TRENDnet®

User's Guide

TL2-E284

1.01

Table of Contents

Chapter 1

Preface

About This Guide

This guide provides instructions on how to install and configure the TL2-E284 24-Port 10/100Mbps Layer 2 Switch w/ 4 Gigabit Ports and 2 Shared Mini-GBIC Slots.

This guide is mainly divided into four parts:
1. Hardware Installation: Step-by-step hardware installation procedure.
2. Using Web User Interface: A startup guide to for the command line interface.
3. Command Reference: Information about the function descriptions and configuration settings.

Terms/Usage

In this guide, the term “Switch” (first letter capitalized) refers to this Switch, and “switch” (first letter lower case) refers to other Ethernet switches. Some technologies refer to terms “switch”, “bridge” and “switching hubs” interchangeably, and both are commonly accepted for Ethernet switches.

Note Alerts you to supplementary information.

Caution Indicates potential property damage or personal injury.

Chapter 2

Product Introduction

Product Introduction

The TL2-E284 is a Layer 2 Managed Switch with 24-10/100Mbps Ethernet ports and 4-10/100/1000Mbps Gigabit Ethernet ports shared with 2-10/100/1000Mbps Mini-GBIC slots.

Front Panel

Port/Button	Action	Function	
Console (RS-232)	N/A	Provide out-of-band connection for Switch Management	
Reset	Push/Hold 15 sec	The switch will be restored to factory defaults	
Device Status LED	**Color**	**Sequence**	**Definition**
PWR (Power)	**Green**	**Solid**	Device powered On
	N/A	**Off**	Device powered Off
SYS (System)	**Green**	**Solid**	Device is ready
	N/A	**Off**	Device is no ready
Ethernet LED (RJ-45)	**Color**	**Sequence**	**Definition**
100M Link/ACT	**Green**	**Solid**	100/200Mbps (Half/Full Duplex) Connected (per port)
		Blinking	100/200Mbps (Half/Full Duplex) Data Transmitting/Receiving (per port)
		Off	No connection to the port

10M Link/ACT	**Amber**	**Solid**	10/20Mbps (Half/Full Duplex) Connected (per port)
		Blinking	10/20Mbps (Half/Full Duplex)Data Transmitting/Receiving (per port)
		Off	No connection to the port
Shared Gigabit Ethernet (RJ-45) / Mini-GBIC Slot LED	**Color**	**Sequence**	**Definition**
1000M Link/ACT	**Green**	**Solid**	2000Mbps (Full Duplex) Connected (per port)
		Blinking	2000Mbps (Full Duplex) Data Transmitting/Receiving (per port)
		Off	No connection to the port
10/100M Link/ACT	**Amber**	**Solid**	10/20Mbps (Half/Full Duplex) or 100/200Mbps (Half/Full Duplex) Duplex Connected (per port)
		Blinking	10/20Mbps (Half/Full Duplex) or 100/200Mbps (Half/Full Duplex) Data Transmitting/Receiving (per port)
		Off	No connection to the port

Note Mini-GBIC ports are shared with normal RJ-45 ports 25 and 26. When Mini-GBIC port is used, the RJ-45 port cannot be used.

Rear Panel

Power Connector The power port is where to connect the AC power cord.

Chapter 3
Hardware Installation

This chapter provides unpacking and installation information for TL2-E284.

Unpacking

Open the shipping carton and carefully unpack its contents. Please consult the packing list located in the User Manual to make sure all items are present and undamaged. If any item is missing or damaged, please contact your local reseller for replacement.

- **TL2-E284**
- **Multi-Language Quick Installation Guide**
- **CD-ROM (User's Guide)**
- **Power Cord (1.8 m / 5.9 ft.)**
- **RS-232 Cable (3 m / 9.8 ft.)**
- **Rack Mounting Kit**
- **Rubber feet**

If any item is found missing or damaged, please contact the local reseller for replacement.

Switch Installation

For safe switch installation and operation, it is recommended that you:

- **Visually inspect the power cord to see that it is secured fully to the AC power connector.**
- **Make sure that there is proper heat dissipation and adequate ventilation around the switch.**
- **Do not place heavy objects on the switch.**

Desktop or Shelf Installation

When installing the switch on a desktop or shelf, the rubber feet included with the device must be attached on the bottom at each corner of the device's base. Allow enough ventilation space between the device and the objects around it.

