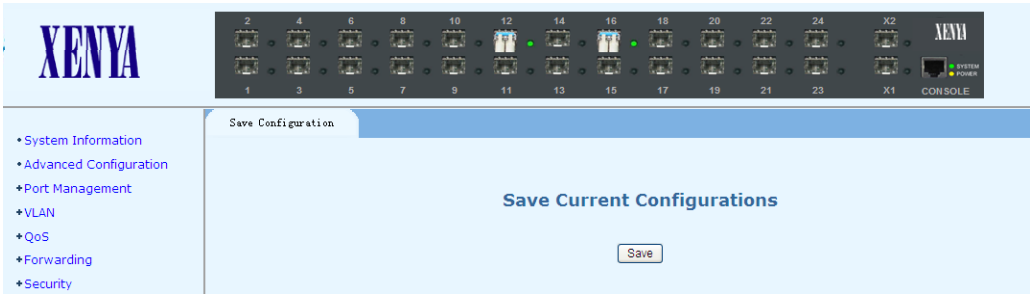


Reset To Default: the switch will be reset to the factory default setting.



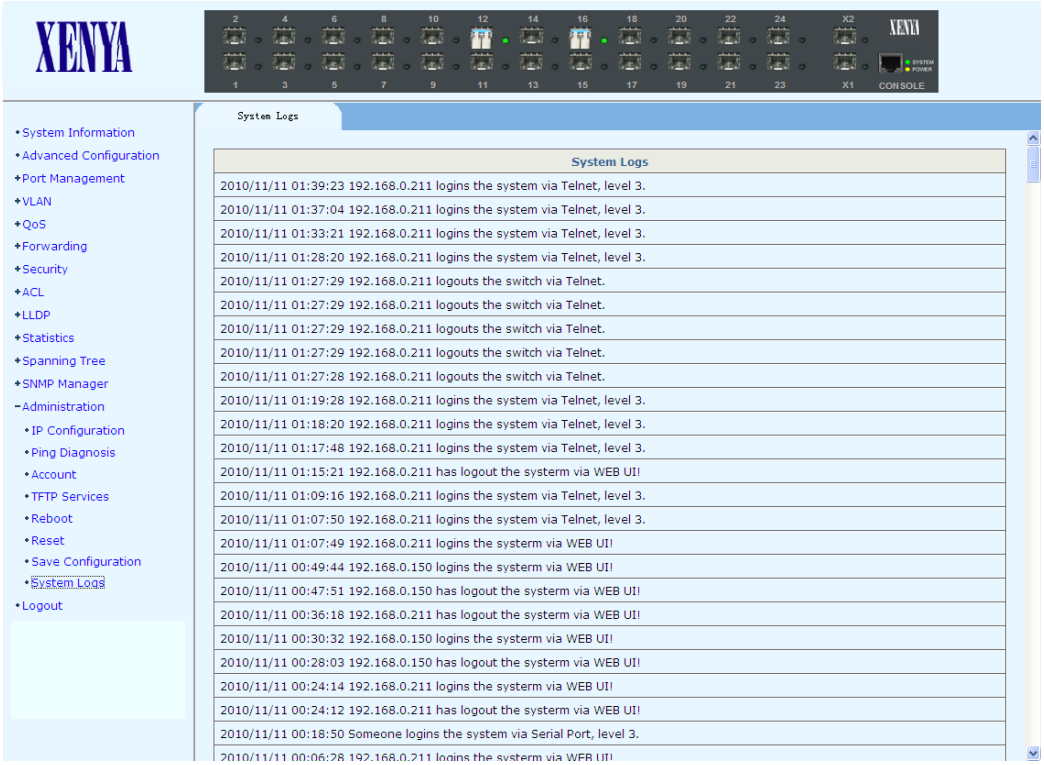
2.14.7 Save Configuration

This page saves current configurations.



2.14.8 System Logs

This page shows all of the system logs, clicking “Clear” button to clear all the records of the system logs.



2.15 Logout

Click “Logout” in the left menu to log out from the switch and close the browser.

3. Command Line Interface (CLI)

3.1 ERROR Message

If an incorrect parameter is entered, or the command cannot be executed, one of the following error messages will be displayed on screen.

- Incomplete command
- Wrong type parameter
- Wrong parameter value
- Ambiguous command
- Too many parameters or wrong parameter
- Invalid parameter
- Missing parameter
- Bad command

3.2 CLI Conventions

Convention	Description
Boldface	The keywords of a command line are in **Boldface.**
Italic	Command arguments are in *italic.*
[]	Items (keywords or arguments) in square brackets [] are optional.
{ x | y | ... }	Alternative items are grouped in braces and separated by vertical bars. Only one item is selected.
[x | y | ...]	Optional alternative items are grouped in square brackets and separated by vertical bars. One item or none is selected.
#	A line starting with the # sign is comments.

3.3 Shortcuts Introduction

Line shortcuts list:

Shortcuts	Explanation
【Delete】	Deletes the character on the cursor, for telnet only.
【← Backspace 】 or 【Ctrl】+【h】	Deletes the left character from the cursor.
【↑】or【Ctrl】+【p】	Execute the last command if the history list has it.
【↓】or【Ctrl】+【n】	Execute the next command if the history list has it.
【←】or【Ctrl】+【b】	Move the cursor one position left.
【→】or【Ctrl】+【f】	Move the cursor one position right.
【Tab】	Autocompletion
【Ctrl】+【z】	Exit current view except in System view.
【Ctrl】+【w】	Delete characters on the left of the cursor until it meets a space.
【Ctrl】+【a】	Move the cursor to the beginning of the line.
【Ctrl】+【e】	Move the cursor to the end of the line.
【Ctrl】+【u】	Delete everything from the beginning of the line to the cursor.
【Ctrl】+【d】	Delete one character on the cursor.
【Ctrl】+【k】	Delete everything from the cursor to the end of the line.

【Ctrl】+【c】	Skip the current command and go to a new line.

Page shortcuts list:

Shortcuts	Explanation
Any key except 【Enter】and【q】	Shows the next page.
【q】	Stops the displaying.
【Enter】	Shows the next line.

3.4 CLI Command Modes

These are the view modes for the switch:

- User view
- System view
- Ethernet port view
- Port-based VLAN view
- VLAN view
- dot1x view
- mst-region

The "Any view" in the below table refers to any one of the following: System view, Ethernet port view, Port-based VLAN view, VLAN view, or dot1x view.

Command Mode	Access Method	Prompt	Exit Method
User view	From System view, enter the **disable** command.	XS>	To back to System view, enter the **enable** command.
System view	This is the top level of access.	XS#	To enter into User view, enter the **disable** command.
Ethernet port view	From System view, specify an interface by entering the **interface ethernet** command followed by interface identification.	XS(Ethernetx/x)#	To exit to System view, enter the **end** command, or press **Ctrl-Z**
Port-based VLAN view	From System view, specify a vlan id by entering the **port-based-vlan** command followed by a vlan id.	XS(port-based-vlan-x)#	To exit to System view, enter the **end** command, or press **Ctrl-Z**
VLAN view	From System view, specify a vlan id by entering the **vlan** command followed by a vlan id.	XS(vlanx)#	To exit to System view, enter the **end** command, or press **Ctrl-Z**
dot1x view	From System view, enter the **dot1x** command.	XS(dot1x)#	To exit to System view, enter the **end** command, or press **Ctrl-Z**
ACL view	From System view, enter the **acl number** command, there are three prompts.	XS(ACL-basic-x)# XS(ACL-advanced-x)# XS(ACL-L2-x)#	To exit to System view, enter the **end** command, or press **Ctrl-Z**

Mst-region view	From system view, enter the **spanning-tree mst-region** view command	XS(mst-region)#	To exit to System view, enter the **end** command, or press **Ctrl-Z**
Ip-binding view	From system view, enter the **ip-binding** view command	XS(ip-binding)#	To exit to System view, enter the **end** command, or press **Ctrl-Z**

3.5 Global Commands

The "Any view" in the below table refers to any one of the following: System view, Ethernet port view, Port-based VLAN view, VLAN view, or dot1x view.

Command list:

View	Command	Explanation
Any view	**help**	shows all available commands on current view.
	clear	**clears screen display.**
	save	**saves current configuration.**
	reboot	reboots the switch.
	exit	**Logs out and disconnects from the switch.**

3.6 User Level

There are three user levels: Visitor, User, and Admin. The default users are listed in the following table:

Username	Password	User level
guest		Visitor
manager	123	User
superuser	123	Admin

The three levels of users have different access privileges as shown on the following table:

User level	Explanation
Visitor	CAN access the following commands: clear disable enable exit help ping ----- show (note) note: CAN NOT access the following commands: show user show snmp community show snmp traps-host show snmp user
User	CAN NOT access the following commands:

	user **no user** *user-name* **reset configuration** **tftp** *server-ip* **{ get** *source-file* **| put** *dest-file* **}** **update firmware** *file-name* **tftp-server** *server-ip*
Admin	CAN access all commands

3.7 System Management Commands

The "Any view" in the below table refers to any one of the following: System view, Ethernet port view, Port-based VLAN view, VLAN view, or dot1x view.

Command list:

View	Command
Any view	**show ipconfig**
Any view	**show user**
Any view	**show history**
Any view	**show system-information**
Any view	**show management**
Any view	**show temperature**
Any view	**show fan-status**
Any view	**show power-status**
Any view	**show local-time**
System view	**local-time date** *date* **month** *month* **year** *year* **local-time hour** *hour* **minute** *minute* **second** *second*
Any view	**show running-config**
System view	**disable**
System view	**enable**
System view	**management mode { disable | port-based ethernet** *interface* **| vlan** *vlan-id* **}**
System view	**ipconfig** { **auto** | **ip** *ip-address* [**netmask** *netmask*] [**gateway** *gateway*] } **no ipconfig**
System view	**ping** *ip-address*
System view	**user** **no user** *user-name*
System view	**reset configuration**
System view	**reset counters** [**ethernet** *interface*]
System view	**tftp** *server-ip* { **get** *source-file* | **put** *dest-file* }
System view	**update firmware** *file-name* **tftp-server** *server-ip*
System view	**xs-view** **no xs-view**

show ipconfig

Syntax

show ipconfig

View

Any view.

Parameters

None.

Description

Use **show ipconfig** command to display the IP address of the switch, including IP address, IP netmask, and IP gateway.

Examples

```
XS# show ipconfig
Operation Mode: Manual Setting
IP address:   192.168.0.253
IP netmask:   255.255.255.0
IP gateway:   192.168.0.201
```

show user

Syntax

show user

View

Any view.

Parameters

None.

Description

Use **show user** command to list all user information, including user name, user password, and user level.

Examples

XS# **show user**

user	password	level
guest		Visitor
manager	xxx	User
superuser	xxx	Admin

show history

Syntax

show history

View

Any view.

Parameters

None.

Description

Use **show history** command to list history commands of the current user.
History commands are those commands that were successfully executed previously and saved in the history command buffer. When the history command buffer is full, the earlier commands will be overwritten by the new ones.
By default, the CLI can save 30 history commands for each user.

Examples

```
XS# show history
 246 show snmp community
 247 show snmp traps-host
 248 show snmp traps-status
 249 show snmp user
 250 interface ethernet 0/23
 251 snmp-traps
 252 no snmp-traps
 253 show snmp
 254 end
 255 show snmp community
 256 show snmp user
 257 show snmp user
 258 show snmp traps-host
 259 show snmp traps-status
 260 show snmp
 261 snmp-server name guohq-XS7424
 262 show snmp
 263 snmp-server name dev-XS7424
 264 show snmp
 265 snmp-server community
 266 snmp-server user
 267 snmp-server user
 268 snmp-server user
 269 snmp-server traps
 270 ping 64.233.189.104
 271 snmp-server traps-host
 272 snmp-server traps-host 192.168.0.111
 273 show log
 274 no log
 275 show history
```

show system-information

Syntax

show system-information

View

Any view.

Parameters

None.

Description

Use **show system-information** command to display the basic information of the switch, including system name, system description, system location, system contact, hardware version, firmware version, boot loader version, MAC address, and System ID.

Examples

XS# **show system-information**

```
System Name          : XS26GS
System Description   : Optical Ethernet Switch
System Location      : Ljubljana, Slovenia
Systme Contact       : support@xenya.si
Hardware Version     : 1.0SFP
Firmware Version     : 1.071
Boot Loader Version  : 1.0.1
MAC Address          : 28-b0-cc-12-34-51
System ID            : R3A1234561
```

show management

Syntax

show management

View

Any view.

Parameters

None.

Description

Use **show management** command to display the management mode. It can be disabled, port-based, vlan and other related information.

Examples

XS# **show management**
Management mode is port-based.
Management port is Ethernet0/2

show temperature

Syntax

Show temperature

View

Any view

Parameters

None

Description

Use **show temperature** command to display the current environmental temperature of switch.

Example

XS# show temperature
Current temperature: 46.5 degree Celsius

show fan-status

Syntax

Show fan-status

View

Any view

Parameters

None

Description

Use **show fan-status** command to display the current status of the fans in the switch.

Example

XS# show fan-status
Fan status: Warning

show power-status

Syntax

show power-status

View

Any view

Parameters

None

Description

Use **show power-status** command to display the current status of power supply. There are two power supplies in the switch.

Example

XS# show power-status

Power A status : Off
Power B status : Off

show local-time

Syntax

Show local-time

View

Any view

Parameters

None

Description

Use **show local-time** command to display the current and local time.

Example

XS# show local-time
Local Time:
Tue Oct 13 10:19:30 2009

local-time

Syntax

local-time date *date* **month** *month* **year** *year*
local-time hour *hour* **minute** *minute* **second** *second*

View

System view

Parameters

d*ate*: Required, between 1 to 31.
month: Required, between 1 to 12.
year: Required, between 2009 to 3000
hour: Required, between 0 to 23.
minute: Required, between 0 to 59.
second: Required, between 0 to 59.

Description

Use **local-time date** *date* **month** *month* **year** *year* command to set the date.
Use **local-time hour** *hour* **minute** *minute* **second** *second* command to set the time.

Example

XS# local-time hour 14 minute 23 second 21
Set successfully!

show running-config

Syntax

show running-config

View

Any view

Parameters

None

Description

Use **show running-config** command to display which configuration you have set.

Example

XS# show running-config

Current Running Configuration:

ACL configuration
Valid ACL Num: 2, 23, 48,

VLAN configuration
VLAN Mode : 802.1Q VLAN
802.1Q Tag VLAN Ingress Filtering: Disable
Vlan 1(VID)
Vlan Name: Default
Untag Members:
Ethernet0/1
Ethernet0/2
Ethernet0/3
Ethernet0/4
Ethernet0/5
Ethernet0/6
Ethernet0/7
Ethernet0/8
Ethernet0/9
Ethernet0/10
Ethernet0/11
Ethernet0/12
Press any key to continue (Q to quit)

disable

Syntax

disable

View

System view.

Parameters

None.

Description

Use **disable** command to log out from the current user.

Examples

XS# **disable**
Exit current level successfully!
XS>

enable

Syntax

enable

View

System view.

Parameters

None.

Description

Use **enable** command to log in as another user.

Examples

XS> **enable**
user : *superuser*
password: ***

Entry level 3 (admin) successfully!

management mode

Syntax

management mode { disable | port-based ethernet *interface* **| vlan** *vlan-id* **}**

View

System view.

Parameters

port-based ethernet *interface*: uses the port based management mode and sets a management interface.
Vlan *vlan-id*: uses vlan management mode and sets a management vlan.

Description

Use the management mode command to set the management mode and related parameters.

Examples

XS# **management mode vlan** *2*
Management mode is vlan.
Management vlan is 2

ipconfig

Syntax

ipconfig { auto | ip *ip-address* **[netmask** *netmask* **] [gateway** *gateway* **] }**
no ipconfig

View

System view.

Parameters

auto: configures IP address automatically (DHCP-client)
ip: configures IP address manually

Description

Use **ipconfig auto** command to configure IP address automatically.
Use **ipconfig ip** command to configure IP address manually.
Use **no ipconfig** to restore the default IP configuration.
The default IP configuration is in the static mode, the IP address is 192.168.0.253, the netmask is 255.255.255.0, and the gateway is 192.168.0.201.

Examples

XS# **ipconfig auto**
Do you want to configure IP automatically (DHCP-client) ? (y/n):y
XS# **show ipconfig**
Operation Mode: Auto (DHCP-Client)
IP address: 192.168.0.11
IP netmask: 255.255.255.0
IP gateway: 192.168.0.201

ping

Syntax

ping *ip-address*

View

System view.

Parameters

ip-address: specifies the destination IP address to send ICMP ECHO-REQUEST packet.

Description

Use **ping** command to check the reachability of a host.
The executing procedure of **ping** command is: First, the source host sends an ICMP

ECHO-REQUEST packet to the destination host. Then, if the connection to the destination network is normal, the destination host receives this packet and responds with an ICMP ECHO-REPLY packet.
You can use **ping** command to check the network connectivity.

Examples

XS# **ping** *192.168.0.234*
This IP is alive!

user

Syntax

user
no user *user-name*

View

System view.

Parameters

user-name: specifies the user name to be deleted.

Description

Use **user** command to add a user. To add the user, you should specify user name, user password, and user level.
Use **no user** command to delete a specified user.

Examples

#add a user named test1, password is test1, user level is admin
XS# **user**
user name : test1

password : *****

password(again): *****

level(2-User, 3-Admin): 3
Add user successfully!

#delete user named test1
XS# **no user** *test1*
Deleting user successfully!

reset configuration

Syntax

reset configuration

View

System view.

Parameters

None.

Description

Use **reset configuration** command to make all of the factory default settings to be restored on the switch. When asked "Do you want to reset all the configurations except IP address and user account? (y/n)" , if you choose "y", the switch will be reset to factory default settings, except for the IP address and user account; if you choose "n", the switch will be reset to factory default settings including IP address and user account. The switch will reboot to take the configuration into effect.

Examples

XS# **reset configuration**
Do you want to reset all the configurations except IP address and user account? (y/n): *n*
Resetting configuration, please wait...
Resetting default configuration successfully!

reset counters

Syntax

reset counters [ethernet *interface* **]**

View

System view.

Parameters

interface: specifies the Ethernet port.

Description

Use **reset counters** command to reset the statistics counters in one or all ports.

Examples

XS# **reset counters ethernet** *0/1*
Clear the statistics of port ethernet 0/1

tftp

Syntax

tftp *server-ip* **{ get** *source-file* **| put** *dest-file* **}**

View

System view.

Parameters

server-ip: IP address or host name of the TFTP server connected; the IP address is in X.X.X.X format.
get: specified to download a file from the TFTP server.
source-file: name of the file to be downloaded.

put: specified to upload a file to the TFTP server.
dest-file: file name used when a file is uploaded and saved to a TFTP server.

Description

Use **tftp** *tftp-server* command to connect to a TFTP server and perform download or upload operations. Upload operation will backup the configuration in a file on tftp server, and download operation will restore the configuration from a file on tftp server.

Examples

XS# **tftp** *192.168.0.234* **put** *configtest*
Backing up the configuration, please wait...
Backup the configuration successfully!

update firmware

Syntax

update firmware *file-name* **tftp-server** *server-ip*

View

System view.

Parameters

server-ip: IP address or host name of the TFTP server connected, the IP address is in X.X.X.X format.
file-name: filename of firmware.

Description

Use **update firmware** command to download new firmware from tftp server and update the new firmware to the switch.

Examples

XS# **update firmware** *rootfs.img.gz* **tftp-server** *192.168.0.234*
Update the firmware, please wait...

xs-view

Syntax

xs-view
no xs-view

View

System view.

Parameters

xs-view: enable/disable the XS View network management function

Description

Use **xs-view** command to enable the XS View network management function.
Use **no xs-view** command to disable the XS View network management function.

Examples

XS# xs-view
XS View function has been enabled successfully.

XS# no xs-view
XS View function has been disabled successfully.

3.8 Port Basic Configuration Commands

The "Any view" in the below table refers to any one of the following: System view, Ethernet port view, Port-based VLAN view, VLAN view, or dot1x view.

Command list:

View	Command
Any view	**show interface [ethernet** *interface* **]**
Any view	**show interface statistics [ethernet** *interface* **]**
Any view	**show interface switchport ethernet** *interface*
Any view	**show storm-control**
System view	**interface ethernet** *interface*
Ethernet port view	**end**
Ethernet port view	**shutdown** **no shutdown**
Ethernet port view	**speed { 10 | 100 | 1000 | auto }** **no speed**
Ethernet port view	**duplex { auto | full | half }** **no duplex**
Ethernet port view	**flow-control** **no flow-control**
Ethernet port view	**learning** **no learning**
Ethernet port view	**line-rate { egress | ingress } rate** *rate-value* **no line-rate { egress | ingress }**
Ethernet port view	**jumboframe** **no jumboframe**
System view	**storm-control type** *type* **rate** *rate* **no storm-control**

show interface

Syntax

show interface [ethernet *interface* **]**

View

Any view.

Parameters

interface : ethernet port, in the form of interface = { interface-type/interface-number}, interface-type = {0 | 1}, when interface-type is 0, interface-number = { 1 | 2 | … | 24 }, when interface-type is 1, interface-number = { 1 | 2 }.

Description

Use **show interface** command to display the brief configuration information of one or all interfaces, including: interface type, link state, link nego, speed, duplex attribute, flow control, ingress rate and egress rate.