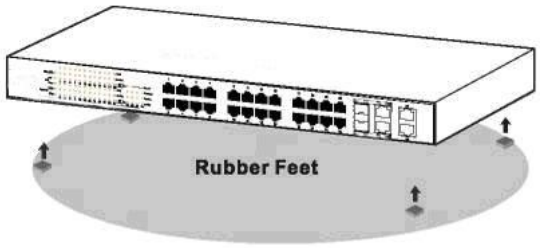


Figure 1 – Attach the adhesive rubber pads to the bottom

Rack Installation

The switch can be mounted in an EIA standard size 19-inch rack, which can be placed in a wiring closet with other equipment. To install, attach the mounting brackets to the switch's side panels (one on each side) and secure them with the screws provided.

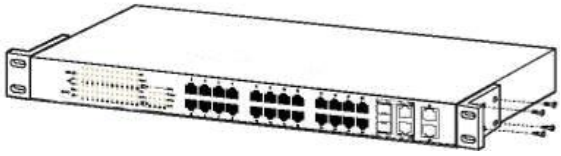


Figure 2 – Attach the mounting brackets to the Switch

Then, use the screws provided with the equipment rack to mount the switch in the

rack.

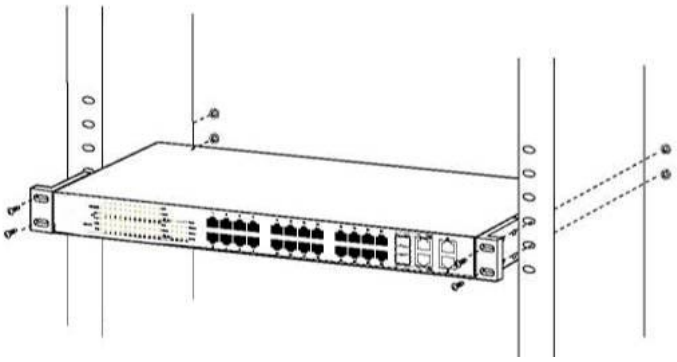


Figure 3 – Mount the Switch in the rack or chassis

⚠Caution

Safety Instructions

A) Elevated Operating Ambient - If installed in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room ambient. Therefore, consideration should be given to installing the equipment in an environment compatible with the maximum ambient temperature (Tma) specified by the manufacturer.

B) Reduced Air Flow - Installation of the equipment in a rack should be such that the amount of air flow required for safe operation of the equipment is not compromised.

C) Mechanical Loading - Mounting of the equipment in the rack should be such that a hazardous condition is not achieved due to uneven mechanical loading.

D) Circuit Overloading - Consideration should be given to the connection of the equipment to the supply circuit and the effect that overloading of the circuits might have on overcurrent protection and supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing this concern.

E) Reliable Earthing - Reliable earthing of rack-mounted equipment should be maintained. Particular attention should be given to supply connections other than direct connections to the branch circuit (e.g. use of power strips)."

Plugging in the AC Power Cord

Users may now connect the AC power cord into the rear of the switch and to an electrical outlet (preferably one that is grounded and surge protected).

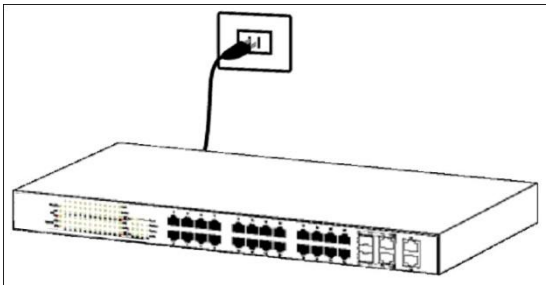


Figure 4 – Plugging the switch into an outlet

Power Failure

As a precaution, the switch should be unplugged in case of power failure. When power is resumed, plug the switch back in.

Chapter 4
Using the Web User Interface

After a successful physical installation, you can configure the Switch, monitor the network status, and display statistics using a web browser.

Supported Web Browsers

The embedded Web-based Management currently supports the following web browsers:

A) Internet Explorer 6 or higher
B) Netscape 8 or higher
C) Mozilla
D) Firefox 1.5/2.0 or higher

Connecting to the Switch

You will need the following equipment to begin the web configuration of your device:

1. A PC with a RJ-45 Ethernet connection
2. A standard Ethernet cable

Connect the Ethernet cable to any of the ports on the front panel of the switch and to the Ethernet port on the PC.