Examples

XS# show interface

```
PORT    STATE/LINK/NEGO/SPEED/DUPLEX/FLOW-CONTROL/LEARN/INGRESS/EGRESS/JUMBOFRAME
     ---------------------------------------------------------------------
Ethernet0/1   enabled /down/ auto/   -   /   - / - / enable/disable/disable/9216
Ethernet0/2   enabled /down/ auto/   -   /   - / - / enable/disable/disable/9216
Ethernet0/3   enabled /down/ auto/   -   /   - / - / enable/disable/disable/1518
Ethernet0/4   enabled /down/ auto/   -   /   - / - / enable/disable/disable/9216
Ethernet0/5   enabled /down/ auto/   -   /   - / - / enable/disable/disable/9216
Ethernet0/6   enabled /down/ auto/   -   /   - / - / enable/disable/disable/9216
Ethernet0/7   enabled /down/ auto/   -   /   - / - / enable/disable/disable/9216
Ethernet0/8   enabled /down/ auto/   -   /   - / - / enable/disable/disable/9216
Ethernet0/9   enabled / up / auto/1000M/full/off/ enable/disable/disable/9216
Ethernet0/10 enabled /down/ auto/   -   /   - / - / enable/disable/disable/9216
Ethernet0/11 enabled /down/ auto/   -   /   - / - / enable/disable/disable/9216
Ethernet0/12 enabled /down/ auto/   -   /   - / - / enable/disable/disable/9216
Ethernet0/13 enabled /down/ auto/   -   /   - / - / enable/disable/disable/9216
Ethernet0/14 enabled /down/ auto/   -   /   - / - / enable/disable/disable/9216
Ethernet0/15 enabled /down/ auto/   -   /   - / - / enable/disable/disable/9216
Ethernet0/16 enabled /down/ auto/   -   /   - / - / enable/disable/disable/9216
Ethernet0/17 enabled /down/ auto/   -   /   - / - / enable/disable/disable/9216
Ethernet0/18 enabled /down/ auto/   -   /   - / - / enable/disable/disable/9216
Ethernet0/19 enabled /down/ auto/   -   /   - / - / enable/disable/disable/9216
Ethernet0/20 enabled /down/ auto/   -   /   - / - / enable/disable/disable/9216
Ethernet0/21 enabled /down/ auto/   -   /   - / - / enable/disable/disable/9216
Ethernet0/22 enabled /down/ auto/   -   /   - / - / enable/disable/disable/9216
Ethernet0/23 enabled /down/ auto/   -   /   - / - / enable/disable/disable/9216
Ethernet0/24 enabled / up / auto/1000M/full/off/ enable/disable/disable/9216
Ethernet1/1   enabled /down/ auto/   -   /   - / - / enable/disable/disable/9216
Ethernet1/2   enabled /down/ auto/   -   /   - / - / enable/disable/disable/9216
```

XS# show interface ethernet 0/1

```
PORT   STATE/LINK/NEGO/SPEED/DUPLEX/FLOW-CONTROL/LEARN/INGRESS/EGRESS/JUMBOFRAME
---------------------------------------------------------------------------
Ethernet0/1      enabled/down/ auto/   -   /   - / - /enable /disable/disable/9216
```

show interface statistics

Syntax

show interface statistics [ethernet *interface* **]**

View

Any view.

Parameters

interface : ethernet port, in the form of interface = { interface-type/interface-number}, interface-type = {0 | 1}, when interface-type is 0, interface-number = { 1 | 2 | … | 24 }, when interface-type is 1, interface-number = { 1 | 2}.

Description

Use **show interface statistics** command to display the statistics information of one or all interfaces, including: transmitted good packets, transmitted bad packets, received good packets, transmitted abort packets, collision packets, dropped packets.

Examples

XS# **show interface statistics ethernet** *0/11*

PORT	TXGOODPKTS		TXBADPKTS		RXGOODPKTS		TXABORT	COLLISION	DROPPKT
	H32bits	L32bits	H32bits	L32bits					
Ethernet0/11	0	79	0	0	5389	0	0	0	

show interface switchport

Syntax

show interface switchport ethernet *interface*

View

Any view.

Parameters

interface : ethernet port, in the form of interface = { interface-type/interface-number}, interface-type = {0 | 1}, when interface-type is 0, interface-number = { 1 | 2 | … | 24 }, when interface-type is 1, interface-number = { 1 | 2}.

Description

Use **show interface switchport** command to display the information of the interface, including: vlan vid, egress rule, port membership type, pvid, link type, and frame type.

Examples

XS# **show interface switchport ethernet** *0/1*
Vlan vid: 1
Egress rule: untagged
Port membership type: static
Pvid: 1
Link type: Hybrid
Frame type: Admit all

show storm-control

Syntax

show storm-control

View

Any view.

Parameters

None.

Description

Use **show storm-control** command to display the storm control configurations.

Examples

```
XS(vlan2)# show storm-control
Show storm-control information
Type      :Broadcast
Rate      :1000pps
```

interface ethernet

Syntax

interface ethernet *interface*

View

System view.

Parameters

interface : ethernet port, in the form of interface = { interface-type/interface-number}, interface-type = {0 | 1}, when interface-type is 0, interface-number = { 1 | 2 | … | 24 }, when interface-type is 1, interface-number = { 1 | 2 }.

Description

Use **interface ethernet** command to enter a specific port view. Before configuring an Ethernet port, you need to enter an Ethernet port view.

Examples

```
XS# interface ethernet 0/23
XS(Ethernet0/23)#
```

end

Syntax

end

View

Ethernet port view.

Parameters

None.

Description

Use **end** command to exit from the Ethernet port configuration environment.

Examples

XS(Ethernet0/9)# **end**
XS#

shutdown

Syntax

shutdown
no shutdown

View

Ethernet port view.

Parameters

None.

Description

Use **shutdown** command to shut down an Ethernet port.
Use **no shutdown** command to bring up an Ethernet port.
By default, an Ethernet port is in up state.

Examples

XS(Ethernet0/24)# **shutdown**
Port ethernet0/24 shut down.

speed

Syntax

speed { 10 | 100 | 1000 | auto }
no speed

View

Ethernet port view.

Parameters

10: specifies the port speed to 10 Mbps.
100: specifies the port speed to 100 Mbps.
1000: specifies the port speed to 1,000 Mbps (only available on Gigabit Ethernet ports).
auto: specifies the port speed to the auto-negotiation mode.

Description

Use **speed** command to set the port speed.
Use **no speed** command to restore the port speed to the default setting.
By default, the port speed is in the auto-negotiation mode.
Note that you can only specify the **1000** and **auto** keyword for Gigabit Ethernet ports.

Examples

XS(Ethernet0/23)# **speed 10**
speed configured at 10Mbps on ethernet0/23

duplex

Syntax

duplex { auto | full | half }
no duplex

View

Ethernet port view.

Parameters

auto: sets the port to auto-negotiation mode.
full: sets the port to full duplex mode.
half: sets the port to half duplex mode.

Description

Use **duplex** command to set the duplex mode of the port.
Use **no duplex** command to restore the default duplex mode, that is, auto-negotiation.
By default, the port is in auto-negotiation mode.

Examples

XS(Ethernet0/23)# **duplex half**
duplex configured half on ethernet0/23

flow-control

Syntax

flow-control
no flow-control

View

Ethernet port view.

Parameters

None.

Description

Use **flow-control** command to enable flow control on the Ethernet port.
Use **no flow-control** command to disable flow control on the port.
In the case that flow control is enabled on both the local and peer switches, when congestion occurs on the local switch, the local switch sends a message to notify the peer switch to stop sending packets to itself or reduce the sending rate temporarily. The peer switch will stop sending packets to the local switch or reduce the sending rate temporarily when it receives the message; and vice versa. In this way, packet loss is avoided to make the network operation normal.
By default, flow control is disabled on a port.

Examples

XS(Ethernet0/23)# **flow-control**
flow-control is enabled on ethernet0/23.

learning

Syntax

learning
no learning

View

Ethernet port view.

Parameters

None.

Description

Use **learning** command to enable learning MAC address on the Ethernet port.
Use **no learning** command to disable learning MAC address on the port.
By default, learning MAC address is enabled on a port.

Examples

XS(Ethernet0/1)# **no learning**
Learning is disabled on ethernet0/1.

line-rate

Syntax

line-rate { egress | ingress } rate *rate-value*
no line-rate { egress | ingress }

View

Ethernet port view.

Parameters

rate *rate-value*: the upper rate threshold of the port. The *rate-value* is one of 64k,128k,192k,256k,320k,484k,512k,640k,768k,896k,1m,2m,4m,8m,10m,15m, 20m,30m,40m,50m,60m,70m,80m,90m

Description

Use **line-rate** command to configure the upper threshold of the traffic rate in Ethernet port view.
Use **no line-rate** command to cancel the upper threshold of the traffic rate in Ethernet port view.

Examples

XS(Ethernet0/1)# **line-rate egress rate** *64k*
Egress rate is 64kbps on ethernet0/1

XS(Ethernet0/1)# **no line-rate egress**
Turn off egress rate-limit on port ethernet0/1.

jumboframe

Syntax

jumboframe
no jumboframe

View

Ethernet port view.

Parameters

Description

Use **jumboframe** command to set the max length of frame as 9216.
Use **no jumboframe** command to restore the max length of frame to the default value 1518.

Examples

XS(Ethernet0/1)# jumboframe
Max frame length is 9216 on ethernet0/1.

XS(Ethernet0/3)# no jumboframe
Max frame length is 1518 on ethernet0/3.

storm-control

Syntax

storm-control type *type* **rate** *rate*
no storm-control

View

System view.

Parameters

type *type*: type is in the range from 1 to 7.
1:Broadcast
2:Multicast
3:Destination Lookup Failed(DLF)
4:Broadcast+Multicast
5:Broadcast+DLF
6:Multicast+DLF
7:Broadcast+Multicast+DLF
rate *rate*: rate is in the range from 1 to 262143.

Description

Use **storm-control** command to set the upper threshold of the broadcast/multicast/DLF (Destination Lookup Failed) traffic received on the port.
Use **no storm-control** command to remove the threshold configuration.
With the traffic upper threshold specified on a port, the system periodically collects statistics of the broadcast/multicast/DLF traffic on the port. Once a type of traffic exceeds the specified upper threshold, it blocks this type of traffic on the port.

Examples

XS# **storm-control type** *2* **rate** *2000*
Configuration completed successfully.

3.9 Link Aggregation Commands

The "Any view" in the below table refers to any one of the following: System view, Ethernet port view, Port-based VLAN view, VLAN view, or dot1x view.

Command list:

View	Command
Any view	**show lacp system-id**
Any view	**show lacp mode**
Any view	**show link-aggregation interface ethernet** *interface* **[to ethernet** *interface* **]**
Any view	**show link-aggregation summary**
Any view	**show link-aggregation verbose** *agg-id*
System view Ethernet port view	**lacp** **no lacp**
System view	**lacp system-priority** *system-priority* **no lacp system-priority**
System view	**link-aggregation group** *agg-id* **description** *agg-name* **no link-aggregation group** *agg-id* **description**
System view	**link-aggregation group** *agg-id* **mode { manual | static }** **no link-aggregation group** *agg-id*
Ethernet port view	**lacp port-priority** *port-priority* **no lacp port-priority**
Ethernet port view	**link-aggregation group** *agg-id* **no link-aggregation group**

show lacp system-id

Syntax

show lacp system-id

View

Any view.

Parameters

None.

Description

Use **show lacp system-id** command to display the device ID of the local system, including system priority and MAC address.

Examples

XS(Ethernet0/8)# **show lacp system-id**

LACP System ID: 1:00-0a-0b-0c-0e-09

show lacp mode

Syntax

show lacp mode

View

Any view.

Parameters

None.

Description

Use **show lacp mode** command to list the lacp mode on each port.

Examples

XS(Ethernet0/1)# **show lacp mode**

```
PORT            ACTIVE-STATE
--------       -------------
Ethernet0/1         active
Ethernet0/2           -
Ethernet0/3           -
Ethernet0/4           -
Ethernet0/5           -
Ethernet0/6           -
Ethernet0/7           -
Ethernet0/8           -
Ethernet0/9           -
Ethernet0/10          -
Ethernet0/11          -
```

```
Ethernet0/12          -
Ethernet0/13          -
Ethernet0/14          -
Ethernet0/15          -
Ethernet0/16          -
Ethernet0/17          -
Ethernet0/18          -
Ethernet0/19          -
Ethernet0/20          -
Ethernet0/21          -
Ethernet0/22          -
Ethernet0/23          -
Ethernet0/24          -
Ethernet1/1           -
Ethernet1/2           -
Ethernet1/3           -
Ethernet1/4           -
```

show link-aggregation interface

Syntax

show link-aggregation interface ethernet *interface 1* **[to ethernet** *interface 2* **]**

View

Any view.

Parameters

Interface 1: port number.
Interface 2: in conjunction with *interface 1,* defines a range of port numbers whose link aggregation details are to be displayed. The value of *interface 2* must not be less than that of *interface 1.*.

Description

Use **show link-aggregation interface** command to display the link aggregation details of a specified port or a range of ports.

Examples

XS# **show link-aggregation interface ethernet** *0/7*

```
link-aggregation ID       : 5
 Actor:
        Port Priority     : 1
        System ID         : 0-a-b-c-e-9
        Oper key          : 5
```

show link-aggregation summary

Syntax

show link-aggregation summary

View

Any view.

Parameters

None.

Description

Use **show link-aggregation summary** command to display summary information of all aggregation groups.

Examples

```
XS# show link-aggregation summary
1:00-0a-0b-0c-0e-09
LA      LA      Partner                 Selected
ID      Type    ID                      Ports
-------------------------------------------------------------------
1       Manual                          Ethernet0/1,3
2       Manual                          Ethernet0/6,8
5       Static                          Ethernet0/5,7
```

show link-aggregation verbose

Syntax

show link-aggregation verbose *agg-id*

View

Any view.

Parameters

agg-id: aggregation group ID, which is in a range from 1 to 13 and must be the ID of an existing aggregation group.

Description

Use **show link-aggregation verbose** command to display the details of a specified aggregation group or all aggregation groups.

Examples

```
XS# show link-aggregation verbose 5
Link-aggregation ID: 5
Link-aggregation Type: Static
Link-aggregation Description: test5
System ID:       1, 0-a-b-c-e-9
Local:
Port No          Status                  Priority        key
-----------------------------------------------------------------
Ethernet0/5      Selected                1               5
Ethernet0/7      Selected                1               5
```

lacp

Syntax

lacp
no lacp

View

System view, Ethernet port view.

Parameters

None.

Description

Use **lacp** command to enable LACP globally in system view or enable LACP on the port in ethernet port view.
Use **no lacp** command to disable LACP globally in system view or disable LACP on the port in ethernet port view.
By default, LACP is disabled on a port.

Examples

#enable LACP globally
XS# **lacp**
LACP is enabled now!

#enable LACP on ethernet port 0/2
XS(Ethernet0/2)# **lacp**
The port is enabled!

lacp system-priority

Syntax

lacp system-priority *system-priority*
no lacp system-priority

View

System view.

Parameters

system-priority: System priority, ranging from 1 to 65,535.

Description

Use **lacp system**-**priority** command to set the system priority.
Use **no lacp system**-**priority** command to restore the default system priority.
By default, the system priority is 1.

Examples

XS# **lacp system-priority** *20*
System priority is 20 now.

link-aggregation group description

Syntax

link-aggregation group *agg-id* **description** *agg-name*
no link-aggregation group *agg-id* **description**

View

System view.

Parameters

agg-id: aggregation group ID, in a range from 1 to 13.
agg-name: aggregation group name, a string of 1 to 32 characters.

Description

Use **link-aggregation group description** command to set a description for an aggregation group.
Use **no link-aggregation group description** command to remove the description of an aggregation group.

Examples

XS# **link-aggregation group** *3* **description** *test3*
The configuration is successful.

link-aggregation group mode

Syntax

link-aggregation group *agg-id* **mode {manual | static}**
no link-aggregation group *agg-id*

View

System view.

Parameters

agg-id: aggregation group ID, in a range from 1 to 13.
manual: creates a manual aggregation group.
static: creates a static aggregation group.

Description

Use **link-aggregation group mode** command to create a manual or static aggregation group.
Use **no link-aggregation group** command to remove the specified aggregation group.

Examples

XS# **link-aggregation group** *3* **mode static**
The link-aggregation group is in the Static Mode now.
The configuration is successful.

lacp port-priority

Syntax

lacp port-priority *port-priority*
no lacp port-priority

View

Ethernet port view.

Parameters

port-priority: port priority, ranging from 1 to 65,535.

Description

Use **lacp port-priority** command to set priority of the port.
Use **undo lacp port-priority** command to restore the default port priority.
By default, the port priority is 1.

Examples

XS(Ethernet0/2)# **lacp port-priority** *50*
The port priority is 50 now.

link-aggregation group

Syntax

link-aggregation group *agg-id*
no link-aggregation group

View

Ethernet port view.

Parameters

agg-id: aggregation group ID, in a range from 1 to 13.

Description

Use **link-aggregation group** command to add the Ethernet port to a manual or static aggregation group.
Use **no link-aggregation group** command to remove the Ethernet port from the aggregation group.

Examples

XS(Ethernet0/1)# **no link-aggregation group**
The port is deleted from the link-aggregation group!

XS(Ethernet0/1)# **link-aggregation group** *1*
The port is added into the link-aggregation group!

3.10 Mirroring Commands

The "Any view" in the below table refers to anyone of the following: System view, Ethernet port view, Port-based VLAN view, VLAN view, or dot1x view.

Command list:

View	Command
System view	**mirror group** *groupid*
mirror group view	**no mirror-group**
Any view	**show mirror**
mirror group view	**monitor-port ethernet** *interface*
mirror group view	**mirroring-port ethernet** *interface* [**to ethernet** *interface*] { **both** | **egress** | **ingress** } **no mirroring-port** [**ethernet** *interface*]

mirror group

Syntax

mirror group *groupid*
no mirror-group

View

System view.

Parameters

groupid: a group ID in the range of 1 to 4.

Description

Use **mirror group** command to enter into mirror group configuration environment.
Use **no mirror group** command to delete all mirror groups.

Examples

```
XS# mirror group 1
XS(MIRROR-1)#
```

mirror-group

Syntax

no mirror-group

View

mirror group view.

Parameters

None.

Description

Use **no mirror-group** command to delete all mirror groups.

Examples

```
XS(MIRROR-1)# no mirror-group
The mirror group have been deleted successfully.
```

show mirror

Syntax

show mirror

View

Any view.

Parameters

None.

Description

Use **show mirror** command to display the port mirroring configurations.

Examples

```
XS# show mirror
Group ID: 1
Mirror State: Enabled
Monitor-port:Ethernet0/1
Mirroring-port:
Ethernet0/2        both

Group ID: 2
Mirror State: Disabled

Group ID: 3
Mirror State: Disabled

Group ID: 4
Mirror State: Disabled
```

monitor-port

Syntax

monitor-port ethernet *interface*

View

System view.

Parameters

interface : ethernet port, in the form of interface = { interface-type/interface-number}, interface-type = {0 | 1}, when interface-type is 0, interface-number = { 1 | 2 | … | 24 }, when interface-type is 1, interface-number = { 1 | 2 }.

Description

Use **monitor-port** command to configure the destination port. You can use **to ethernet** *interface* to configure a range of continuous destination ports.

Examples

XS(MIRROR-1)# monitor-port ethernet 0/20
Configuration completed successfully.

mirroring-port

Syntax

mirroring-port ethernet *interface* [**to ethernet** *interface*] {**both** | **egress** | **ingress**}
no mirroring-port [**ethernet** *interface*]

View

System view.

Parameters

interface : ethernet port, in the form of interface = { interface-type/interface-number}, interface-type = {0 | 1}, when interface-type is 0, interface-number = { 1 | 2 | … | 24 }, when interface-type is 1, interface-number = { 1 | 2}.
to: specifies the last port number of the range.
both: specified to mirror all packets received on and sent from the port.
ingress: specified to mirror the packets received on the port.
egress: specified to mirror the packets sent from the port.

Description

Use **mirroring-port** command to configure the source port. You can use **to ethernet** *interface* to configure a range of continuous source ports.
Use **no mirroring-port** command to remove the configuration from the source port(s). If no Ethernet interface is specified, all configured mirror ports are removed.

Examples

XS(MIRROR-1)# mirroring-port ethernet 0/7 both
Configuration completed successfully.
XS(MIRROR-1)# mirroring-port ethernet 0/8 to ethernet 0/12 both
Configuration completed successfully.
XS(MIRROR-1)# no mirroring-port ethernet 0/3
Configuration completed successfully.

3.11 VLAN Commands

3.11.1 VLAN Configuration Commands

The "Any view" in the below table refers to anyone of the following: System view, Ethernet port view, Port-based VLAN view, VLAN view, or dot1x view.

Command list:

View	Command
Any view	**show vlan-mode**
Any view	**show vlan { all | dynamic | static |** *vlan-id1* **[to** *vlan-id2* **] }**
System view	**vlan-mode { none | port-based | 8021Q }**
System view	**vlan** *vlan-id* **no vlan { all |** *vlan-id1* **[to** *vlan-id2* **] }**
VLAN view	**end**
VLAN view	**description** *name*
VLAN view	**switchport { forbidden | tagged | untagged } ethernet** *interface* [**to ethernet** *interface*] **no switchport { forbidden | tagged | untagged } ethernet** *interface* [**to ethernet** *interface*]
VLAN view	**protocol-vlan { at | ip | ipx | mode ethernetii** *etype-id* **}** **no protocol-vlan { at | ip | ipx | mode ethernetii** *etype-id* **}**
VLAN view	**mac-based-vlan mac** *mac-address* **priority** *priority* **no mac-based-vlan mac** *mac-address*
VLAN view	**unknown-multicast-flood** **no unknown-multicast-flood**
VLAN view	**igmp-snooping** **no igmp-snooping**
VLAN view	**show igmp-snooping vlan{** *vlan-id1* **[to** *vlan-id2* **] }**
Ethernet port view	**switchport pvid** *vlan-id* **no switchport pvid**
Ethernet port view	**switchport link-type { access | hybrid | trunk }** **no switchport link-type**
Ethernet port view	**switchport admit-frame { all | only-tag }** **no switchport admit-frame**
Ethernet port view	**switchport protected** **no switchport protected**
Ethernet port view	**switchport ingress-filtering** **no switchport ingress-filtering**

show vlan-mode

Syntax

show vlan-mode

View

Any view.

Parameters

None.

Description

Use **show vlan-mode** to display the current setting of vlan mode.
By default, vlan mode is No VLAN.

Examples

XS# **show vlan-mode**
Current vlan mode is 8021Q vlan.

show vlan

Syntax

show vlan { all | dynamic | static | *vlan-id1* **[to** *vlan-id2* **] }**

View

Any view.

Parameters

vlan-id1: specifies the ID of a VLAN the information of which is to be displayed, in the range of 1 to 4094.
to *vlan-id2*: in conjunction with *vlan-id1*, defines a VLAN range to display information of all existing VLANs in the range. The *vlan-id2* argument takes a value in the range of 1 to 4094, and must not be less than that of *vlan-id1*.
all: displays information of all the VLANs.
dynamic: displays the number of dynamic VLANs and the ID of each dynamic VLAN. Dynamic VLANs refer to VLANs that are generated through GVRP.
static: displays the number of static VLANs and the ID of each static VLAN. Static VLANs refer to VLANs manually created.

Description

Use **show vlan** command to display information of VLANs, including ID, type, VLAN interface state and member ports of a VLAN.

Examples

```
XS# show vlan static
  VLAN ID: 1
  VLAN Type:   static
  Description: default
  Tag Ports:

  unTag Ports:
  Ethernet0/1          Ethernet0/2          Ethernet0/3
  Ethernet0/4          Ethernet0/5          Ethernet0/6
  Ethernet0/7          Ethernet0/8          Ethernet0/9
  Ethernet0/10         Ethernet0/11         Ethernet0/12
  Ethernet0/13         Ethernet0/14         Ethernet0/15
  Ethernet0/16         Ethernet0/17         Ethernet0/18
  Ethernet0/19         Ethernet0/20         Ethernet0/21
  Ethernet0/22         Ethernet0/23         Ethernet0/24
  Ethernet1/1          Ethernet1/2
  Forbidden Ports:

  Protocol vlan information:

  VLAN ID: 2
  VLAN Type:   static
  Description: test2
  Tag Ports:

  unTag Ports:

  Forbidden Ports:

  Protocol vlan information:
```

VLAN ID: 3
VLAN Type: static
Description: test3
Tag Ports:

unTag Ports:

Forbidden Ports:

Protocol vlan information:

vlan-mode

Syntax

vlan-mode { none | port-based | 8021Q }

View

System view.

Parameters

none: disabled VLAN function.
port-based: allows port based VLAN.
8021Q: allows 802.1q VLAN.

Description

Use **vlan-mode** to set a vlan mode.
By default, vlan mode is No VLAN.

Examples

XS# **vlan-mode port-based**
Config port based vlan successfully!

vlan

Syntax

vlan *vlan-id*
no **vlan { all |** *vlan-id1* **[to** *vlan-id2* **] }**

View

System view.

Parameters

vlan-id: specifies the ID of a VLAN the information of which is to be created, in a range from 1 to 4094.
vlan-id1: specifies the ID of a VLAN the information of which is to be deleted, in the range of 1 to 4094.
to *vlan-id2*: in conjunction with *vlan-id1*, defines a VLAN range to delete information of all existing VLANs in the range. The *vlan-id2* argument takes a value in the range of 1 to 4094, and must not be less than that of *vlan-id1*.

all: deletes all VLANs.

Description

Use **vlan** command to enter into vlan configuration environment.
Use **no vlan** command to delete all VLANs or specified VLAN(s).

Examples

XS# **vlan** *2*
XS(vlan2)#

end

Syntax

end

View

VLAN view.

Parameters

None.

Description

Use **end** command to exit from the vlan configuration environment.

Examples

XS(vlan2)# **end**
XS#

description

Syntax

description *name*

View

VLAN view.

Parameters

name: VLAN name, a description of 1 to 255 characters. It can contain special characters, but cannot be spaces.

Description

Use **description** command to assign a name to the VLAN.
By default, the name of a VLAN is its VLAN ID, **VLAN0001** for example.

Examples

XS(vlan2)# **description** *test2222*
set vlan group description successfully!!!

switchport

Syntax

switchport { forbidden | tagged | untagged } ethernet *interface* [**to ethernet** *interface*]
no switchport { forbidden | tagged | untagged } ethernet *interface* [**to ethernet** *interface*]

View

VLAN view.

Parameters

forbidden: does not allow the port to be added to the VLAN group, even if GARP indicates so.
tagged: indicates the port is a tagged member of the VLAN group. All packets forwarded by the port are tagged. The packets contain VLAN information.
untagged: indicates the port is an untagged VLAN member of the VLAN group. Packets forwarded by the port are untagged.
interface: port number. Ethernet ports to be added to or removed from the current VLAN.
to: specifies the last port number of the range.

Description

Use **switchport** command to add forbidden, tagged or untagged port to the VLAN.
Use **no switchport** command to delete forbidden, tagged or untagged port from the VLAN.

Examples

XS(vlan5)# **switchport tagged ethernet** *0/8* **to ethernet** *0/15*
Ethernet0/8 belongs to a trunk. The other member in the same trunk will be added to this vlan as well!
Add tagged ports successfully!

XS(vlan5)# **no switchport tagged ethernet** *0/8* **to ethernet** *0/15*
Ethernet0/8 belongs to a trunk. The other member in the same trunk will be removed from this vlan!
Delete tagged ports successfully!

protocol-vlan

Syntax

protocol-vlan { at | ip | ipx | mode ethernetii *etype-id* **}**
no protocol-vlan { at | ip | ipx | mode ethernetii *etype-id* **}**

View

VLAN view.

Parameters

at: creates the AppleTalk-based protocol template.
ip: creates the IP-based protocol template.

ipx: creates the IPX-based protocol template.
mode: configures a user-defined protocol template.
ethernetii *etype-id*: creates the protocol template that matches the Ethernet II encapsulation format and the corresponding protocol type value of the packet. The *etype-id* argument indicates the protocol type value and ranges from 0x0600 to 0xFFFF (excluding 0x0800, 0x8137, and 0x809b).

Description

Use **protocol-vlan** command to configure the protocol template used for classifying protocol-based VLANs.
Use **no protocol-vlan** command to disable the configuration.
By default, no protocol template is configured.

Examples

XS(vlan5)# protocol-vlan 1 mode ethernetii 0x8899
Settings are updated successfully!

mac-based-vlan

Syntax

mac-based-vlan mac *mac-address* priority *priority*
no mac-based-vlan mac *mac-address*

View

VLAN view.

Parameters

mac-address:LLC address.
priority:vlan tag header priority.

Description

Use **mac-based-vlan** command to configure the mac-address used for classifying mac-based VLANs.
Use **no mac-based-vlan** command to delete the configuration.
By default, no mac-address is configured.

Examples

XS(vlan5)# **mac-based-vlan mac 00-11-22-33-44-55 priority 0**
Setting successfully
XS(vlan5)#
XS(vlan5)# **no mac-based-vlan mac 00-11-22-33-44-55**
Delete successfully

unknown-multicast-flood

Syntax

unknown-multicast-flood
no unknown-multicast-flood

View

VLAN view.

Parameters

None.

Description

Use **unknown-multicast-flood** command to enable the Unknown Multicast Flood Status for this VLAN group.
Use **no unknown-multicast-flood** command to disable the Unknown Multicast Flood Status for this VLAN group.
By default, no unknown-multicast-flood is configured.

Examples

XS(vlan5)# unknown-multicast-flood
XS(vlan5)# no unknown-multicast-flood

igmp-snooping

Syntax

igmp-snooping
no igmp-snooping

View

VLAN view.

Parameters

None.

Description

Use **igmp-snooping** command to enable the igmp snooping function for this VLAN group.
Use **no igmp-snooping** command to enable the igmp snooping function for this VLAN group.
By default, no igmp-snooping is configured.

Examples

XS(vlan5)# igmp-snooping
Igmp-snooping has been enabled on vlan 5

XS(vlan5)# no igmp-snooping
Igmp-snooping has been disabled in this vlan group 5.

show igmp-snooping

Syntax

show igmp-snooping vlan{ *vlan-id1* **[to** *vlan-id2* **] }**

View

VLAN view.

Parameters

vlan-id: specifies the ID of a VLAN the information of which is to be created, in a range from 1 to 4094.
vlan-id1: specifies the ID of a VLAN the information of which is to be deleted, in the range of 1 to 4094.
to *vlan-id2*: in conjunction with *vlan-id1*, defines a VLAN range to delete information of all existing VLANs in the range. The *vlan-id2* argument takes a value in the range of 1 to 4094, and must not be less than that of *vlan-id1*.

Description

Use **show igmp-snooping** command to display the igmp snooping configuration for the specified VLAN group.

Examples

XS(vlan5)# show igmp-snooping vlan 5
show igmp-snooping configuration on vlan 5
Igmp-snooping state: Enabled
VLAN route interface:
Ethernet0/7
Ethernet0/8

switchport pvid

Syntax

switchport pvid *vlan-id*
no switchport pvid

View

Ethernet port view

Parameters

vlan-id: specifies the default VLAN ID of the port, in a range from 1 to 4094.

Description

Use **switchport pvid** command to set the default VLAN ID for the port. A trunk port sends packets of the default VLAN untagged.
Use **no switchport pvid** command to restore the default.
By default, the default VLAN ID of a port is VLAN 1.

Examples

XS(Ethernet0/9)# **switchport pvid** *5*
Setting successfully

switchport link-type

Syntax

switchport link-type { access | hybrid | trunk }
no switchport link-type

View

Ethernet port view

Parameters

access: sets the port link type to access.
hybrid: sets the port link type to hybrid.
trunk: sets the port link type to trunk.

Description

Use **switchport link-type** command to set link type of the Ethernet port.
Use **no switchport link-type** command to restore the default link type.
The default link type of an Ethernet port is **hybrid**.

Examples

XS(Ethernet0/9)# **switchport link-type trunk**
Set successfully

switchport admit-frame

Syntax

switchport admit-frame { all | only-tag }
no switchport admit-frame

View

Ethernet port view

Parameters

all: the port accepts all ingress packages
only-tag: the port accepts tagged packages, and discards untagged ones.

Description

Use **switchport admit-frame** command to configure how the port accepts ingress packages.
Use **no switchport admit-frame** command to restore the default admit-frame type on a port.
By default, the admit-frame type is **all**.

Examples

XS(Ethernet0/9)# **switchport admit-frame only-tag**
Set successfully

switchport protected

Syntax

switchport protected
no switchport protected

View

Ethernet port view

Parameters

None.

Description

Use **switchport protected** command to enable switchport protected function for the specified switch interface.
Use **no switchport protected** command to disable switchport protected function for the specified switch interface.
By default, the switchport protected is configured.

Examples

XS(Ethernet0/9)# switchport protected
Port ethernet0/9 has been protected.

XS(Ethernet0/9)# no switchport protected
Port ethernet0/9 has been normal.

switchport ingress-filtering

Syntax

switchport ingress-filtering
no switchport ingress-filtering

View

Ethernet port view

Parameters

None.

Description

Use **switchport ingress-filtering** command to enable switchport ingress-filterting function for the specified switch interface.
Use **no switchport ingress-filtering** command to disable switchport ingress-filterting function for the specified switch interface.
By default, the switchport igress-filtering is configured.

Examples

XS(Ethernet0/9)# switchport ingress-filtering
Ingress-filtering has been enabled successfully!
XS(Ethernet0/9)# no switchport ingress-filtering

Ingress-filtering has been disabled successfully!

3.11.2 Port-Based VLAN Configuration Commands

The "Any view" in the below table refers to anyone of the following: System view, Ethernet port view, Port-based VLAN view, VLAN view, or dot1x view.

Command list:

View	Command
Any view	**show port-based-vlan { all |** *vlan-id1* **[to** *vlan-id2* **] }**
System view	**port-based-vlan** *vlan-id* **no port-based-vlan { all |** *vlan-id1* **[to** *vlan-id2* **] }**
Port-based VLAN view	**end**
Port-based VLAN view	**description** *name*
Port-based VLAN view	**interface ethernet** *interface* **[to ethernet** *interface* **]** **no interface ethernet** *interface* **[to ethernet** *interface* **]**

show port-based-vlan

Syntax

show port-based-vlan { all | *vlan-id1* **[to** *vlan-id2* **] }**

View

Any view.

Parameters

vlan-id1: specifies the ID of a VLAN the information of which is to be displayed, in the range of 1 to 255.
to *vlan-id2*: in conjunction with *vlan-id1*, defines a VLAN range to display information of all existing VLANs in the range. The *vlan-id2* argument takes a value in the range of 1 to 255, and must not be less than that of *vlan-id1*.
all: displays information of all the VLANs.

Description

Use **show port-based-vlan** command to display information of port based VLANs, including ID, description and member ports of a VLAN.

Examples

XS# **show port-based-vlan** *1* **to** *2*

```
VLAN ID: 1
Description:vlan1
Member Ports:
Ethernet0/9          Ethernet0/10          Ethernet0/11
Ethernet0/12

VLAN ID: 2
Description: vlan2
Member Ports:
```

Ethernet0/12 Ethernet0/13 Ethernet0/14

port-based-vlan

Syntax

port-based-vlan *vlan-id*
no port-based-vlan { all | *vlan-id1* **[to** *vlan-id2* **] }**

View

System view.

Parameters

vlan-id: specifies the ID of a VLAN the information of which is to be created, in the range of 1 to 255.
vlan-id1: specifies the ID of a VLAN the information of which is to be deleted, in the range of 1 to 255.
to *vlan-id2*: in conjunction with *vlan-id1*, defines a VLAN range to delete information of all existing VLANs in the range. The *vlan-id2* argument takes a value in the range of 1 to 255, and must not be less than that of *vlan-id1*.
all: deletes all port based VLANs.

Description

Use **port-based-vlan** command to enter into the port-based vlan configuration environment.
Use **no port-based-vlan** command to delete all port-based VLANs or specified VLAN(s).

Examples

XS# **port-based-vlan** *3*
XS(port-based-vlan-3)#

end

Syntax

end

View

Port-based VLAN view.

Parameters

None.

Description

Use **end** command to exit from the port-based vlan configuration environment.

Examples

XS(port-based-vlan-3)# **end**
XS#

description

Syntax

description *name*

View

Port-based VLAN view.

Parameters

name: VLAN name, a description of 1 to 255 characters. It can contain special characters, but cannot be spaces.

Description

Use **description** command to assign a name to the VLAN.
By default, the name of a VLAN is its VLAN ID, **VLAN0001** for example.

Examples

XS(port-based-vlan-3)# **description** *vlan*8*3*
XS(port-based-vlan-3)#

interface ethernet

Syntax

interface ethernet *interface* **[to ethernet** *interface* **]**
no interface ethernet *interface* **[to ethernet** *interface* **]**

View

Port-based VLAN view.

Parameters

interface: port number, Ethernet port to be added to or removed from the VLAN.
to: in conjunction with the other parameter to define a range of ports to add to or remove from the VLAN.

Description

Use **interface** command to assign one or multiple ports to the VLAN.
Use **no interface** command to remove the specified port(s) from the VLAN.

Examples

XS(port-based-vlan-4)# **interface ethernet** *0/2* **to ethernet** *0/24*
Ethernet0/2 belongs to a trunk. The other member in the same trunk will be added to this vlan!
Add the port successfully.

XS(port-based-vlan-4)# no interface ethernet 0/2 to ethernet 0/24
Ethernet0/2 belongs to a trunk. The other member in the same trunk will be removed from this vlan!
Delete the port successfully.

3.12 VLAN VPN

The "Any view" in the below table refers to anyone of the following: System view, Ethernet port view, Port-based VLAN view, VLAN view, or dot1x view.

Command list:

View	Command
Any view	**show vlan-vpn**
System view	**vlan-vpn** **no vlan-vpn**
System view	**vlan-vpn tpid** *tpid* **no vlan-vpn tpid** *tpid*
System view Ethernet port view	**vlan-vpn QinQ ethernet** *ethernet-port* **priority** *priority* **new-vid** *new-vid* **old-vid** *old-vid* **to** *old-end-vid* **no vlan-vpn QinQ ethernet** *ethernet-port* **new-vid** *new-vid* **old-vid** *old-vid* **to** *old-end-vid*

show vlan-vpn

Syntax

show vlan-vpn

View

Any view.

Parameters

None.

Description

Use show vlan-vpn command to display the settings of the vlan-vpn of all ports. This command displays the following settings:

- Global vlan-vpn status
- Vlan-vpn per Ethernet port
- QinQ

Examples

XS# show vlan-vpn

```
 Global vlan-vpn Status:Disabled
   Port              Vlan-vpn State      Tpid
--------------   ----------------- -------
Ethernet0/1         Disabled          0x8100
Ethernet0/2         Disabled          0x8100
Ethernet0/3         Disabled          0x8100
Ethernet0/4         Disabled          0x8100
Ethernet0/5         Disabled          0x8100
Ethernet0/6         Disabled          0x8100
Ethernet0/7         Disabled          0x8100
Ethernet0/8         Disabled          0x8100
Ethernet0/9         Disabled          0x8100
```

```
Ethernet0/10        Disabled          0x8100
Ethernet0/11        Disabled          0x8100
Ethernet0/12        Disabled          0x8100
Ethernet0/13        Disabled          0x8100
Ethernet0/14        Disabled          0x8100
Ethernet0/15        Disabled          0x8100
Ethernet0/16        Disabled          0x8100
Ethernet0/17        Disabled          0x8100
Ethernet0/18        Disabled          0x8100
Ethernet0/19        Disabled          0x8100
Ethernet0/20        Disabled          0x8100
Ethernet0/21        Disabled          0x8100
Ethernet0/22        Disabled          0x8100
Ethernet0/23        Disabled          0x8100
Ethernet0/24        Disabled          0x8100
Ethernet1/1        Disabled          0x8100
Ethernet1/2        Disabled          0x8100

 New VLAN ID    Old Low VID     Old Hight VID     Priority      Port
------------- -------------- ---------------- ---------- ------------ ------------
```

vlan-vpn

Syntax

vlan-vpn
no vlan-vpn

View

System view.

Parameters

none.

Description

Use **vlan-vpn** command to enable VLAN-VPN on this switch.
Use **no vlan-vpn** command to disable VLAN-VPN on this switch.

Examples

XS# vlan-vpn
Vlan-vpn has been enabled successfully.

vlan-vpn tpid

Syntax

vlan-vpn tpid *tpid*
no vlan-vpn tpid *tpid*

View

System view.

Parameters

tpid(Tag Protocol Identifier): includes an Ethernet Type value that is used to identify the frame as a tagged frame and to select the correct tag decoding functions.

Description

Use **vlan-vpn tpid** command to set a TPID value.
Use **no vlan-vpn tpid** command to restore to the default setting of TPID.

Examples

XS# vlan-vpn ethernet 0/2 tpid 0x8100
Tpid has been configured successfully.

vlan-vpn QinQ

Syntax

vlan-vpn QinQ ethernet *ethernet-port* **priority** *priority* **new-vid** *new-vid* **old-vid** *old-vid* **to** *old-end-vid*
no vlan-vpn QinQ ethernet *ethernet-port* **new-vid** *new-vid* **old-vid** *old-vid* **to** *old-end-vid*

View

System view.

Parameters

interface : ethernet port, in the form of interface = { interface-type/interface-number}, interface-type = {0 | 1}, when interface-type is 0, interface-number = { 1 | 2 | … | 24 }, when interface-type is 1, interface-number = { 1 | 2 }.

priority: the outer VLAN priority, in the range from 0 to 7.
new-vid: the outer double VLAN ID, in the range from 1 to 4094.
old-vid: the incoming VLAN ID to be added double tag in the range from 1 to 4094.
to *old-end-vid*: in conjunction with *old-vid*, defines a VLAN ID range to be added double tag.

Description

Use **vlan-vpn QinQ** command to set a double tag on the incoming VLAN.
Use no **vlan-vpn QinQ** command to delete the QinQ configuration.

Examples

XS# vlan-vpn QinQ ethernet 0/3 priority 0 new-vid 100 old-vid 3 to 4
Configure QinQ successfully.

3.13 GVRP Commands

The "Any view" in the below table refers to anyone of the following: System view, Ethernet port view, Port-based VLAN view, VLAN view, or dot1x view.

Command list:

View	Command
Any view	**show garp timer**
Any view	**show gvrp status**
System view	**garp timeout {hold | join | leave | leaveall }** *timer-value* **no garp timeout {hold | join | leave | leaveall }** *timer-value*
System view Ethernet port view	**gvrp** **no gvrp**
Ethernet port view	**gvrp registration { fixed | forbidden | normal }** **no gvrp registration**

show garp timer

Syntax

show garp timer

View

Any view.

Parameters

None.

Description

Use **show garp timer** command to display the settings of the GARP timer of all ports.
This command displays the settings of the following timers:

- Join timer
- Leave timer
- LeaveAll timer
- Hold timer

Examples

XS# **show garp timer**

```
  Join     Leave    Leave-all    Hold
------- ------- ----------- -------
   200      600       10000      10
```

show gvrp status

Syntax

show gvrp status

View

Any view.

Parameters

None.

Description

Use **show gvrp status** command to display the GVRP settings of all ports.

Examples

XS# **show gvrp status**

Gvrp feature is currently enabled on this switch!

Ports	Gvrp-status	Registration
Ethernet0/1	Disabled	Normal
Ethernet0/2	Disabled	Normal
Ethernet0/3	Disabled	Normal
Ethernet0/4	Disabled	Normal
Ethernet0/5	Disabled	Normal
Ethernet0/6	Disabled	Normal
Ethernet0/7	Disabled	Normal
Ethernet0/8	Disabled	Normal
Ethernet0/9	Disabled	Normal
Ethernet0/10	Disabled	Normal
Ethernet0/11	Disabled	Normal
Ethernet0/12	Disabled	Normal
Ethernet0/13	Disabled	Normal
Ethernet0/14	Disabled	Normal
Ethernet0/15	Disabled	Normal
Ethernet0/16	Disabled	Normal
Ethernet0/17	Disabled	Normal
Ethernet0/18	Disabled	Normal
Ethernet0/19	Disabled	Normal
Ethernet0/20	Disabled	Normal
Ethernet0/21	Disabled	Normal
Ethernet0/22	Disabled	Normal
Ethernet0/23	Disabled	Normal
Ethernet0/24	Disabled	Normal
Ethernet1/1	Disabled	Normal
Ethernet1/2	Disabled	Normal

garp timeout

Syntax

garp timeout {hold | join | leave | leaveall } *timer-value*
no garp timeout {hold | join | leave | leaveall } *timer-value*

View

System view.

Parameters

hold: sets the GARP Hold timer. The argument ranges from 10 to 2147483640.
join: sets the GARP Join timer. The argument ranges from 10 to 2147483640, and the default value is 200 milliseconds.
leave: sets the GARP Leave timer. The argument ranges from 10 to 2147483640, and the default value is 600 milliseconds.
leaveall: sets the GARP Leaveall timer. The argument ranges from 10 to

2147483640, the default value is 10000 milliseconds.
timer-value: timeout time (in milliseconds) of the GARP timer (Hold, Join, Leave or Leaveall) to be set.

Description

Use **garp timeout** command to set a GARP timer.
Use **no garp timeout** command to restore to the default setting of a GARP timer.

Examples

XS# **garp timeout leaveall** *20000*
Configure successfully.

gvrp

Syntax

gvrp
no gvrp

View

System view.
Ethernet port view.

Parameters

None.

Description

Use **gvrp** command to enable GVRP globally (in System view) or for a port (in Ethernet port view).
Use **no gvrp** command to disable GVRP globally (in System view) or for a port (in Ethernet port view).
By default, GVRP is disabled both globally and on a port.

Examples

XS(Ethernet0/1)# **gvrp**
Enable this interface gvrp successfully.

gvrp registration

Syntax

gvrp registration {fixed | forbidden | normal}
no gvrp registration

View

Ethernet port view

Parameters

fixed: specifies the fixed GVRP registration mode. A port operating in this mode cannot register or deregister VLAN information dynamically. It only propagates static VLAN information. Besides, the port permits only static VLANs, that is, it

propagates only static VLAN information to the other GARP members.

forbidden: specifies the forbidden GVRP registration mode. A port operating in this mode cannot register or deregister VLAN information dynamically. It permits only VLAN 1, that is, it propagates only the information of VLAN 1 to the other GARP members.

normal: specifies the normal mode. A port operating in this mode can register or deregister VLAN information dynamically, and can propagate both dynamic and static VLAN information.

Description

Use **gvrp registration** command to configure the GVRP registration mode on a port.
Use **no gvrp registration** command to restore to the default GVRP registration mode on a port.
By default, the GVRP registration mode is **normal**.

Examples

XS(Ethernet0/1)# **gvrp registration fixed**
forbid registering vlan dynamically or logging out of vlan, only allow transmitting vlan information statically.

3.14 QoS Commands

The "Any view" in the below table refers to anyone of the following: System view, Ethernet port view, Port-based VLAN view, VLAN view, or dot1x view.

Command list:

View	Command
Any view	**show qos queue-scheduler**
Any view	**show qos cos-local-precedence-map**
Any view	**show qos map dscp cos**
Any view	**show qos interface [ethernet** *interface*]
System view	**qos queue-scheduler {strict-priority | wrr** *queue0-weight queue1-weight queue2-weight queue3-weight* **}** **no qos queue-scheduler**
System view	**qos cos-local-precedence-map** *cos0-map-local-prec cos1-map-local-prec cos2-map-local-prec cos3-map-local-prec cos4-map-local-prec cos5-map-local-prec cos6-map-local-prec cos7-map-local-prec* **no qos cos-local-precedence-map**
System view	**qos map dscp** *dscp* **to cos** *cos* **no qos map dscp** *dscp*
Ethernet port View	**qos-mode dscp** **no qos-mode dscp**
Ethernet port View	**priority** *priority-level* **no priority**

show qos queue-scheduler

Syntax

show qos queue-scheduler

View

Any view.

Parameters

None.

Description

Use **show qos queue-scheduler** command to display the global queue scheduling configuration.

Examples

XS# **show qos queue-scheduler**
Queue scheduling mode: weighted round robin
weight of queue 0: 2
weight of queue 1: 5
weight of queue 2: 7
weight of queue 3: 8

show qos cos-local-precedence-map

Syntax

show qos cos-local-precedence-map

View

Any view.

Parameters

None.

Description

Use **show qos cos-local-precedence-map** command to display the 802.1p priority-to-local precedence mapping, illustrated by an 802.1p priority to local precedence mapping table as shown in the following example.

After a packet enters a switch, the switch sets the 802.1p priority and local precedence for the packet according to its own capability and the corresponding rules. The local precedence is locally significant precedence that the switch assigns to the packet. It corresponds to an output queue. Packets with higher local precedence values take precedence over those with lower precedence values and will be processed preferentially.

Examples

XS# show qos cos-local-precedence-map
cos-local-precedence-map:
cos(802.1p) :0 1 2 3 4 5 6 7

queue :0 0 1 1 2 2 3 3

show qos map dscp cos

Syntax

show qos map dscp cos

View

Any view.

Parameters

None.

Description

Use **show qos map dscp cos** command to display the mapping of DSCP priority to 802.1p priority, illustrated by a DSCP priority to 802.1p priority mapping table as shown in the following example.

Examples

```
XS# show qos map dscp cos
Dscp-cos map:
d1 :  d2 0   1   2   3   4   5   6   7   8   9
0  :     0   0   0   0   0   0   0   0   1   1
1  :     1   1   1   1   1   1   2   2   2   2
2  :     2   2   2   2   3   3   3   3   3   3
3  :     3   3   4   4   4   4   4   4   4   4
4  :     5   5   5   5   5   5   5   5   6   6
5  :     6   6   6   6   6   6   7   7   7   7
6  :     7   7   7   7
```

show qos interface

Syntax

show qos interface [ethernet *interface*]

View

Any view.

Parameters

ethernet *interface*: displays the qos information of a specified port.
interface : ethernet port, in the form of *interface* = { *interface-type*/*interface-number*}, *interface-type* = {0 | 1}, when *interface-type* is 0, *interface-number* = { 1 | 2 | … | 24 }, when *interface-type* is 1, *interface-number* = { 1 | 2 }..

Description

Use **show qos interface** command to display the QoS information of all Ethernet ports or a specified port.

Examples

#display the qos information of all ports
XS# **show qos interface**

```
PORT           DEFAULT PRIORITY        DSCP
-----------  -------------------- ------
Ethernet0/1          0                disabled
Ethernet0/2          0                disabled
Ethernet0/3          0                disabled
Ethernet0/4          0                disabled
Ethernet0/5          0                disabled
Ethernet0/6          0                disabled
Ethernet0/7          0                disabled
Ethernet0/8          0                disabled
Ethernet0/9          0                disabled
Ethernet0/10         0                disabled
Ethernet0/11         0                disabled
Ethernet0/12         0                disabled
Ethernet0/13         0                disabled
Ethernet0/14         0                disabled
Ethernet0/15         0                disabled
Ethernet0/16         0                disabled
Ethernet0/17         0                disabled
Ethernet0/18         0                disabled
Ethernet0/19         0                disabled
Ethernet0/20         0                disabled
Ethernet0/21         0                disabled
Ethernet0/22         0                disabled
Ethernet0/23         0                disabled
Ethernet0/24         0                disabled
Ethernet1/1          0                disabled
Ethernet1/2          0                disabled
```

#display the qos information of Ethernet port 0/1
XS# **show qos interface ethernet** *0/1*

```
PORT           DEFAULT PRIORITY       DSCP
-----------      -------------------      ------
Ethernet0/1          0                disabled
```

qos queue-scheduler

Syntax

qos queue-scheduler {strict-priority | wrr *queue0-weight queue1-weight queue2-weight queue3-weight***}**
no qos queue-scheduler

View

System view.

Parameters

strict-priority: uses the Strict Priority (SP) algorithm for queue scheduling.
wrr: uses the Weighted Round Robin (WRR) algorithm for queue scheduling.
queue0-weight queue1-weight queue2-weight queue3-weight: customizes the weights to be assigned to queues 0 through 3. The value ranges from 0 to 55. A value of 0 means the corresponding queue adopts the SP algorithm for queue scheduling.

Description

Use **qos queue-scheduler** command to configure the queue scheduling algorithm and the related parameters.
Use **no qos queue-scheduler** command to restore to the default setting.
By default, the SP algorithm is used for all output queues of a port.

Examples

XS# **qos queue-scheduler wrr** *1 2 3 4*
The configuration is successful.

qos cos-local-precedence-map

Syntax

qos cos-local-precedence-map *cos0-map-local-prec cos1-map-local-prec cos2-map-local-prec cos3-map-local-prec cos4-map-local-prec cos5-map-local-prec cos6-map-local-prec cos7-map-local-prec*
no qos cos-local-precedence-map

View

System view.

Parameters

cos0-map-local-prec: Local precedence to which 802.1p 0 is to be mapped, in the range 0 to 3.
cos1-map-local-prec: Local precedence to which 802.1p 1 is to be mapped, in the range 0 to 3.
cos2-map-local-prec: Local precedence to which 802.1p 2 is to be mapped, in the range 0 to 3.
cos3-map-local-prec: Local precedence to which 802.1p 3 is to be mapped, in the range 0 to 3.
cos4-map-local-prec: Local precedence to which 802.1p 4 is to be mapped, in the range 0 to 3.
cos5-map-local-prec: Local precedence to which 802.1p 5 is to be mapped, in the range 0 to 3.
cos6-map-local-prec: Local precedence to which 802.1p 6 is to be mapped, in the range 0 to 3.
cos7-map-local-prec: Local precedence to which 802.1p 7 is to be mapped, in the range 0 to 3.

Description

Use **qos cos-local-precedence-map** command to configure the mapping between 802.1p priority and local precedence.
Use **no qos cos-local-precedence-map** command to restore to default settings.
The following table lists the default 802.1p priority-to-local precedence mapping.

802.1p priority	Local precedence
0	0
1	0
2	1
3	1
4	2

5	2
6	3
7	3

Examples

XS# **qos cos-local-precedence-map** *3 3 2 2 1 1 0 0*
The configuration succeeds.

qos map

Syntax

qos map dscp *dscp* **to cos** *cos*
no qos map dscp *dscp*

View

System view.

Parameters

dscp *dscp*: the DSCP priority, this argument ranges from 0 to 63.
cos *cos*: the 802.1p priority, this argument ranges from 0 to 7.

Description

Use **qos map** command to map a DSCP priority to an 802.1p priority.
Use **no qos map** command to restore to default settings.
The default DSCP priority to 802.1p priority mapping is 0.

Examples

XS# **qos map dscp** *0* **to cos** *7*
The configuration succeeds.

qos-mode dscp

Syntax

qos-mode dscp
no qos-mode dscp

View

Ethernet port view

Parameters

None.

Description

Use **qos-mode dscp** command to enable DSCP priority.
Use **no qos-mode dscp** command to disable DSCP priority.
By default, the DSCP priority is disabled.

Examples

XS(Ethernet0/1)# **qos-mode dscp**
Dscp is enabled on port ethernet0/1.

priority

Syntax

priority *priority-level*
no priority

View

Ethernet port view

Parameters

priority-level: port priority, ranging from 0 to 7.

Description

Use **priority** command to set the priority of a port.
Use **no priority** command to restore to the default.
By default, the priority of an Ethernet port is 0.

After executing **priority** command on a port, the port priority will be used to identify the matching local precedence for the packet (in the 802.1p-priority-to-local-precedence mapping table) regardless of what is the 802.1p priority of each inbound 802.1q-tagged packet. The packet is then assigned to an output queue corresponding to the local precedence.

Examples

XS(Ethernet0/1)# **no priority**
802.1p default priority restored to default 0 on port ethernet0/1

3.15 MAC Address Table Management Commands

The "Any view" in the below table refers to anyone of the following: System view, Ethernet port view, Port-based VLAN view, VLAN view, or dot1x view.

Command list:

View	Command
Any view	**show mac-address-table**
Any view	**show mac-address aging-time**
Any view	**show mac-address { static | dynamic | blackhole } [interface ethernet** *interface-number* **] [vlan** *vlan-id* **]** **show mac-address address** *mac-address* **[vlan** *vlan-id* **] [count]** **show mac-address interface ethernet** *interface-number* **[vlan** *vlan-id* **]** **show mac-address vlan** *vlan-id* **[count]** **show mac-address count**
System view	**mac-address { static | dynamic | blackhole }** *mac-address* **interface ethernet** *interface-number* **vlan**

	vlan-id **no mac-address { static | dynamic | blackhole }** *mac-address* **vlan** *vlan-id* **no mac-address interface ethernet** *interface-number* **no mac-address vlan** *vlan-id* **no mac-address vlan** *vlan-id mac-address*
Ethernet port view	**mac-address { static | dynamic | blackhole }** *mac-address* **vlan** *vlan-id* **no mac-address { static | dynamic | blackhole }** *mac-address* **vlan** *vlan-id*
System view	**mac-address timer aging** *age* **mac-address timer no-aging** **no mac-address timer**

show mac-address-table

Syntax

show mac-address-table

View

Any view.

Parameters

None.

Description

Use **show mac-address-table** command to display information of all MAC address entries in MAC address table, including: MAC address, VLAN and port corresponding to the MAC address, the type (static learned or dynamic) of a MAC address entry, whether a MAC address is within the aging time, and so on.

Examples

XS# **show mac-address-table**
show the mac address table

MAC ADDRESS	VLAN ID	STATE	PORT	AGING
00-1d-0f-7f-62-18	3	Learned	Ethernet0/7	Yes
00-1d-7d-76-1a-46	3	Learned	Ethernet0/7	Yes
00-80-77-94-dd-92	3	Dynamic	Ethernet0/7	Yes
00-0d-61-45-71-d3	3	Dynamic	Ethernet0/7	Yes
00-1d-7d-74-fa-71	3	Dynamic	Ethernet0/7	Yes
00-1f-d0-6a-df-59	3	Dynamic	Ethernet0/7	Yes
00-0e-1f-01-80-74	3	Learned	Ethernet0/7	Yes
00-1d-7d-44-a8-f7	3	Learned	Ethernet0/7	Yes
00-1d-7d-44-a9-23	3	Learned	Ethernet0/7	Yes
00-1f-d0-6a-de-f0	3	Dynamic	Ethernet0/7	Yes
00-0c-6e-c6-54-85	3	Learned	Ethernet0/7	Yes
00-1d-7d-44-a9-37	3	Learned	Ethernet0/7	Yes
00-0f-ea-4f-36-e5	3	Learned	Ethernet0/7	Yes
00-30-e3-fd-12-98	3	Dynamic	Ethernet0/7	Yes
00-40-63-ca-5b-79	3	Learned	Ethernet0/7	Yes
00-1d-7d-4c-f7-4e	3	Learned	Ethernet0/7	Yes
00-1d-7d-3f-63-ad	3	Learned	Ethernet0/7	Yes
00-1e-68-6a-ae-3d	3	Learned	Ethernet0/7	Yes
00-21-70-b9-62-4f	3	Learned	Ethernet0/7	Yes

```
00-1d-7d-41-46-09       3          Dynamic      Ethernet0/7        Yes
00-0a-0b-0c-0e-09       3          Learned      CPU                Yes
00-1a-4d-23-32-0a       3          Learned      Ethernet0/7        Yes
00-16-ec-5a-b6-fe       3          Dynamic      Ethernet0/7        Yes
00-1a-4d-3a-2a-d8       3          Learned      Ethernet0/7        Yes
00-1d-72-09-fa-b4       3          Learned      Ethernet0/7        Yes
00-1a-4d-6a-8b-64       3          Learned      Ethernet0/7        Yes
00-1e-68-6a-b5-3f       3          Learned      Ethernet0/7        Yes
00-1a-4d-38-9f-a6       3          Learned      Ethernet0/7        Yes
00-1a-4d-6a-8a-de       3          Learned      Ethernet0/7        Yes
00-0a-0b-0c-0e-09       1          Static       CPU                No
00-0d-61-4e-f5-e4       3          Dynamic      Ethernet0/7        Yes
02-10-18-58-36-11       3          Learned      Ethernet0/7        Yes
00-0d-61-97-b6-cc       3          Dynamic      Ethernet0/7        Yes
00-0d-61-97-a6-b4       3          Dynamic      Ethernet0/7        Yes
34 mac addresses found
```

show mac-address aging-time

Syntax

show mac-address aging-time

View

Any view.

Parameters

None.

Description

Use **show mac-address aging-time** command to display the aging time of the dynamic MAC address entries in MAC address table.

Examples

```
XS# show mac-address aging-time
The aging time of mac address is 300s.
```

show mac-address

Syntax

show mac-address { static | dynamic | blackhole} [interface ethernet *interface-number* **] [vlan** *vlan-id* **]**
show mac-address address *mac-address* **[vlan** *vlan-id* **]**
show mac-address interface ethernet *interface-number* **[vlan** *vlan-id* **]**
show mac-address vlan *vlan-id* **[count]**
show mac-address count

View

Any view.

Parameters

static: displays static MAC address entries.

dynamic: displays dynamic MAC address entries.
blackhole: displays blackhole MAC address entries.
interface ethernet *interface-number*: specifies a port by its interface type and number, of which the MAC address entries are displayed.
vlan *vlan-id*: specifies a VLAN by its ID in a range from 1 to 4094, for which the MAC address entries are displayed.
address *mac-address*: specifies a MAC address, in the form of H-H-H-H-H-H.
count: displays the total number of MAC address entries.

Description

Use **show mac-address** command to display information of certain MAC address entries in MAC address table, including: MAC address, VLAN and port corresponding to the MAC address, the type (static or dynamic) of a MAC address entry, whether a MAC address is within the aging time, and so on.

Examples

#display the static MAC address entries for the vlan 1
XS# **show mac-address static vlan** *1*

MAC ADDRESS	VLAN ID	STATE	PORT	AGING
00-1d-72-23-ed-8f	1	Static	2	No
00-1d-72-23-ed-8e	1	Static	1	No

2 static mac addresses found in 1 vlan

#display the MAC address entries for the port Ethernet 0/1
XS# **show mac-address interface ethernet** *0/1*

MAC ADDRESS	VLAN ID	STATE	PORT	AGING
00-1d-72-23-ed-8d	1	BlackHole	Ethernet0/1	No
00-1d-72-23-ed-8e	1	Static	Ethernet0/1	No

2 mac addresses found on port Ethernet0/1

mac-address

Syntax

In System view:
mac-address { static | dynamic | blackhole } *mac-address* **interface ethernet** *interface-number* **vlan** *vlan-id*
no mac-address { static | dynamic | blackhole } *mac-address* **vlan** *vlan-id*
no mac-address interface ethernet *interface-number*
no mac-address vlan *vlan-id*
no mac-address vlan *vlan-id mac-address*

In Ethernet port view:
mac-address { static | dynamic | blackhole } *mac-address* **vlan** *vlan-id*
no mac-address { static | dynamic | blackhole } *mac-address* **vlan** *vlan-id*

View

System view, Ethernet port view

Parameters

static: specifies a static MAC address entry.
dynamic: specifies a dynamic MAC address entry.
blackhole: specifies a blackhole MAC address entry.
mac-address: specifies a MAC address, in the form of H-H-H-H-H-H.

interface ethernet *interface-number*: specifies the outgoing port by its type and number for the MAC address. All traffic destined for the MAC address will be sent out from the port.
vlan *vlan-id*: specifies a VLAN ID, in a range from 1 to 4094. The VLAN must exist.

Description

Use **mac-address** command to add or modify a MAC address entry.
Use **no mac-address** command to remove one or more MAC address entries.

In Ethernet port view, the MAC address entry configured by **mac-address** command takes the Ethernet port as an outgoing port. If the MAC address you input in the **mac-address** command already exists in the MAC address table, the system will modify the attributes of the corresponding MAC address entry according to your settings in the command.

You can remove all unicast MAC address entries on a port, or remove a specific type of MAC address entries, such as the addresses learnt by the system, dynamic or static MAC address entries configured, or blackhole addresses.

Examples

XS# **mac-address dynamic** *00-1d-72-23-ed-70* **interface ethernet** *0/13* **vlan** *3*
The configuration is successful.

XS# **no mac-address vlan** *3*
Delete mac address successfully.

mac-address timer

Syntax

mac-address timer aging *age*
mac-address timer no-aging
no mac-address timer

View

System view

Parameters

aging *age*: specifies the aging time (in seconds) for dynamic MAC address entries. The *age* argument ranges from 10 to 1000000.
no-**aging**: specifies not-to-age dynamic MAC address entries.

Description

Use **mac**-**address timer** command to set MAC address aging timer.
Use **no mac**-**address timer** command to restore to the default.
The default MAC address aging timer is 300 seconds.

The timer applies only to dynamic address entries, including both entries learned and configured.

Setting an appropriate MAC address aging timer is important for the switch to run efficiently.

- If the aging timer is set too short, the MAC address entries that are still valid may be removed due to aging. Upon receiving a packet destined for a MAC address that is already removed, the switch broadcasts the packet to all ports within the VLAN to which the packet belongs. This decreases the operating performance.
- If the aging timer is set too long, MAC address entries may still exist even if they turn into invalid. This causes the switch to be unable to update its MAC address table in time. In this case, the MAC address table cannot reflect the change of network devices in time.

Examples

XS# **mac-address timer aging** *500*
Aging time of dynamic MAC address is 500 seconds.

3.16 Multicast Commands

The "Any view" in the below table refers to anyone of the following: System view, Ethernet port view, Port-based VLAN view, VLAN view, or dot1x view.

Command list:

View	Command
Any view	**show mac-address multicast [count | static { all | count |** *mac-address* **vlan** *vlan-id* **}]**
System view	**mac-address multicast** *mac-address* **interface ethernet** *interface* **[to ethernet** *interface* **] vlan** *vlan-id* **no mac-address multicast** { **all** | **interface ethernet** *interface* [**to ethernet** *interface*] **vlan** *vlan-id* | *mac-address* **vlan** *vlan-id* }
Ethernet port view	**mac-address multicast** *mac-address* **vlan** *vlan-id* **no mac-address multicast** *mac-address* **vlan** *vlan-id*

show mac-address multicast

Syntax

show mac-address multicast [count | static { all | count | *mac-address* **vlan** *vlan-id* **}]**

View

Any view

Parameters

mac-address: displays the static multicast MAC entry information for the specified MAC address.
vlan *vlan-id*: displays the static multicast MAC entry information in the specified VLAN.
count: displays the number of static multicast MAC entries.

Description

Use **show mac-address multicast** command to display the information of the multicast MAC address entry or entries manually configured on the switch.

Examples

XS# **show mac-address multicast**
show all of the multicast mac-address

Vlan ID :1
MAC address :01-00-5e-00-00-e1
Port Member :Ethernet0/2, Ethernet0/4, Ethernet0/6, Ethernet0/8,

Vlan ID :1
MAC address :01-00-5e-00-00-e0
Port
Member :Ethernet0/1,Ethernet0/2,Ethernet0/3,Ethernet0/4,Ethernet0/5,

Total Entries : 2

mac-address multicast

Syntax

In System view:
mac-address multicast *mac-address* **interface ethernet** *interface* **[to ethernet** *interface* **] vlan** *vlan-id*

no mac-address multicast { all | interface ethernet *interface* **[to ethernet** *interface* **] vlan** *vlan-id* **|** ***mac-address*** **vlan** *vlan-id* **}**

In Ethernet port view:
mac-address multicast *mac-address* **vlan** *vlan-id*
no mac-address multicast *mac-address* **vlan** *vlan-id*

View

System view, Ethernet port view

Parameters

mac-address: multicast MAC address, in the form of H-H-H-H-H-H.
vlan *vlan-id*: specifies the VLAN to which the forwarding ports belong. The effective range for *vlan-id* is from 1 to 4094.
interface : ethernet port, in the form of *interface* = { *interface-type***/***interface-number*}, *interface-type* = {0 | 1}, when *interface-type* is 0, *interface-number* = { 1 | 2 | … | 24 }, when *interface-type* is 1, *interface-number* = { 1 | 2 }.

Description

Use **mac-address multicast interface** command to create a multicast MAC address entry.
Use **no mac-address multicast interface** command to remove the specified multicast MAC address entry or all multicast MAC address entries.
Use **mac-address multicast vlan** command to create a multicast MAC address

entry on the port.
Use **no mac-address multicast vlan** command to remove the specified multicast MAC address entry or all multicast MAC address entries on the port.
Each multicast MAC address entry contains multicast address, forward port, VLAN ID, and so on.

Examples

XS# mac-address multicast *01-00-5e-00-00-e8* interface ethernet *0/7* to ethernet *0/8* vlan *2*
The configuration succeeds.

XS(Ethernet0/8)# no mac-address multicast 01-00-5e-00-00-e8 vlan 2

Delete successfully.

3.17 IGMP Snooping Configuration Commands

The "Any view" in the below table refers to anyone of the following: System view, Ethernet port view, Port-based VLAN view, VLAN view, or dot1x view.

Command list:

View	Command
Any view	**show igmp-snooping configuration**
Any view	**show igmp-snooping group [vlan** *vlan-id* **]**
System view VLAN view	**igmp-snooping** **no igmp-snooping**
System view	**igmp-snooping querier** **no igmp-snooping querier**
System view	**igmp-snooping query-interval [time** *seconds***]** **no igmp-snooping query-interval**
System view	**igmp-snooping host-aging-time** *seconds* **no igmp-snooping host-aging-time**
System view	**igmp-snooping router-aging-time** *seconds* **no igmp-snooping router-aging-time**
System view	**igmp-snooping leave-time** *seconds* **no igmp-snooping leave-time**
System view	**igmp-snooping max-response-time** *seconds* **no igmp-snooping max-response-time**
VLAN view	**multicast static-router-port ethernet** *interface-number* **no multicast static-router-port ethernet** *interface-number*

show igmp-snooping configuration

Syntax

show igmp-snooping configuration

View

Any view.

Parameters

None.

Description

Use **show igmp-snooping configuration** command to display IGMP Snooping configuration information.
If IGMP Snooping is disabled, this command displays a message showing that IGMP Snooping is not enabled.
With IGMP Snooping enabled, this command displays the following information:

- IGMP Snooping status
- aging time of the host port
- aging time of the router port
- IGMP querying
- querying transmit timer
- max response timer
- leave timer

Examples

XS# **show igmp-snooping configuration**
show igmp-snooping configuration

XS# show igmp-snooping configuration
show igmp-snooping configuration

```
Igmp-snooping global state      :Disabled
Host Timeout                    :260
Route Timeout                   :105
IGMP Querier                    :Disabled
Query Transmit Interval         :125
Max Response Time                 :10
Last Member Query Interval        :1
```

show igmp-snooping group

Syntax

show igmp-snooping group [vlan *vlan-id* **]**

View

Any view.

Parameters

vlan *vlan-id*: specifies the VLAN in which the multicast group information is to be displayed, where *vlan-id* ranges from 1 to 4094. If you do not specify a VLAN, this command displays the multicast group information of all VLANs.

Description

Use **show igmp-snooping group** command to display the IGMP Snooping multicast group information.

Examples

#display the information about the multicast groups of all VLANs.
XS# **show igmp-snooping group**

show igmp-snooping group information

Vlan ID :1
Multicast group :239.0.0.10
MAC address :01-00-5e-00-00-0a
Port Member :Ethernet0/4,

Total Entries : 1

igmp-snooping

Syntax

igmp-snooping
no igmp-snooping

View

System view, VLAN view.

Parameters

None.

Description

Use **igmp-snooping** command to enable the IGMP Snooping feature.
Use **no igmp-snooping** command to disable the IGMP Snooping feature.
By default, the IGMP Snooping feature is disabled.

Examples

XS(vlan3)# **igmp-snooping**
Igmp-snooping is enabled on vlan 3.

igmp-snooping querier

Syntax

igmp-snooping querier
no igmp-snooping querier

View

System view

Parameters

None.

Description

Use **igmp-snooping querier** command to enable IGMP qurier**.**
Use **no igmp-snooping querier** command to disbale IGMP qurier**.**
By default, igmp-snooping querier is disabled.

Examples

XS# igmp-snooping querier
IGMP querier has been enabled.
XS# no igmp-snooping querier
IGMP querier has been disabled.

igmp-snooping query-interval

Syntax

igmp-snooping query-interval [time *seconds***]**
no igmp-snooping query-interval

View

System view

Parameters

seconds: time of query transmit interval, in a range from 1 to 300, in seconds.

Description

Use **igmp-snooping query-interval** command to set the igmp snooping query transmit interval.
Use **no igmp-snooping query-interval** command to make the query transmit interval restore to the default setting.
By default, the query transmit interval is configured as 125 seconds.

Examples

XS# igmp-snooping query-interval 30
Query-interval of igmp-snooping has been set to 30 seconds

XS# no igmp-snooping query-interval
The query transmit interval has been restored to default 125 seconds.

igmp-snooping host-aging-time

Syntax

igmp-snooping host-aging-time *seconds*
no igmp-snooping host-aging-time

View

System view.

Parameters

seconds: aging time (in seconds) of multicast member ports, in a range from 200 to 1,000.

Description

Use **igmp-snooping host-aging-time** command to configure the aging time of multicast member ports.
Use **no igmp-snooping host-aging-time** command to restore to the default

aging time.
By default, the aging time of multicast member ports is 260 seconds.
The aging time of multicast member ports determines the refresh frequency of multicast group members. In an environment where multicast group members change frequently, a relatively shorter aging time is required.

Examples

XS# **igmp-snooping host-aging-time** *300*
Host-aging-time of igmp-snooping set to 300 seconds

igmp-snooping router-aging-time

Syntax

igmp-snooping router-aging-time *seconds*
no igmp-snooping router-aging-time

View

System view.

Parameters

seconds: aging time of router ports, in a range from 1 to 1,000, in seconds.

Description

Use **igmp-snooping router-aging-time** command to configure the aging time of router ports.
Use **no igmp-snooping router-aging-time** command to restore to the default aging time.
By default, the aging time of router ports is 105 seconds.

Examples

XS# **igmp-snooping router-aging-time** *200*
Router-aging-time of igmp-snooping set to 200 seconds

igmp-snooping leave-time

Syntax

igmp-snooping leave-time *seconds*
no igmp-snooping leave-time

View

System view.

Parameters

seconds: IGMP leave timer, in a range from 1 to 300, in seconds.

Description

Use **igmp-snooping leave-time** command to configure the IGMP query interval, i.e. the interval at which the switch sends IGMP general queries.
Use **no igmp-snooping leave-time** command to restore to the default.

By default, the leave timer is 30 seconds.

Examples

XS# **igmp-snooping leave-time** *200*
Leave-time of igmp-snooping set to 200 seconds

igmp-snooping max-response-time

Syntax

igmp-snooping max-response-time *seconds*
no igmp-snooping max-response-time

View

System view.

Parameters

seconds: maximum response time in IGMP general queries, in a range from 1 to 25, in seconds.

Description

Use **igmp-snooping max-response-time** command to configure the maximum response time in IGMP general queries.
Use **no igmp-snooping max-response-time** command to restore to the default.
By default, the maximum response time in IGMP general queries is 10 seconds.

An appropriate setting of the maximum response time in IGMP queries allows hosts to respond to queries quickly and thus the querier can learn the existence of multicast members quickly.

Examples

XS# **igmp-snooping max-response-time** *20*
Max_response_time of igmp-snooping set to 20 seconds

multicast static-router-port

Syntax

multicast static-router-port ethernet *interface-number*
no multicast static-router-port ethernet *interface-number*

View

VLAN view.

Parameters

interface-number : ethernet port, in the form of interface = { interface-type/interface-number}, interface-type = {0 | 1}, when interface-type is 0, interface-number = { 1 | 2 | … | 24 }, when interface-type is 1, interface-number = { 1 | 2 }.

Description

Use **multicast static-router-port** command to configure the specified port in the VLAN as a static router port.
Use **no multicast static-router-port** command to remove the specified port from the VLAN as a static router port.
By default, a port is not a static router port.

Examples

XS(vlan2)# **multicast static-router-port ethernet** *0/3*
Succeed.

3.18 802.1x Configuration Commands

The "Any view" in the below table refers to anyone of the following: System view, Ethernet port view, Port-based VLAN view, VLAN view, or dot1x view.

Command list:

View	Command
Any view	**show dot1x** { **status** | **interface** [**ethernet** *interface*] }
System view	**dot1x**
dot1x view	**end**
dot1x view	**max-req**
dot1x view	**timeout** { **quiet-period** *quiet-period-value* | **reauth-period** *reauth-period-value* | **server** *server-timeout-value* | **supplicant** *supp-timeout-value* | **tx-period** *tx-period-value* } **no timeout** { **quiet-period** *quiet-period-value* | **reauth-period** *reauth-period-value* | **server** *server-timeout-value* | **supplicant** *supp-timeout-value* | **tx-period** *tx-period-value* }
dot1x view	**system-auth-control** **no system-auth-control**
dot1x view	**radius-server host** *host-ip-address* **auth-port** *auth-port-number* **[acct-port** *acct-port-number* **] key** *key-string*
Ethernet port view	**dot1x** **no dot1x**
Ethernet port view	**dot1x re-authentication** **no dot1x re-authentication**
Ethernet port view	**dot1x port-control** { **auto** | **forceauthorized** | **forceunauthorized** }

show dot1x

Syntax

show dot1x { **status** | **interface** [**ethernet** *interface*] }

View

Any view.

Parameters

status: displays the information of 802.1x.
interface: displays the 802.1x-related information of all ports.
ethernet *interface*: displays the 802.1x-related information of a specified port.
interface : ethernet port, in the form of *interface* = { *interface-type*/*interface-number*}, *interface-type* = {0 | 1}, when *interface-type* is 0, *interface-number* = { 1 | 2 | … | 24 }, when *interface-type* is 1, *interface-number* = { 1 | 2 }.

Description

Use **show dot1x** command to display 802.1x related information.

Examples

#display 802.1x-related information.
XS# dot1x
XS(dot1x)# system-auth-control
802.1x has been enabled
Configuration completed successfully.

XS(dot1x)# show dot1x status
802.1x is enabled

Radius authentication server configuration:
authentication IP address :192.168.0.234
authentication port :1812
authentication key :admin

Radius accounting server configuration:
accounting IP address :192.168.0.234
accounting port :1813
accounting key :admin

misc configuration:
quiet period :60
server timeout :30
supplicant timeout :30
tx period :30
reauth max count :2
reauth period :3600

display the 802.1x-related information of all ports
XS# **show dot1x interface**

PORT	802.1X ADMIN	PORTCONTROL	REAUTH	STATUS
Ethernet0/1	Disabled	ForceAuthorized	Disabled	Link down
Ethernet0/2	Disabled	ForceAuthorized	Disabled	Link down
Ethernet0/3	Disabled	ForceAuthorized	Disabled	Link down
Ethernet0/4	Disabled	ForceAuthorized	Disabled	Link down
Ethernet0/5	Disabled	ForceAuthorized	Disabled	Link down
Ethernet0/6	Disabled	ForceAuthorized	Disabled	Link down
Ethernet0/7	Disabled	ForceAuthorized	Disabled	Authorized
Ethernet0/8	Disabled	ForceAuthorized	Disabled	Link down
Ethernet0/9	Disabled	ForceAuthorized	Disabled	Link down
Ethernet0/10	Disabled	ForceAuthorized	Disabled	Link down
Ethernet0/11	Disabled	ForceAuthorized	Disabled	Link down
Ethernet0/12	Disabled	ForceAuthorized	Disabled	Link down
Ethernet0/13	Disabled	ForceAuthorized	Disabled	Link down
Ethernet0/14	Disabled	ForceAuthorized	Disabled	Link down
Ethernet0/15	Disabled	ForceAuthorized	Disabled	Link down

```
Ethernet0/16      Disabled       ForceAuthorized      Disabled       Link down
Ethernet0/17      Disabled       ForceAuthorized      Disabled       Link down
Ethernet0/18      Disabled       ForceAuthorized      Disabled       Link down
Ethernet0/19      Disabled       ForceAuthorized      Disabled       Link down
Ethernet0/20      Disabled       ForceAuthorized      Disabled       Link down
Ethernet0/21      Disabled       ForceAuthorized      Disabled       Link down
Ethernet0/22      Disabled       ForceAuthorized      Disabled       Link down
Ethernet0/23      Disabled       ForceAuthorized      Disabled       Link down
Ethernet0/24      Disabled       ForceAuthorized      Disabled       Link down
Ethernet1/1       Disabled       ForceAuthorized      Disabled       Link down
Ethernet1/2       Disabled       ForceAuthorized      Disabled       Link down

# display the 802.1x-related information of a specified port
XS# show dot1x interface ethernet 0/1
PORT              802.1X ADMIN    PORTCONTROL       REAUTH       STATUS
Ethernet0/1       Disabled        ForceAuthorized    Disabled     Link down
```

dot1x

Syntax

dot1x

View

System view.

Parameters

None.

Description

Enter into 802.1x configuration environment.

Examples

```
XS# dot1x
XS(dot1x)#
```

end

Syntax

end

View

dot1x view

Parameters

None.

Description

Exit from 802.1x configuration environment.

Examples

XS(dot1x)# **end**
XS#

max-req

Syntax

max-req *max-retry-value*

View

dot1x view

Parameters

max-retry-value: Maximum number of times that a switch sends authentication request packets to a user. This argument ranges from 1 to 10.

Description

By default, a switch sends authentication request packets to a user for up to 2 times.
After a switch sends an authentication request packet to a user, it will send another authentication request packet if it has not received response from the user after a specific period of time. If the switch still receives no response when the configured maximum number of authentication request transmission attempts is reached, it stops sending requests to the user. This command applies to all ports.

Examples

XS(dot1x)# **max-req** *5*
Max request count is 5.

timeout

Syntax

timeout { quiet-period *quiet-period-value* | **reauth-period** *reauth-period-value* | **server** *server-timeout-value* | **supplicant** *supp-timeout-value* | **tx-period** *tx-period-value* }
no timeout { quiet-period *quiet-period-value* | **reauth-period** *reauth-period-value* | **server** *server-timeout-value* | **supplicant** *supp-timeout-value* | **tx-period** *tx-period-value* }

View

dot1x view

Parameters

quiet-period *quiet-period-value*: sets the quiet-period timer. This timer sets the quiet-period. When a supplicant system fails to pass the authentication, the switch quiets for the set period (set by the quiet-period timer) before it processes another authentication request re-initiated by the supplicant system. During this quiet period, the switch does not perform any 802.1x authentication-related actions for the supplicant system.

The *quiet-period-value* argument ranges from 1 to 65535 (in seconds). By default,

the quiet-period timer is set to 60 seconds.

reauth-period *reauth-period-value*: specifies re-authentication interval, in seconds. After this timer expires, the switch initiates 802.1x re-authentication. The value of the *reauth-period-value* argument ranges from 60 to 7200. By default, the reauth-period timer is set to 3600 seconds.

server *server-timeout-value*: sets the RADIUS server timer. This timer sets the server-timeout period. After sending an authentication request packet to the RADIUS server, a switch will send another authentication request packet if it has not received the response from the RADIUS server when this timer times out.
The *server-timeout-value* argument ranges from 1 to 300 (in seconds). By default, the RADIUS server timer is set to 30 seconds.

supplicant *supp-timeout-value*: sets the supplicant system timer. This timer sets the supp-timeout period and is triggered by the switch after the switch sends a request/challenge packet to a supplicant system (The packet is used to request the supplicant system for the MD5 encrypted string). The switch will send another request/challenge packet to the supplicant system if the switch does not receive the response from the supplicant system when this timer times out.

The *supp-timeout-value* argument ranges from 1 to 300 (in seconds). By default, the supplicant system timer is set to 30 seconds.

tx-period *tx-period-value*: sets the transmission timer. This timer sets the tx-period and is triggered in two cases. The first case is when the client requests for an authentication. The switch sends a unicast request/identity packet to a supplicant system and then triggers the transmission timer. The switch will send another request/identity packet to the supplicant system if it has not received the reply packet from the supplicant system when this timer times out. The second case is when the switch authenticates the 802.1x client who cannot request for authentication actively. The switch sends multicast request/identity packets periodically through the port with 802.1x function enabled. In this case, this timer sets the interval of sending the multicast request/identity packets.

The *tx-period-value* argument ranges from 1 to 65535 (in seconds). By default, the transmission timer is set to 30 seconds.

Description

Use **timeout** command to set a specified 802.1x timer.
Use **no timeout** command to restore a specified 802.1x timer to the default setting.

Examples

XS(dot1x)# **timeout quiet-period** *120*
Timeout of the quiet period is 120 seconds.

system-auth-control

Syntax

system-auth-control
no system-auth-control

View

dot1x view

Parameters

None.

Description

Use **system-auth-control** command to enable 802.1x globally.
Use **no system-auth-control** command to disable 802.1x globally.

Examples

XS(dot1x)# **system-auth-control**
802.1x is enabled
The configuration succeeds.

radius-server

Syntax

radius-server host *host-ip-address* **auth-port** *auth-port-number* **[acct-port** *acct-port-number* **] key** *key-string*

View

dot1x view

Parameters

host *host-ip-address*: IP address of the radius server to be used, a valid unicast address in dotted decimal notation, the default value is 192.168.0.234.
auth-port *auth-port-number*: UDP port number of the radius server, ranging from 1 to 65535, the default value is 1812.
acct-port *acct-port-number*: UDP port number of the radius server, ranging from 1 to 65535, the default value is 1813.
key *key-string*: sets a shared key for radius messages. String length is from 1 to 15 characters.

Description

Use radius-server command to set radius server related configurations.

Examples

XS(dot1x)# **radius-server host** *192.168.0.222* **auth-port** *1855* **acct-port** *1856* **key** *admin*
The configuration succeeds.

dot1x

Syntax

dot1x
no dot1x

View

Ethernet port view

Parameters

None.

Description

Use **dot1x** command to enable 802.1x for the specified Ethernet port.
Use **no dot1x** command to disable 802.1x for the specified Ethernet port.

Examples

XS(Ethernet0/1)# **dot1x**
802.1x is enabled on port ethernet0/1

dot1x re-authentication

Syntax

dot1x re-authentication
no dot1x re-authentication

View

Ethernet port view

Parameters

None.

Description

Use **dot1x re-authentication** command to enable 802.1x re-authentication for the specified Ethernet port.
Use **no dot1x** command to disable 802.1x re-authentication for the specified Ethernet port.

Examples

XS(Ethernet0/1)# **dot1x re-authentication**
The configuration succeeds.

dot1x port-control

Syntax

dot1x port-control { auto | forceauthorized | forceunauthorized }

View

Ethernet port view

Parameters

auto: specified to operate in **auto** access control mode. When a port operates in this mode, all the unauthenticated hosts connected to it are unauthorized. In this case, only EAPoL packets can be exchanged between the switch and the hosts. After passing the authentication, the hosts connected to the port are authorized to access the network resources. Normally, a port operates in this mode.

forceauthorized: specified to operate in **forceauthorized** access control mode. When a port operates in this mode, all the hosts connected to it can access the

network resources without the need of authentication.

forceunauthorized: specified to operate in **forceunauthorized** access control mode. When a port operates in this mode, the hosts connected to it cannot access the network resources.

Description

Use **dot1x port-control** command to specify the access control mode for the specified Ethernet port.

Examples

XS(Ethernet0/1)# **dot1x port-control auto**
The configuration succeeds.

3.19 STP Commands

The "Any view" in the below table refers to anyone of the following: System view, Ethernet port view, Port-based VLAN view, VLAN view, or dot1x view.

Command list:

View	Command
Any view	**show spanning-tree [ethernet** *interface* **]**
Any view	**show spanning-tree {ethernet** *ethernet-port* **instance** *mstid* **| mst-configuration | instance** *mstid***}**
System view Ethernet port view	**spanning-tree** **no spanning-tree**
System view	**spanning-tree forward-time** *timer-value* **no spanning-tree forward-time**
System view	**spanning-tree hello-time** *timer-value* **no spanning-tree hello-time**
System view	**spanning-tree max-age** *timer-value* **no spanning-tree max-age**
System view	**spanning-tree priority** *priority* **no spanning-tree priority**
System view	**spanning-tree max-hops** *hops* **no spanning-tree max-hops**
System view	**spanning-tree mode {stp | rstp | mstp}**
Ethernet port view	**spanning-tree hold-count** *num* **no spanning-tree hold-count**
System view	**spanning-tree bpdu-guard** **no spanning-tree bpdu-guard**
Ethernet port view	**spanning-tree root-guard** **no spanning-tree root-guard**
Ethernet port view	**spanning-tree path-cost** *cost* **no spanning-tree path-cost**
Ethernet port view	**spanning-tree priority** *priority* **no spanning-tree priority**
Ethernet port view	**spanning-tree point-to-point** **no spanning-tree point-to-point**
Ethernet port view	**spanning-tree protocol-migration** **no spanning-tree protocol-migration**
Ethernet port view	**spanning-tree edge** **no spanning-tree edge**

System view	**spanning-tree mst-region**
Mst-region view	**instance** *msti* **no instance** *msti*
Mst-region view	**instance** *msti* **ethernet** *ethernet-port* **path-cost** *cost* **no instance** *msti* **ethernet** *ethernet-port* **path-cost** pri
Mst-region view	**instance** *msti* **ethernet** *ethernet-port* **priority** *cost* **no instance** *msti* **ethernet** *ethernet-port* **priority** pri
Mst-region view	**instance** *msti* **priority** *pri* **no instance** *msti priority*
Mst-region view	**instance** *msti* **vlan** *vlan-vid* [**to** *vlan-end-vid*] **no instance vlan** *vlan-vid* [**to** *vlan-end-vid*]
Mst-region view	**region-name** *name*
Mst-region view	**revision-level** *level*

show spanning-tree

Syntax

show spanning-tree [ethernet *interface* **]**

View

Any view.

Parameters

interface : ethernet port, in the form of interface = { interface-type/interface-number}, interface-type = {0 | 1}, when interface-type is 0, interface-number = { 1 | 2 | … | 24 }, when interface-type is 1, interface-number = { 1 | 2}.

Description

Use **show spanning-tree** command to display the settings of STP. If an Ethernet interface is specified, the STP information of this interface will be displayed.

Examples

#display the STP information of all ports
XS(Ethernet0/1)# **show spanning-tree**

The spanning tree is enabled on this switch!

The spanning tree mode is RSTP!

Bridge Priority: 32768
Hello time: 2
Max age time: 20
Forward delay time: 15

Bridge ID: 32768:28-b0-cc-00-31-d4
Root ID: 32768:28-b0-cc-00-31-d4

Interfaces

Port	StpState	Priority	PathCost	PortRole	PortState	Designed Port
Ethernet0/1	Enabled	0	Auto	Disabled	Disabled	0:0

Ethernet0/2	Enabled	128	Auto	Designated	Disabled
1:128					
Ethernet0/3	Enabled	128	Auto	Designated	Disabled
2:128					
Ethernet0/4	Enabled	128	Auto	Designated	Disabled
3:128					
Ethernet0/5	Enabled	128	Auto	Designated	Disabled
4:128					
Ethernet0/6	Enabled	128	Auto	Designated	Disabled
5:128					
Ethernet0/7	Enabled	128	Auto	Designated	Forwarding
6:128					
Ethernet0/8	Enabled	128	Auto	Designated	Disabled
7:128					
Ethernet0/9	Enabled	128	Auto	Designated	Disabled
8:128					
Ethernet0/10	Enabled	128	Auto	Designated	Disabled
9:128					
Ethernet0/11	Enabled	128	Auto	Designated	Disabled
10:128					
Ethernet0/12	Enabled	128	Auto	Designated	Disabled
11:128					
Ethernet0/13	Enabled	128	Auto	Designated	Disabled
12:128					
Ethernet0/14	Enabled	128	Auto	Designated	Disabled
13:128					
Ethernet0/15	Enabled	128	Auto	Designated	Disabled
14:128					
Ethernet0/16	Enabled	128	Auto	Designated	Disabled
15:128					
Ethernet0/17	Enabled	128	Auto	Designated	Disabled
16:128					
Ethernet0/18	Enabled	128	Auto	Designated	Disabled
17:128					
Ethernet0/19	Enabled	128	Auto	Designated	Disabled
18:128					
Ethernet0/20	Enabled	128	Auto	Designated	Disabled
19:128					
Ethernet0/21	Enabled	128	Auto	Designated	Disabled
20:128					
Ethernet0/22	Enabled	128	Auto	Designated	Disabled
21:128					
Ethernet0/23	Enabled	128	Auto	Designated	Disabled
22:128					
Ethernet0/24	Enabled	128	Auto	Designated	Disabled
23:128					
Ethernet1/1	Enabled	128	Auto	Designated	Disabled
24:128					
Ethernet1/2	Enabled	128	Auto	Designated	Disabled
25:128					

#display the STP information of ethernet 0/1 interface
XS(Ethernet0/1)# **show spanning-tree ethernet** *0/1*

Port: Ethernet0/1
STP admin: enabled
Edge Port: Disabled
Point to point: auto
Protocol migration: Disabled
TX hold count: 3

LBD: Disabled
Path cost: 20000
Port priority: 128
STP State: Disabled
STP Role: Disabled
Desigated Port id: 0-0
Designated Path Cost: 0
Designated Bridge id: 0:00-00-00-00-00-00

show spanning-tree

Syntax

show spanning-tree {ethernet *Ethernet-port* **instance** *mstid* **| mst-configuration | instance** *mstid***}**

View

Any view.

Parameters

Ethernet-port : ethernet port, in the form of interface = { interface-type/interface-number}, interface-type = {0 | 1}, when interface-type is 0, interface-number = { 1 | 2 | … | 24 }, when interface-type is 1, interface-number = { 1 | 2 }.
mst-configuration: MST Configuration Identification.
instance mstid : MSTP instance ID, in the range from 0 to 15.

Description

Use **show spanning-tree** command to display the settings of MSTP. If an Ethernet interface and an instance are specified, the MSTP information of this interface in the specified instance will be displayed.
Note: This command is only used in MSTP spanning tree mode.

Examples

```
XS# show spanning-tree

  The spanning tree is enabled on this switch!

  The spanning tree mode is MSTP!

    Bridge Priority: 32768
    Max hops: 20
    Hello time: 2
    Max age time: 20
    Forward delay time: 15

    MSTI 0 VLANS map: 1-4094
    MST Region Name: 28:B0:CC:01:01:64
    MST Revision Level: 0

    Bridge ID: 32768:28-b0-cc-00-31-d4
    Root ID: 32768:28-b0-cc-00-31-d4     Root PortId: 0-0

Interfaces
      Port      Priority   PathCost   PortRole    PortState   D.BridgeID       D.PortID
------------ -------- --------- ---------- ----------- -------------- --------
```

```
Ethernet0/1    128        0        Disabled     Disabled   32768:28b0cc0031d4 128:1
Ethernet0/2    128        0        Disabled     Disabled   32768:28b0cc0031d4 128:2
Ethernet0/3    128        0        Disabled     Disabled   32768:28b0cc0031d4 128:3
Ethernet0/4    128        0        Disabled     Disabled   32768:28b0cc0031d4 128:4
Ethernet0/5    128        0        Disabled     Disabled   32768:28b0cc0031d4 128:5
Ethernet0/6    128        0        Designated Forwarding 32768:28b0cc0031d4 128:6
Ethernet0/7    128        0        Disabled     Disabled   32768:28b0cc0031d4 128:7
Ethernet0/8    128        0        Disabled     Disabled   32768:28b0cc0031d4 128:8
Ethernet0/9    128        0        Disabled     Disabled   32768:28b0cc0031d4 128:9

XS# show spanning-tree ethernet 0/3 instance 2

  Port: Ethernet0/3
  STP admin: enabled
  Edge Port: Disabled
  Point to point: Auto
  External Path cost: 200000

        MSTI 2 Ethernet0/3 port information:
  MSTI priority: 128
  MSTI path cost: 0
  MSTI port role: Disabled
  MSTI port state: Disabled
  MSTI designed bridge ID: 43820:4600f4aa4600
  MSTI designed port ID: 0:0

XS# show spanning-tree mst-configuration

 Current MST configuration:
 MST Region Name: 28:B0:CC:01:01:64
 MST Revision Level: 0

 MSTI instance 0 information:
 State: Enabled
 Priority: 32768
 VLAN Mapped: 1-4094

XS# show spanning-tree instance 1
    MSTI 1 VLANS map:
    Bridge ID: 32769:28-b0-cc-00-31-d4
    Root ID: 32769:28-b0-cc-00-31-d4     Root PortId :   0-0

Interfaces
     Port      Priority   PathCost   PortRole    PortState   D.BridgeID       D.PortID
------------ -------- --------- ---------- ----------- -------------- --------
Ethernet0/1    128        0        Disabled     Disabled   32769:28b0cc0031d4 0:00
Ethernet0/2    128        0        Disabled     Disabled   32769:28b0cc0031d4 0:00
Ethernet0/3    128        0        Disabled     Disabled   32769:28b0cc0031d4 0:00
Ethernet0/4    128        0        Disabled     Disabled   32769:28b0cc0031d4 0:00
Ethernet0/5    128        0        Disabled     Disabled   32769:28b0cc0031d4 0:00
```

spanning-tree

Syntax

spanning-tree
no spanning-tree

View

System view, Ethernet port view

Parameters

None.

Description

Use **spanning-tree** command to enable STP globally (in System view) or for a port (in Ethernet port view).
Use **no spanning-tree** command to disable STP globally (in System view) or for a port (in Ethernet port view).
By default, STP is disabled both globally and on ports.

Examples

XS(Ethernet0/1)# **spanning-tree**
Enable ethernet0/1 spanning tree successfully.

spanning-tree forward-time

Syntax

spanning-tree forward-time *timer-value*
no spanning-tree forward-time

View

System view

Parameters

timer-value: forward delay in seconds to be set. This argument ranges from 4 to 30. The default value is 15 seconds.

Description

Use **spanning-tree forward-time** command to set the forward delay of the switch.
Use **no spanning-tree forward-time** command to restore the forward delay to the default value.

By default, the forward delay of the switch is 15 seconds.
To prevent the occurrence of temporary loops, when a port changes its state from discarding to forwarding, it undergoes an intermediate state and waits for a specific period of time to synchronize with the state transition of the remote switches. This state transition period is determined by the forward delay configured on the root bridge.

The forward delay setting configured on a root bridge applies to all non-root bridges. As for the configuration of the three time-related parameters (hello time, forward delay, and max age), the following formulas must be met to prevent network jitter.

- 2 x (forward delay – 1 second) >= max age
- Max age >= 2 x (hello time + 1 second)

Examples

XS# **spanning-tree forward-time** *17*
Configure successfully

spanning-tree hello-time

Syntax

spanning-tree hello-time *timer-value*
no spanning-tree hello-time

View

System view

Parameters

timer-value: hello time in seconds to be set. This argument ranges from 1 to 10. The default value is 2 seconds.

Description

Use **spanning-tree hello-time** command to set the hello time.
Use **no spanning-tree hello-time** command to restore the hello time to the default value.
By default, the hello time is 2 seconds.

A root bridge regularly sends out configuration BPDUs to maintain the stability of existing spanning trees. If the switch does not receive a BPDU packet in a specified period, spanning trees will be recalculated when BPDU packet times out. When a switch becomes a root bridge, it regularly sends BPDUs at the interval specified by the hello time you have configured on it. The other none-root-bridge switches adopt the interval specified by the hello time.

As for the configuration of the three time-related parameters (hello time, forward delay, and max age), the following formula must be met to prevent network jitter.

- 2 × (forward delay – 1 second) >= max age
- Max age >= 2 × (hello time + 1 second)

Examples

XS# **spanning-tree hello-time** *3*
Configure successfully.

spanning-tree max-age

Syntax

spanning-tree max-age *timer-value*
no spanning-tree max-age

View

System view

Parameters

timer-value: max age to be set, in a range from 6 to 40 (seconds). The default value is 20 seconds.

Description

Use **spanning-tree max-age** command to set the max age.
Use **no spanning-tree max-age** command to restore to the default max age.

By default, the max age of a switch is 20 seconds.
To set the three time-related parameters (hello time, forward delay, and max age), the following formulas must be met to prevent network jitter.

- 2 × (forward delay – 1 second) >= max age
- Max age >= 2 × (hello time + 1 second)

Examples

XS# **spanning-tree max-age** *25*
Configure successfully.

spanning-tree priority

Syntax

spanning-tree priority *priority*
no spanning-tree priority

View

System view

Parameters

priority: switch priority to be set. This argument ranges from 0 to 65535. The default value is 32768.

Description

Use **spanning-tree priority** command to set the priority.
Use **no spanning-tree priority** command to restore the priority to default priority.
The default priority is 32768.
The priorities of switches are used for spanning tree calculation.

Examples

XS# **spanning-tree priority** *35000*
Configure stp successfully!

spanning-tree max-hops

Syntax

spanning-tree max-hops *hops*
no spanning-tree max-hops

View

System view

Parameters

hops: switch priority to be set. This argument ranges from 0 to 65535. The default value is 32768.

Description

Use **spanning-tree max-hops** command to set the MSTP max-hops.
Use **no spanning-tree max-hops** command to restore the max-hops to default value.
The default max-hops are 20.

Examples

XS# spanning-tree max-hops 18
Configure successfully

spanning-tree mode

Syntax

spanning-tree mode {stp | rstp | mstp}

View

System view

Parameters

stp: specifies the STP mode.
rstp: specifies the RSTP mode.
mstp: specifies the MSTP mode

Description

Use **stp mode** command to set the operating mode of the switch.
To make the switch compatible with STP/RSTP/MSTP, the following three operating modes are provided.

stp: in this mode, the ports of the switch send STP BPDUs to neighbor devices. In the case that there is a neighbor switch working in RSTP or MSTP mode, the port between them will work in STP mode.

rstp: in this mode, the ports of a switch send RSTP BPDUs to neighbor devices.
mstp: in this mode, the ports of a switch send MSTP BPDUs to neighbor devices.

Examples

XS# **spanning-tree mode stp**
Set successfully

spanning-tree bpdu-guard

Syntax

spanning-tree bpdu-guard
no spanning-tree bpdu-guard

View

System view

Parameters

None.

Description

Use **spanning-tree bpdu-guard** command to enable the bpdu-guard.
Use **no spanning-tree bpdu-guard** command to disable the bpdu-guard.

Examples

XS# spanning-tree bpdu-guard
Set successfully

spanning-tree hold-count

Syntax

spanning-tree hold-count *num*
no spanning-tree hold-count

View

System view

Parameters

hold-count *num*:ranges from 1 to 10.

Description

Use **spanning-tree hold-count** command to set the hold-count for a specified Ethernet port.
Use **no spanning-tree hold-count** command to restore to the default value 3 for a specified Ethernet port.

Examples

XS(Ethernet0/1)# spanning-tree hold-count 5
Set successfully

spanning-tree root-guard

Syntax

spanning-tree root-guard
no spanning-tree root-guard

View

Ethernet port view

Parameters

None.

Description

Use **spanning-tree root-guard** command to enable the root protection function for a specified port on the switch.
Use **no spanning-tree root-guard** command to disable the root protection for a specified port on the switch.

Examples

XS(Ethernet0/1)# **spanning-tree root-guard**
Set successfully

spanning-tree path-cost

Syntax

spanning-tree path-cost *cost*
no spanning-tree path-cost

View

Ethernet port view

Parameters

cost: path cost to be set for the port. The range of the *cost* argument varies with the standard used for calculating the default path cost of a port as follows:
With IEEE 802.1D-1998 standard selected, the path cost of an Ethernet port ranges from 1 to 65535.
With IEEE 802.1t standard selected, the path cost of an Ethernet port ranges from 1 to 200000000.
The argument ranges from 1 to 200000000, and the default value is auto (0) .

Description

Use **spanning-tree path-cost** command to set the path cost(s) of the specified port(s).
Use **no spanning-tree path-cost** command to restore to the default value of the path cost(s) of the specified port(s).

Examples

XS(Ethernet0/1)# **spanning-tree path-cost** 300
Set successfully

spanning-tree priority

Syntax

spanning-tree priority *priority*
no spanning-tree priority

View

Ethernet port view

Parameters

priority: port priority to be set. This argument ranges from 0 to 255, and the default value is 128.

Description

Use **spanning-tree priority** command to set a port priority for the specified ports.
Use **no spanning-tree priority** command to restore to the default priority of the specified ports.

Examples

XS(Ethernet0/1)# **spanning-tree priority** *200*
Set successfully

spanning-tree point-to-point

Syntax

spanning-tree point-to-point
no spanning-tree point-to-point

View

Ethernet port view

Parameters

None.

Description

Use **spanning-tree point-to-point** command to specify that the links connected to the specified Ethernet ports be point-to-point.
Use **no spanning-tree point-to-point** command to specify that the links connected to the specified Ethernet ports be not point-to-point.
By default, the Ethernet ports are point-to-point links.

The rapid transition feature is not applicable to ports connected to non-point-to-point links.

If an Ethernet port is the master port among aggregated ports or operates in full-duplex mode, the link connected to the port is a point-to-point link.

Examples

XS(Ethernet0/1)# **no spanning-tree point-to-point**
Set default value false

spanning-tree protocol-migration

Syntax

spanning-tree protocol-migration
no spanning-tree protocol-migration

View

Ethernet port view

Parameters

None.

Description

Use **spanning-tree protocol-migration** command to enable the protocol migration feature.
Use **no spanning-tree protocol-migration** command to disable the protocol migration feature.
By default, the protocol migration feature is enabled.

Examples

XS(Ethernet0/1)# **no spanning-tree protocol-migration**
Set default value false

spanning-tree edge

Syntax

spanning-tree edge
no spanning-tree edge

View

Ethernet port view

Parameters

None.

Description

Use **spanning-tree edge** command to configure the specified Ethernet ports as edge ports.
Use **no spanning-tree edge** command to configure the specified Ethernet ports as non-edge ports.
By default, all Ethernet ports of a switch are non-edge ports.

An edge port is directly connected to a user terminal instead of through another switch or a network segment. Rapid transition to the forwarding state is applied to edge ports because no loops can be incurred by network topology changes on these ports. You can enable a port to turn to the forwarding state rapidly by setting it to an edge port. And it is recommended to configure the Ethernet ports directly connected to user terminals as edge ports.

Normally, configuration BPDUs cannot reach an edge port because the port is not connected to another switch. But when the BPDU guard function is disabled on an edge port, configuration BPDUs sent deliberately by a malicious user may reach the port. If an edge port receives a BPDU, it turns into a non-edge port.

Examples

XS(Ethernet0/1)# **spanning-tree edge**
Set successfully

spanning-tree mst-configuration

Syntax

spanning-tree mst-configuration

View

System view.

Parameters

None.

Description

Use **spanning-tree mst-configuration** command to enter mst-region configuration environment.

Examples

XS# spanning-tree mst-region
XS(mst-region)#

instance

Syntax

i**nstance** *msti*
no Instance *msti*

View

Mst-region view

Parameters

msti: MST instance ID

Description

Use **instance** command to enable the specified MST instance.
Use **no instance** command to disable the specified MST instance.
By default, the all instances except 0-feature are disabled.

Examples

XS(mst-region)# instance 3
Enable this msti successfully

instance *msti* ethernet *ethernet-port* path-cost

Syntax

instance *msti* **ethernet** *ethernet-port* **path-cost** *cost*
no instance *msti* **ethernet** *ethernet-port* **path-cost** *cost*

View

Mst-region view

Parameters

Msti: MST instance ID

ethernet-port: ethernet port, in the form of interface = { interface-type/interface-number}, interface-type = {0 | 1}, when interface-type is 0, interface-number = { 1 | 2 | … | 24 }, when interface-type is 1, interface-number = { 1 | 2 }
cost: path to be set. This argument ranges from 0 to 200000000, and the default value is atuo (0)

Description

Use **instance** *msti* **ethernet** *ethernet-port* **path-cost** command to set the path cost for an Ethernet port in specific MST instance.
Use **no instance** *msti* **ethernet** *ethernet-port* **path-cost** command to restore to the default value for the Ethernet port in specific MST instance.
By default, the path cost value is auto (0).

Examples

XS(mst-region)# instance 3 ethernet 0/3 path-cost 20000
Set successfully

instance *msti* ethernet *ethernet-port* priority

Syntax

instance *msti* **ethernet** *ethernet-port* **priority** *pri*
no instance *msti* **ethernet** *ethernet-port* **priority** *pri*

View

Mst-region view

Parameters

*Msti:*instance ID
ethernet-port: ethernet port, in the form of interface = { interface-type/interface-number}, interface-type = {0 | 1}, when interface-type is 0, interface-number = { 1 | 2 | … | 24 }, when interface-type is 1, interface-number = { 1 | 2 }
pri: port priority to be set. This argument ranges from 0 to 255, and the default value is 128

Description

Use **instance** *msti* **ethernet** *ethernet-port* **priority** command to set the priority for an Ethernet port in the specified MST instance.
Use **no instance** *msti* **ethernet** *ethernet-port* **priority** command to restore to the default value for the Ethernet port in the specified MST instance.
By default, all instances except 0-feature are disabled.

Examples

XS(mst-region)# instance 3 ethernet 0/3 priority 120
Set successfully

instance *msti* priority

Syntax

instance *msti* **priority** *pri*
no instance *msti* **priority** *pri*

View

Mst-region view

Parameters

*Msti:*instance ID
Pri: the priority for the specified instance. It is in the range of 0 to 65535, the default value is 32768.

Description

Use **instance** *msti* **priority** command to set the priority for an instance.
Use **no instance** command to restore to the default value 32768 for the instance.

Examples

XS(mst-region)# instance 3 priority 4096
Set successfully

instance *msti* vlan

Syntax

instance *msti* **vlan** *vlan-vid* **[to** *vlan-end-vid***]**
no instance *msti* **vlan** *vlan-vid* **[to** *vlan-end-vid***]**

View

Mst-region view

Parameters

Msti: instance ID
vlan-vid: specifies the ID of a VLAN to be added to this instance, in the range of 1 to 4094.
to *vlan-end-vid:* in conjunction with vlan-id1, defines a VLAN range to be added to this instance. The vlan-end-vid argument takes a value in the range of 1 to 4094, and must not be less than that of vlan-vid.

Description

Use **instance** *msti* **vlan** command to set a vlan mapping for the specified MST instance.
Use **no instance** *msti* **vlan** command to remove a VLAN(s) from the specified MST instance.

Examples

XS(mst-region)# instance 3 vlan 4 to 6
Set successfully

region-name

Syntax

region-name *name*

View

Mst-region view

Parameters

name: a variable length text string encoded within a fixed field of 32 octets

Description

Use **region-name** command to set the configuration name of MST Configuration Identification.

Examples

XS(mst-region)# region-name example
configure mstp region name successfully!

revision-level

Syntax

revision-level *level*

View

Mst-region view

Parameters

level: an unsigned short value, in the range from 0 to 65535

Description

Use **revision-level** command to set the revision level of MST Configuration Identification.

Examples

XS(mst-region)# revision-level 25
configure mstp region level successfully!

3.20 SNMP Configuration Commands

The "Any view" in the below table refers to anyone of the following: System view, Ethernet port view, Port-based VLAN view, VLAN view, or dot1x view.

Command list:

View	Command
Any view	**show snmp**

Any view	**show snmp community**
Any view	**show snmp user**
Any view	**show snmp traps-host**
Any view	**show snmp traps-status**
System view	**snmp-server { name | description | contact | location }** *text*
System view	**snmp-server community** **no snmp-server community** *community-name*
System view	**snmp-server user** **no snmp-server user** *username*
System view	**snmp-server traps** **no snmp-server traps**
System view	**snmp-server traps-host** *host-ip* **no snmp-server traps-host** *host-ip*
Ethernet port view	**snmp-traps** **no snmp-traps**

show snmp

Syntax

show snmp

View

Any view.

Parameters

None.

Description

Use **show snmp** command to display the system SNMP information, including system name, system description, contact information, and geographical location. By default, the system name is "XS7424", the system description is "Optical Ethernet Switch", the contact information is support@xenya.si, and the geographical location is "Ljubljana, Slovenia".

Examples

XS(Ethernet0/23)# **show snmp**

SNMP System Name : XS7424
SNMP System Description: Optical Ethernet Switch
SNMP System Contact : support@xenya.si
SNMP System Location : Ljubljana, Slovenia

show snmp community

Syntax

show snmp community

View

Any view.

Parameters

None.

Description

Use **show snmp community** command to display the information of SNMPv1/SNMPv2c communities.

SNMPv1 and SNMPv2c use community name authentication. Therefore, the SNMPv1 and SNMPv2c messages carry community names; if the carried community names are not permitted by the NMS/agent, the messages will be discarded.

You need to create a read community name and a write community name separately, and these two community names on the NMS and on the device should be consistent.

To display the current configuration username information of SNMPv3, use **show snmp user** command.

Examples

XS# **show snmp community**

Version	Community	Popedom
v1	public	RO
v2c	com2	RW

show snmp user

Syntax

show snmp user

View

Any view.

Parameters

None.

Description

Use **show snmp user** command to display the information of SNMPv3 users, including username, auth type, auth password, privacy type, and privacy password.

SNMPv3 introduces the concepts of username and group. You can set the authentication and privacy functions. The former is used to authenticate the validity of sending packets, preventing the access of illegal users; the latter is used to encrypt packets between the NMS and agent, preventing the packets from being intercepted. A more secure communication between SNMP NMS and SNMP agent can be ensured by configuring whether to perform authentication and encryption or not.

You can configure whether to perform authentication and encryption when you create a SNMPv3 group, and configure the specific algorithms and passwords for authentication and encryption when a user is created.

Examples

```
XS# show snmp user
Ver User              AuthType: AuthPwd      PrivType: PrivPwd       Privilege
--- ---------------- -------------------- -------------------   ---------
v3   user1                :                    :                    RW
v3   user2             MD5:useruser2222         :                    RW
v3   user3             MD5:agewhrjykkl       DES:sageriutu6ui        RW
```

show snmp traps-host

Syntax

show snmp traps-host

View

Any view.

Parameters

None.

Description

Use **show snmp traps-host** command to list destination hosts that receive SNMP traps generated by the local device.

Examples

```
XS# show snmp traps-host
SNMP traps-host IP:
192.168.0.234
192.168.0.235
```

show snmp traps-status

Syntax

show snmp traps-status

View

Any view.

Parameters

None.

Description

Use **show snmp traps-status** command to display global trap configurations and per port trap configurations.

Examples

```
XS# show snmp traps-status
            Global trap is enabled.
interface                          status
--------------------------------------------------
ethernet 0/1                       enable
```

ethernet 0/2	enable
ethernet 0/3	enable
ethernet 0/4	enable
ethernet 0/5	**enable**
ethernet 0/6	enable
ethernet 0/7	enable
ethernet 0/8	enable
ethernet 0/9	enable
ethernet 0/10	enable
ethernet 0/11	enable
ethernet 0/12	enable
ethernet 0/13	enable
ethernet 0/14	enable
ethernet 0/15	enable
ethernet 0/16	enable
ethernet 0/17	enable
ethernet 0/18	enable
ethernet 0/19	enable
ethernet 0/20	enable
ethernet 0/21	enable
ethernet 0/22	enable
ethernet 0/23	disable
ethernet 0/24	enable
ethernet 1/1	enable
ethernet 1/2	enable

snmp-server

Syntax

snmp-server { name | description | contact | location } *text*

View

System view.

Parameters

text: a string of 1 to 256 characters
name: SNMP System Name, the default value is "XS7424"
description: SNMP System Description, the default value is "Optical Ethernet Switch"
contact: SNMP System Contact, the default value is support@xenya.si
location: SNMP System Location, the default value is "Ljubljana, Slovenia"

Description

Use **snmp-server** command to set the system information, including system name, system description, contact information, and location.

Examples

XS# **snmp-server name** *dev-xs7424*
Configure system name successfully!

snmp-server community

Syntax

snmp-server community
no snmp-server community *community-name*

View

System view.

Parameters

community-name: name of the community to be created; it is a string of 3 to 16 characters.

Description

Use **snmp-server community** command to create a SNMP community. SNMPv1 and SNMPv2c use a community name to restrict access rights. You can use this command to configure a community name and configure read or write access rights.

Use **no snmp-server community** command to remove an SNMP community. Typically, "public" is used as a read community name, and "private" is used as a write community name. For security reason, it is recommended to use a community name other than these two.

Examples

XS# **snmp-server community**
Version (v1 or v2c): *v2c*
Community (3-16chars): *com3*
Privilege (ro or rw): *ro*

Add snmp agent user successfully!

snmp-server user

Syntax

snmp-server user
no snmp-server user *username*

View

System view.

Parameters

username: username, a string of 3 to 16 characters.
Auth-Algorithm: specifies the security mode for authentication. If this is not specified, neither authentication nor encryption is performed.
MD5: uses HMAC MD5 algorithm for authentication.
SHA: uses HMAC SHA algorithm for authentication, which is more secure than MD5.
auth-password: authentication password, a string of 9 to 15 characters in plain text, a 32-bit hexadecimal number in cipher text if MD5 algorithm is used, and a 40-bit hexadecimal number in cipher text if SHA algorithm is used.
Priv-Algorithm: specifies the security mode as encrypted.
DES: specifies the encryption protocol as Data Encryption Standard (DES).
AES: specifies the encryption protocol as Advanced Encryption Standard (AES),

which is more secure than DES.
priv-password: encryption password, a string of 1 to 64 characters in plain text, a 32-bit hexadecimal number in cipher text if MD5 algorithm is used, and a 40-bit hexadecimal number in cipher text if SHA algorithm is used.

Description

Use **snmp-server user** command to add a user.
Use **no snmp-server user** command to remove a user.

This command is applicable to SNMPv3. If the agent and the NMS communicate using SNMPv3 messages, a SNMPv3 user needs to be created first. Whether to perform authentication or encryption can be configured at the creation of a user, the algorithm and password for authentication or encryption can be set as well.

Examples

XS# **snmp-server user**
UserName (3-16chars): *user3*
Popedom (ro or rw): *ro*
Auth-Alogrithm (MD5 or SHA or NULL): *SHA*
auth-password (9-15chars): *galhgowegqgq*
Priv-Alogrithm (DES or AES or NULL): *NULL*

Add snmp agent user successfully!

snmp-server traps

Syntax

snmp-server traps
no snmp-server traps

View

System view.

Parameters

None.

Description

Use **snmp-server traps** command to enable a device to send SNMP traps.
Use **no snmp-server traps** command to disable a device from sending SNMP traps.
By default, a device sends SNMP traps.

snmp-server traps command needs to be used together with **snmp-server traps-host** command. The **snmp-server traps-host** command specifies the destination hosts of SNMP traps. At least one destination host is required for SNMP traps.

Examples

XS# **snmp-server traps**
Enable global traps successfully!

snmp-server traps-host

Syntax

snmp-server traps-host *host-ip*
no snmp-server traps-host *host-ip*

View

System view.

Parameters

host-ip: specifies the destination for the SNMP traps.

Description

Use **snmp-server traps-host** command to set a destination host to receive the SNMP traps generated.
Use **no snmp-server traps-host** command to cancel the current setting.
Multiple destination hosts can be set to receive traps.

Examples

XS# **snmp-server traps-host** *192.168.0.111*
Add traps-host successfully!

snmp-traps

Syntax

snmp-traps
no snmp-traps

View

Ethernet port view

Parameters

None.

Description

Use **snmp-traps** command to enable the sending of port/interface linkUp/linkDown traps.
Use **no snmp-traps** command to disable the sending of linkUp/linkDown traps.
By default, sending port/interface linkUp/linkDown traps is enabled.

Note that you need to enable the generation of port/interface linkUp/linkDown traps on both port/interface and global to make it effective. To enable this function on a port/interface, use **snmp-traps** command; to enable this function globally, use **snmp-server traps** command.
By default, both are enabled.

Examples

XS(Ethernet0/23)# **snmp-traps**
Enable this interface snmp trap (sending linkUp or linkDown) successfully!

3.21 System Log Commands

The "Any view" in the below table refers to anyone of the following: System view, Ethernet port view, Port-based VLAN view, VLAN view, or dot1x view.

command lists:

View	command
Any view	**show log**
System view	**no log**

show log

Syntax

show log

View

Any view.

Parameters

None

Description

Show all the system logs , including when the system was started, who had logged in the system and how, and so on.

Examples

XS# show log
2009/10/10 10:47:28 192.168.0.209 logins WEB-SERVER!
2009/10/10 10:46:43 Someone logins CLI with serial port, level 3!
2009/10/10 10:46:24 Starting system!

no log

Syntax

no log

View

System view

Parameters

None

Description

Clear all the logs that were saved in the system.

Examples

XS# no log
Clear all the logs successfully!

3.22 LLDP Configuration Commands

The "Any view" in the below table refers to anyone of the following: System view, Ethernet port view, Port-based VLAN view, VLAN view, or dot1x view.

Command list:

View	command
System view Ethernet port view	**lldp** **no lldp**
System view	**lldp admin-status { disable| rx| tx| rxtx }**
Ethernet port view	**lldp encapsulation { snap| Ethernet-ii }**
System view	**lldp timer tx-interval** *interval*
System view	**lldp hold-multiplier** *value*
System view	**lldp timer tx-delay** *delay*
System view	**lldp fast-count** *count*
System view	**lldp timer reinit-delay** *timer*
System view	**lldp tlv-enable basic-tlv { all | system-capability | system-description | system-name | port-description | management-address}** **no lldp tlv-enable basic-tlv { all | system-capability | system-description | system-name | port-description | management-address}**
Any view	**show lldp neighbor-information**
Any view	**show lldp statistics**
Any view	**show lldp status**
Any view	**show lldp tlv-config**

lldp

Syntax

lldp
no lldp

View

System view or Ethernet port view

Parameters

None

Description

It is used to enable or disable the global LLDP or port LLDP. If you want to enable port LLDP, you need to enable the global LLDP first. By default, LLDP is disabled globally; but when the global LLDP is enabled, the port LLDP is enabled by default.

Examples

XS# lldp
Set successfully!
XS# interface ethernet 0/1
XS(Ethernet0/1)# lldp
Set successfully!

lldp admin-status

Syntax

lldp admin-status { disable| rx| tx| rxtx }

View

Ethernet port view

Parameters

disable: A port in this mode does not send or receive LLDPDUs.
rx: A port in this mode only receives LLDPDUs.
tx: A port in this mode only sends LLDPDUs.
rxtx: A port in this mode sends and receives LLDPDUs.

Description

Set the LLDP operating mode.

Examples

XS(Ethernet0/1)# lldp admin-status rxtx
Set successfully!

lldp encapsulation

Syntax

lldp encapsulation { snap | Ethernet-ii}

View

Ethernet port view

Parameters

snap, **ethernet-ii**: The encapsulation format. It is the Ethernet II encapsulation format by default.

Description

Configure the encapsulation format for LLDPDUs.

Examples

XS(Ethernet0/1)# lldp encapsulation ethernet-ii
Set successfully!

lldp timer tx-interval

Syntax

lldp timer tx-interval *interval*

View

System view

Parameters

interval: Required, between 5 to 32768 seconds, 30 seconds by default.

Description

Set the interval to send LLDPDUs.

Examples

XS# lldp timer tx-interval 50
Set successfully!

lldp timer tx-delay

Syntax

lldp timer tx-delay *delay*

View

System view

Parameters

delay: Required, between 1 to 8192 seconds, 2 seconds by default.

Description

Set the delay period to send LLDPDUs.

Examples

XS# lldp timer tx-delay 6
Set successfully!

lldp timer reinit-delay

Syntax

lldp timer reinit-delay *timer*

View

System view

Parameters

timer: Required, between 1 to 10 seconds, 2 seconds by default.

Description

Set the initialization delay period.

Examples

XS# lldp timer reinit-delay 3
Set successfully!

lldp hold-multiplier

Syntax

lldp hold-multiplier *value*

View

System view

Parameters

Value: Required, range between 1 to 10, 5 by default.

Description

Set the TTL multiplier.

Examples

XS# lldp hold-multiplier 5
Set successfully!

lldp fast-count

Syntax

lldp fast-count *count*

View

System view

Parameters

count: Required, between 1 to 10, 3 by default.

Description

Set the number of LLDPDUs to be sent successively when a new neighboring device is detected.

Examples

XS# lldp fast-count 3
Set successfully!

lldp tlv-enable basic-tlv

Syntax

lldp tlv-enable basic-tlv { all | system-capability | system-description | system-name | port-description | management-address}

no lldp tlv-enable basic-tlv { all | system-capability | system-description | system-name | port-description | management-address}

View

System view

Parameters

all: All basic LLDP TLVs, including End of LLDPDU TLV, Chassis ID TLV, Port ID TLV, Time To Live TLV, Time To Live TLV, Port Description TLV, System Name TLV, System Description TLV, System Capabilities TLV, and Management Address TLV. And End of LLDPDU TLV, Chassis ID TLV, Port ID TLV, Time To Live TLV and Time To Live TLV are required.
system-capability: System Capabilities TLV.
system-description: System Description TLV.
system-name: System Name TLV.
port-description: Port Description TLV.
management-address: Management Address TLV.

Description

Enable or disable LLDP TLV sending for specific types of LLDP TLVs.

Examples

XS# lldp tlv-enable basic-tlv all
Set successfully!

show lldp neighbor-information

Syntax

show lldp neighbor-information

View

Any view

Parameters

None

Description

Display the information contained in the LLDP TLVs received through a port.

Examples

XS# show lldp neighbor-information

show lldp statistics

Syntax

show lldp statistics

View

Any view

Parameters

None

Description

Display the LLDP statistics.

Examples

```
XS# show lldp statistics
Ethernet0/1
     Transmit Frames                : 0
     Receive Frames                 : 0
     Receive Error Frames           : 0
     Discarded Frames                 : 0
     TLVs Discarded Packets         : 0
     TLVs Unrecognized Packets    : 0
     Org. TLVs Discarded Packets : 0
     Aged Out Packets               : 0
```

show lldp status

Syntax

show lldp status

View

Any view

Parameters

None

Description

Display the LLDP status.

Examples

```
XS# show lldp status
Global status of LLDP: Enable
Transmit interval : 50s
Hold multiplier    : 5
Reinit delay       : 3s
Transmit delay     : 6s
Fast start times   : 3

Port LLDP status:
    Port          PortStatus       AdminStatus     Encapsulation
Ethernet0/1     Disable           Rx&Tx           Ethernet-II
Ethernet0/2     Enable            Disable         Ethernet-II
Ethernet0/3     Enable            Disable         Ethernet-II
```

Ethernet0/4	Enable	Disable	Ethernet-II
Ethernet0/5	Enable	Disable	Ethernet-II
Ethernet0/6	Enable	Disable	Ethernet-II

show lldp tlv-config

Syntax

show lldp tlv-config

View

Any view

Parameters

None

Description

Display the types of the LLDP TLVs that are currently sent.

Examples

```
XS# show lldp tlv-config
Basic (optional) TLV:
    Port description         : YES
    System name              : YES
    System description       : YES
    System capability        : YES
    Management address : YES
```

3.23 ACL Configuration Commands

The "Any view" in the below table refers to anyone of the following: System view, Ethernet port view, Port-based VLAN view, VLAN view, or dot1x view.

Command list:

View	command
System view	**acl number** *acl-number* **no acl number {** *acl-number*| **all}**
ACL view	**rule** *rule-id* **{permit| deny}** *rule-string* **no rule {***rule-id* **| all}**
Ethernet port view	**packet-filter acl-number** *acl-number* **no packet-filter acl-number {***acl-number*| **all}**
Any view	**show acl number [***acl-number***]**

acl number

Syntax

acl number *acl-number*
no acl number {*acl-number* **\| all}**

View

System view

Parameters

acl-number: Required, between 1 to 30
all: All the ACL number.

Description

Use **acl number** *acl-number* command to create an ACL and enter the ACL view.
Use **no acl number {***acl-number* **| all}** command to delete an ACL or all.

Note that the number from 1 to 10 is for basic ACL, the number from 11 to 20 is for advanced ACL, and the number from 21 to 30 is for L2 ACL.

Examples

XS# acl number 3
XS(ACL-basic-3)#

rule

Syntax

rule *rule-id* **{permit| deny}** *rule-string*
no rule {*rule-id***| all}**

View

ACL view

Parameters

rule-id: Required, between 1 to 10.
permit, **deny**: specifies whether the rule is to permit or deny access.
rule-string: ACL rule string. The string format varies with the type of ACL. For example, for basic ACL , the valid rule string is "**source-ip** *ip-address netmask";* for advanced ACL, the valid rule string is "**source-ip** *ip-address netmask* **[source-port** *port-number* **] destination** *ip-address netmask* **[destination-port** *port-number* **]**"; for L2 ACL, the valid rule string is "**source-mac** *mac-address mac-address-mask* **destination** *mac-address mac-address-mask*".
all: the command is applied to all the rule IDs.

Description

Use **rule** *rule-id* **{permit| deny}** *rule-string* command to define an ACL rule.
Use **no rule {***rule-id***| all}** command to delete a specific rule or all rules of this ACL.

Examples

XS# acl number 2
XS(ACL-basic-2)# rule 1 permit source-ip 192.168.0.111 255.255.255.0
Configure successfully!

packet-filter acl-number

Syntax

packet-filter acl-number *acl-number*
no packet-filter acl-number {*acl-number***| all}**

View

Ethernet port view

Parameters

acl-number: Required, between 1 to 30.
all: the comand is applied to all the ACLs.

Description

Use **packet-filter acl-number** *acl-number* command to apply an ACL to a specific port.
Use **no packet-filter acl-number {***acl-number***| all}** command to unbind an ACL from a specific port.

Examples

XS(Ethernet0/1)# packet-filter acl-number 2
Configuration has been completed successfully!
XS(Ethernet0/1)# no packet-filter acl-number 2
Delete acl binding port successfully!

show acl number

Syntax

show acl number [*acl-number***]**

View

Any view

Parameters

acl-number: Optional, between 1 to 30

Description

Use **show acl number** command to display valid ACL number;
Use **show acl number** *acl-number* to display the rules associated to this ACL number.

Examples

XS# show acl number 2
Basic ACL 2:
rule 01 permit source 192.168.0.111 255.255.255.0

3.24 Port Binding Configuration Commands

The "Any view" in the below table refers to anyone of the following: System view, Ethernet port view, Port-based VLAN view, VLAN view, or dot1x view.

Command list:

View	command
System view	**ip-binding**
Ip-binding view	**user-bind mac-addr** *mac* **ip-addr** *ip* **ethernet** *ethernet-port* **no user-bind { all| ethernet** *ethernet-port*| **mac-addr** *mac* **ip-addr** *ip* **ethernet** *ethernet-port***}**
Any view	**show ip-binding**

ip-binding

Syntax

ip-binding

View

System view

Parameters

None

Description

Use **ip-binding** to enter the ip-binding view, then you can use the port binding commands.

Examples

XS# ip-binding
XS(ip-binding)#

user-bind

Syntax

user-bind mac-addr *mac* **ip-addr** *ip* **ethernet** *ethernet-port*
no user-bind { all| ethernet *ethernet-port*| **mac-addr** *mac* **ip-addr** *ip* **ethernet** *ethernet-port***}**

View

Ip-binding view

Parameters

mac: MAC address, in the format xx-xx-xx-xx-xx-xx.
ip: IP address, in the format x.x.x.x, with x no larger than 255.
ethernet-port: The ethernet port to which the MAC address and IP address are bound.
all: to clear all port binding commands of all ports

Description

Use **user-bind mac-addr** *mac* **ip-addr** *ip* **ethernet** *ethernet-port* command to bind the MAC address and IP address to a specific port. By default, no user MAC address or IP address is bound to a port.
Use **no user-bind all** command to clear all the port binding commands of all the

ports.
Use **no user-bind ethernet** *ethernet-port* command to clear all the port binding commands of a specific port.
Use **no user-bind mac-addr** *mac* **ip-addr** *ip* **ethernet** *ethernet-port* command to clear a specific port binding command.

Examples

XS(ip-binding)# no user-bind all
Set successfully!

show ip-binding

Syntax

show ip-binding

View

Any view

Parameters

None

Description

Use **show ip-binding** command to display the ip-binding information.

Examples

XS# show ip-binding
ip-binding information:
No configuration...

3.25 MVR configuration commands

The "Any view" in the below table refers to anyone of the following: System view, Ethernet port view, Port-based VLAN view, VLAN view, or dot1x view.

Command list:

View	command
System view	**mvr** **no mvr**
System view	**mvr group** *mvr-group* **no mvr group** *mvr-group*
System view	**mvr port type** *{receiver|source|none}* **ethernet** *ethernet-port* **[to ethernet** *ethernet-port***]**
System view	**mvr mode** *{dynamic| compatible}*
System View	**mVlanId** *vlan-id*
Any view	**show configuration**
Any view	**show group**
Any view	**show port**

mvr

Syntax

mvr

View

System view

Parameters

None

Description

Use **mvr** to enable global mvr.
Use **no mvr** to disable global mvr.

Examples

XS# mvr
Enable mvr

mvr group

Syntax

mvr group *mvr-group*
no mvr group *mvr-group*

View

System view

Parameters

mvr-group: a multicast IP address

Description

Use **mvr group** to configure an IP multicast address statically.
Use **no mvr group** to delete an IP multicast address.

Examples

XS# mvr group 225.1.1.2
Groups of mvr set to 225.1.1.2

mvr port type

Syntax

mvr port type *{receiver|source|none}* **ethernet** *ethernet-port* **[to ethernet** *ethernet-port***]**

View

System view

Parameters

source: set uplink ports that receive and send multicast data as source ports.
receiver: set a port as a receiver port if it is a subscriber port and should only receive multicast data. It does not receive data unless it becomes a member of the multicast group, either statically or by using IGMP leave and join messages.
none: remove the *source* or *receiver* port from the multicast VLAN.
ethernet-port: ethernet port, in the form of *interface* = { *interface-type*/*interface-number*}, *interface-type* = {0 | 1}, when *interface-type* is 0, *interface-number* = { 1 | 2 | … | 24 }, when *interface-type* is 1, *interface-number* = { 1 | 2 }.

Description

Use **mvr port type** to configure a source or receiver port for multicast VLAN or remove them from the multicast VLAN.

Examples

XS# mvr port type receiver ethernet 0/3 to ethernet 0/5
The configuration is successful.

mvr mode

Syntax

mvr mode *{dynamic| compatible}*

View

System view

Parameters

compatible mode: multicast data received by MVR hosts is forwarded to all MVR data ports, regardless of MVR host membership on those ports. The multicast data is forwarded only to those receiver ports that MVR hosts have joined, either by IGMP reports or by MVR static configuration. IGMP reports received from MVR hosts are never forwarded from MVR data ports that were configured in the switch.

dynamic mode: multicast data received by MVR hosts on the switch is forwarded from only those MVR data and client ports that the MVR hosts have joined, either by IGMP reports or by MVR static configuration. Any IGMP reports received from MVR hosts are also forwarded from all the MVR data ports in the switch. This eliminates the use of unnecessary bandwidth on MVR data port links, which occurs when the switch runs in compatible mode.

Description

Use **mvr mode** to specify a mode for the mvr.
The default mode is dynamic.

Examples

XS# mvr mode dynamic
mode of mvr set to dynamic

mvr mVlan

Syntax

mVlanId *vlan-id*

View

System view

Parameters

vlan-id: a VLAN ID in the range of 2 to 4094.

Description

Use **mvr mVlanId** to set the multicast VLAN ID to transmit data and igmp-snooping packets.

Examples

XS# mvr mVlanId 200
multicast vlan id of mvr set to 200

show mvr configuration

Syntax

show mvr configuration

View

Any view

Parameters

None

Description

Display the basic configuration of mvr.

Examples

XS# show mvr configuration
show mvr configuration

MVR Global state : Enabled
Multicast Vlan Id : 200
Mode : dynamic

show mvr group

Syntax

show mvr group

View

Any view

Parameters

None

Description

Display all multicast IP address groups.

Examples

```
XS# show mvr group
Vlan ID                 : 200
Multicast group         : 225.1.1.2
Vlan ID                 : 200
Multicast group         : 226.1.1.2
```

show mvr port

Syntax

show mvr port

View

Any view

Parameters

None

Description

Display the "source", "receive", and "none mvr" ports.

Examples

```
XS# show mvr port
source ports:
Ethernet0/5 Ethernet0/7
receiver ports:
Ethernet0/9 Ethernet0/10
None mvr ports:
Ethernet0/1 Ethernet0/2 Ethernet0/3
Ethernet0/4 Ethernet0/6 Ethernet0/8
Ethernet0/11 Ethernet0/12 Ethernet0/13
Ethernet0/14 Ethernet0/15 Ethernet0/16
Ethernet0/17 Ethernet0/18 Ethernet0/19
Ethernet0/20 Ethernet0/21 Ethernet0/22
Ethernet0/23 Ethernet0/24 Ethernet1/25
Ethernet1/26 Ethernet1/27 Ethernet1/28
```

3.26 Loopback-detection

Command list

View	command
System view and Ethernet port view	**loopback-detection** **no loopback-detection**

System view	**loopback-detection interval-time** **no loopback-detection interval-time**
Ethernet port view	**loopback-detection control** **no loopback-detection control**
Any view	**show loopback-detection**

loopback-detection

Syntax

loopback-detection
no loopback-detection

View

System view and Ethernet port view

Parameters

None

Description

Use the **loopback-detection** command to enable loopback detection globally or on a specified port.
Use the **no loopback-detection** command to disable loopback detection globally or on a specified port.

Examples

XS# loopback-detection
Enable loopback detection successfully

loopback-detection interval-time

Syntax

loopback-detection interval-time *second*
no loopback-detection interval-time

View

System view

Parameters

second: time interval for loopback detection, in the range of 5 to 300 (seconds). It defaults to 30 seconds.

Description

Use the **loopback-detection interval-time** command to set time interval for loopback detection.
Use the **no loopback-detection interval-time** command to restore to the default time interval.

Examples

XS# loopback-detection interval-time 50

Set successfully

loopback-detection control

Syntax

loopback-detection control
no loopback-detection control

View

Ethernet port view

Parameters

None

Description

Use the **loopback-detection control** command to enable loopback-detection control on a specific port.
Use the **no loopback-detection control** command to disable loopback-detection control on a specific port.

Examples

XS(Ethernet0/2)# loopback-detection control
Enable loopback detection control on this port successfully.

show loopback-detection

Syntax

show loopback-detection

View

Any view

Parameters

None

Description

Display loopback detection status on the global and on each port.

Examples:

XS# show loopback-detection

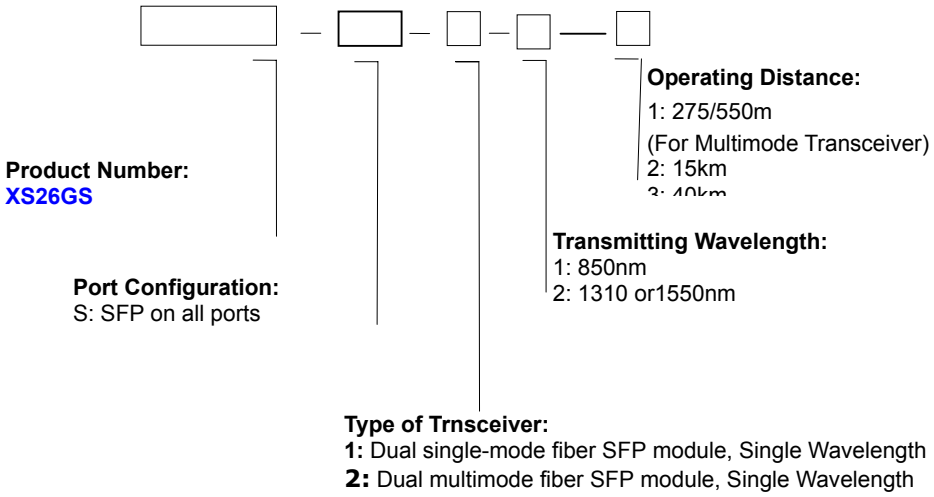
Loopback detection is currently enabled on this switch!
Interval Time(s): 30

Ports	LBD	LBD Control
Ethernet0/1	Disabled	Disabled
Ethernet0/2	Disabled	Enabled
Ethernet0/3	Disabled	Disabled

Ethernet0/4	Disabled	Disabled
Ethernet0/5	Disabled	Disabled
Ethernet0/6	Disabled	Disabled
Ethernet0/7	Disabled	Disabled
Ethernet0/8	Disabled	Disabled
Ethernet0/9	Disabled	Disabled
Ethernet0/10	Disabled	Disabled
Ethernet0/11	Disabled	Disabled
Ethernet0/12	Disabled	Disabled
Ethernet0/13	Disabled	Disabled
Ethernet0/14	Disabled	Disabled
Ethernet0/15	Disabled	Disabled
Ethernet0/16	Disabled	Disabled
Ethernet0/17	Disabled	Disabled
Ethernet0/18	Disabled	Disabled
Ethernet0/19	Disabled	Disabled
Ethernet0/20	Disabled	Disabled

4.Ordering Information

Work In Praraes



5. Appendix A: Command Index

The command index includes all the commands in the User Manual, which are arranged alphabetically.

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

A

acl number *acl-number*

B

C

clear

D

disable
duplex { auto | full | half }
description *name* VLAN view
description *name* Port-based VLAN view
dot1x System view
dot1x Ethernet port view
dot1x re-authentication
dot1x port-control { auto | forceauthorized | forceunauthorized }

E

exit
enable
end Ethernet port view
end VLAN view
end Port-based VLAN view
end dot1x view

F

flow-control

G

garp timeout {hold | join | leave | leaveall } *timer-value*
gvrp
gvrp registration { fixed | forbidden | normal }

H

help

I

ipconfig { **auto** | **ip** *ip-address* [**netmask** *netmask*] [**gateway** *gateway*] }
interface ethernet *interface*
interface ethernet *interface* **[to ethernet** *interface* **]**
igmp-snooping VLAN view
igmp-snooping System view, VLAN view
igmp-snooping querier
igmp-snooping query-interval [time *seconds***]**
igmp-snooping host-aging-time *seconds*
igmp-snooping router-aging-time *seconds*
igmp-snooping leave-time *seconds*
igmp-snooping max-response-time *seconds*
ip-binding
instance *msti*
instance *msti* **ethernet** *ethernet-port* **path-cost** *cost*
instance *msti* **ethernet** *ethernet-port* **priority** *pri*
instance *msti* **priority** *pri*
instance *msti* **vlan** *vlan-vid* **to** *vlan-end-vid*

J

jumboframe

K

L

line-rate { egress | ingress } rate *rate-value*
lacp
lacp system-priority *system-priority*
link-aggregation group *agg-id* **description** *agg-name*
link-aggregation group *agg-id* **mode { manual | static }**
lacp port-priority *port-priority*
link-aggregation group *agg-id*
learning
local-time date *date* **month** *month* **year** *year*
local-time hour *hour* **minute** *minute* **second** *second*
lldp
lldp admin-status { disable| rx| tx| rxtx }
lldp encapsulation { snap| Ethernet-ii }
lldp timer tx-interval *interval*
lldp hold-multiplier *value*
lldp timer tx-delay *delay*
lldp fast-count *count*
lldp timer reinit-delay *timer*
lldp tlv-enable basic-tlv { all | system-capability | system-description | system-name | port-description | management-address}
loopback-detection
loopback-detection interval-time *second*
loopback-detection control

M

management mode { disable | port-based ethernet *interface* | **vlan** *vlan-id* }
monitor-port ethernet *interface*
mirroring-port ethernet *interface* [**to ethernet** *interface*] { **both** | **egress** | **ingress** }
mac-address { static | dynamic | blackhole } *mac-address* **interface ethernet** *interface-number* **vlan** *vlan-id*
mac-address { static | dynamic | blackhole } *mac-address* **vlan** *vlan-id*
mac-address timer aging *age*
mac-address timer no-aging
mac-address multicast *mac-address* **interface ethernet** *interface* **[to ethernet** *interface* **] vlan** *vlan-id*
mac-address multicast mac-address vlan vlan-id
multicast static-router-port ethernet *interface-number*
max-req
mvr
mvr group mvr-group
mvr mode {dynamic | compatible}
mvr port type {receiver | source } ethernet *ethernet-port* **to ethernet** *ethernet-port*
mac-based-vlan mac *mac-address* **priority** *priority*

N

no log
no lldp
no lldp tlv-enable basic-tlv { all | system-capability | system-description | system-name | port-description | management-address}
no acl number { *acl-number***| all}**
no rule {*rule-id* **| all}**
no packet-filter acl-number {*acl-number***| all}**
no user-bind { all| ethernet *ethernet-port***| mac-addr** *mac* **ip-addr** *ip* **ethernet** *ethernet-port***}**
no ipconfig
no user *user-name*
no shutdown
no speed
no duplex
no flow-control
no learning
no line-rate { egress | ingress }
no storm-control
no lacp
no lacp system-priority
no link-aggregation group *agg-id* **description**
no link-aggregation group *agg-id*
no lacp port-priority
no link-aggregation group
no mirror-group
no mirroring-port [**ethernet** *interface*]
no vlan { all | *vlan-id1* **[to** *vlan-id2* **] }**
no vlan-vpn
no vlan-vpn tpid
no vlan-vpn QinQ ethernet *ethernet-port* **old-vid** *old-vid* **to** *old-end-vid*
no switchport { forbidden | tagged | untagged } ethernet *interface* [**to ethernet** *interface*]
no protocol-vlan { at | ip | ipx | mode ethernetii *etype-id* **}**
no mac-based-vlan mac *mac-address*
no unknown-multicast-flood

no igmp-snooping VLAN view
no switchport pvid
no switchport link-type
no switchport admit-frame
no switchport protected
no switchport ingress-filtering
no port-based-vlan { all | *vlan-id1* **[to** *vlan-id2* **] }**
no interface ethernet *interface* **[to ethernet** *interface* **]**
no garp timeout {hold | join | leave | leaveall } *timer-value*
no gvrp
no gvrp registration
no qos queue-scheduler
no qos cos-local-precedence-map
no qos map dscp *dscp*
no qos-mode dscp
no priority
no mac-address { static | dynamic | blackhole } *mac-address* **vlan** *vlan-id*
no mac-address interface ethernet *interface-number*
no mac-address vlan *vlan-id*
no mac-address vlan *vlan-id mac-address*
no mac-address { static | dynamic | blackhole } *mac-address* **vlan** *vlan-id*
no mac-address timer
no mac-address multicast { **all** | **interface ethernet** *interface* [**to ethernet** *interface*] **vlan** *vlan-id* | *mac-address* **vlan** *vlan-id* }
no mac-address multicast mac-address vlan vlan-id
no igmp-snooping System view, VLAN view
no igmp-snooping querier
no igmp-snooping query-interval
no igmp-snooping host-aging-time
no igmp-snooping router-aging-time
no multicast static-router-port ethernet *interface-number*
no timeout { quiet-period *quiet-period-value* | **reauth-period** *reauth-period-value* | **server** *server-timeout-value* | **supplicant** *supp-timeout-value* | **tx-period** *tx-period-value* }
no system-auth-control
no dot1x
no dot1x re-authentication
no spanning-tree
no spanning-tree forward-time
no spanning-tree hello-time
no spanning-tree max-age
no spanning-tree priority
no spanning-tree bpdu-guard
no spanning-tree max-hops
no spanning-tree hold-count
no spanning-tree root-guard
no spanning-tree path-cost
no spanning-tree priority
no spanning-tree point-to-point
no spanning-tree protocol-migration
no spanning-tree edge
no instance *msti*
no instance *msti* **ethernet** *ethernet-port* **path-cost** *cost*
no instance *msti* **ethernet** *ethernet-port* **priority** *pri*
no instance *msti* **priority** *pri*
no instance *msti* **vlan** *vlan-vid* **to** *vlan-end-vid*

no snmp-server community *community-name*
no snmp-server user *username*
no snmp-server traps

no snmp-server traps-host *host-ip*
no snmp-traps
no igmp-snooping leave-time
no igmp-snooping max-response-time
no loopback-detection interval-time
no loopback-detection control

O

P

ping *ip-address*
protocol-vlan { at | ip | ipx | mode ethernetii *etype-id* **}**
port-based-vlan *vlan-id*
priority *priority-level*
packet-filter acl-number *acl-number*

Q

qos queue-scheduler {strict-priority | wrr *queue0-weight queue1-weight queue2-weight queue3-weight* **}**
qos cos-local-precedence-map *cos0-map-local-prec cos1-map-local-prec cos2-map-local-prec cos3-map-local-prec cos4-map-local-prec cos5-map-local-prec cos6-map-local-prec cos7-map-local-prec*
qos map dscp *dscp* **to cos** *cos*
qos-mode dscp

R

reboot
reset configuration
reset counters [**ethernet** *interface*]
radius-server host *host-ip-address* **auth-port** *auth-port-number* **[acct-port** *acct-port-number* **] key** *key-string*
rule *rule-id* **{permit| deny}** *rule-string*
region-name *name*
revision-level *level*

S

save
show ipconfig
show user
show history
show system-information
show fan-status
show temperature
show power-status
show running-config
show log
show management
show interface [ethernet *interface* **]**
show interface statistics [ethernet *interface* **]**
show interface switchport ethernet *interface*
show storm-control
shutdown

speed { 10 | 100 | 1000 | auto }
storm-control type *type* **rate** *rate*
show lacp system-id
show lacp mode
show local-time
show lldp neighbor-information
show lldp statistics
show lldp status
show lldp tlv-config
show acl number [*acl-number***]**
show ip-binding
show link-aggregation interface ethernet *interface* **[to ethernet** *interface* **]**
show link-aggregation summary
show link-aggregation verbose *agg-id*
show mirror
show vlan-mode
show vlan { all | dynamic | static | *vlan-id1* **[to** *vlan-id2* **] }**
switchport { forbidden | tagged | untagged } ethernet *interface* [**to ethernet** *interface*]
show igmp-snooping vlan{ *vlan-id1* **[to** *vlan-id2* **] }**
switchport pvid *vlan-id*
switchport link-type { access | hybrid | trunk }
switchport admit-frame { all | only-tag }
switchport protected
switchport ingress-filtering
show port-based-vlan { all | *vlan-id1* **[to** *vlan-id2* **] }**
show garp timer
show gvrp status
show qos queue-scheduler
show qos cos-local-precedence-map
show qos map dscp cos
show qos interface [ethernet *interface*]
show mac-address-table
show mac-address aging-time
show mac-address { static | dynamic | blackhole } [interface ethernet *interface-number* **] [vlan** *vlan-id* **]**
show mac-address address *mac-address* **[vlan** *vlan-id* **]**
show mac-address interface ethernet *interface-number* **[vlan** *vlan-id* **]**
show mac-address vlan *vlan-id* **[count]**
show mac-address count
show mac-address multicast [count | static { all | count | *mac-address* **vlan** *vlan-id* **}]**
show igmp-snooping configuration
show igmp-snooping group [vlan *vlan-id* **]**
show dot1x { **status** | **interface** [**ethernet** *interface*] }
system-auth-control
show spanning-tree [ethernet *interface* **]**
show spanning-tree {mst-configuration | instance *msti* **| ethernet** *ethernet-port* **instance** *msti***}**
spanning-tree
spanning-tree forward-time *timer-value*
spanning-tree hello-time *timer-value*
spanning-tree max-age *timer-value*
spanning-tree priority *priority*
spanning-tree mode {stp | rstp|mstp}
spanning-tree hold-count *num*
spanning-tree bpdu-guard
spanning-tree root-guard
spanning-tree path-cost *cost*
spanning-tree priority *priority*

spanning-tree point-to-point
spanning-tree protocol-migration
spanning-tree edge
show snmp
show snmp community
show snmp user
show snmp traps-host
show snmp traps-status
snmp-server { name | description | contact | location } *text*
snmp-server community
snmp-server user
snmp-server traps
snmp-server traps-host *host-ip*
snmp-traps
show mvr configuration
show mvr group
show mvr port
show loopback-detection

T

tftp *server-ip* { **get** *source-file* | **put** *dest-file* }
timeout { quiet-period *quiet-period-value* | **reauth-period** *reauth-period-value* | **server** *server-timeout-value* | **supplicant** *supp-timeout-value* | **tx-period** *tx-period-value* }

U

user
update firmware *file-name* **tftp-server** *server-ip*
unknown-multicast-flood
user-bind mac-addr *mac* **ip-addr** *ip* **ethernet** *ethernet-port*

V

vlan-mode { none | port-based | 8021Q }
vlan vlan-id
vlan-vpn
vlan-vpn QinQ Ethernet *Ethernet-port* priority *priority* new-vid *new-vid* old-vid *old-vid* to *old-end-vid*
vlan-vpn tpid *tpid*

W

X

Y

Z

6. Appendix B: Supported MIBs

This appendix lists the supported Management Information Base (MIBs) for this release of the XS26GS switch.

MIB list

RFC1213-MIB

RFC1493-BRIDGE-MIB

RFC1573-IF-MIB

RFC1643-EtherLike-MIB

RFC1757-RMON-MIB

RFC2618-RADIUS-AUTH-CLIENT-MIB

RFC2620-RADIUS-ACC-CLIENT-MIB

RFC2674-P-BRIDGE-MIB

RFC2674-Q-BRIDGE-MIB

LLDP-MIB

IEEE8021-PAE-MIB

FMC-SWITCH-MIB

FMC-IGMP-SNOOPING-MIB

FMC-SWITCH-MAC-AUTHENTICATION-MIB

FMC-SWITCH-RADIUS-MIB

FMC-MSTP-MIB

FMC-MVR-MIB

RSTP-MIB