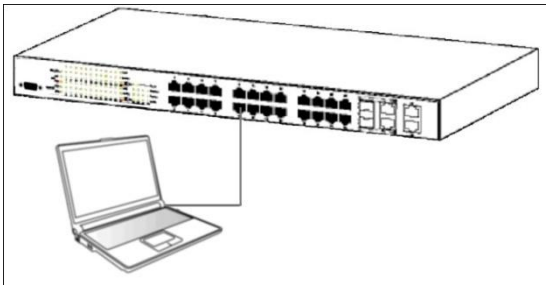


Figure 5 – Connected to an end node via Ethernet cable

Login Web-based Management

In order to login and configure the switch via an Ethernet connection, the PC must have an IP address in the same subnet as the switch. For example, if the switch has an IP address of **192.168.10.200**, the PC should have an IP address of **192.168.10.x** (where x is a number between 1 ~ 254), and a subnet mask of **255.255.255.0**.

Open the web browser and enter **192.168.10.200** (the factory-default IP address) in the address bar. Then press <Enter>.

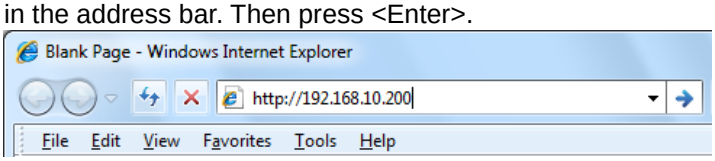


Figure 6 – Enter the IP address 192.168.10.200 in the web browser

When the following page appears, enter the user name and password then click **Login**.

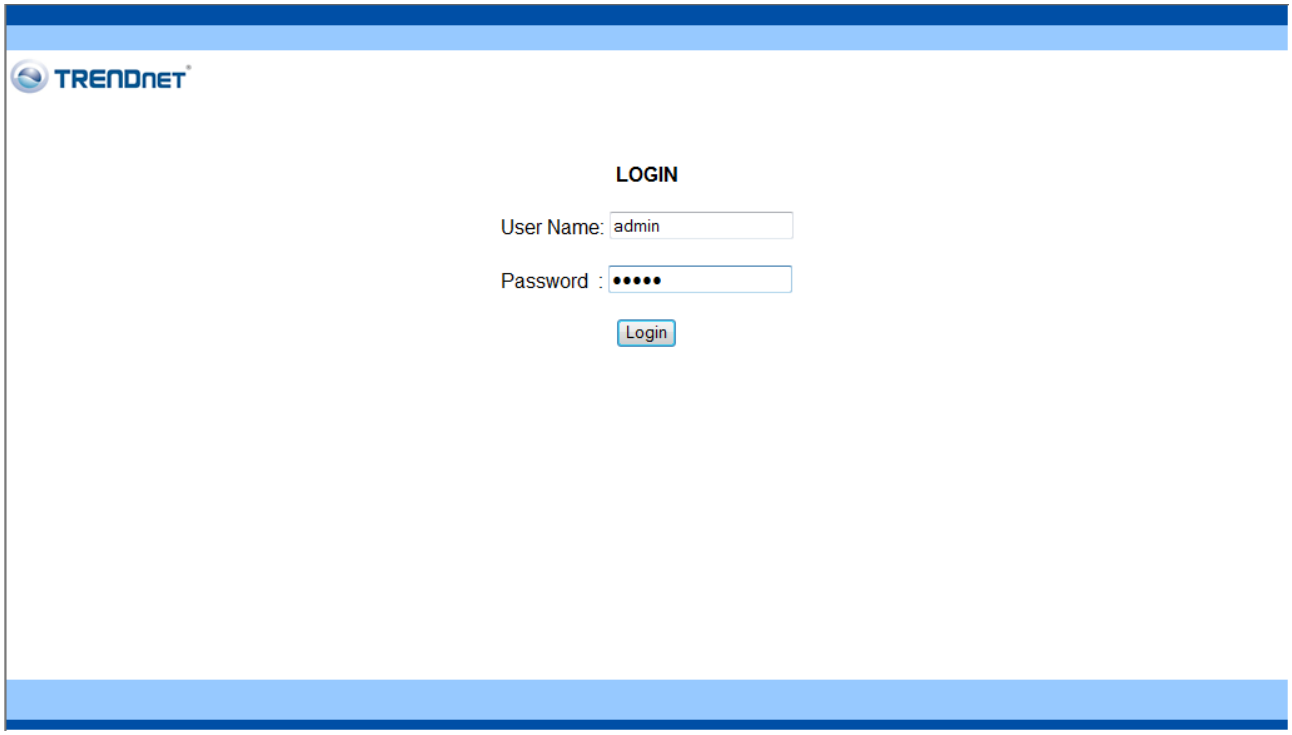


Figure 7 – Enter the IP address 192.168.10.200 in the web browser

Note

The default user name and password are:

User Name	Password	Privilege
admin	admin	15
guest	guest123	1

After login successfully, following page will appear.

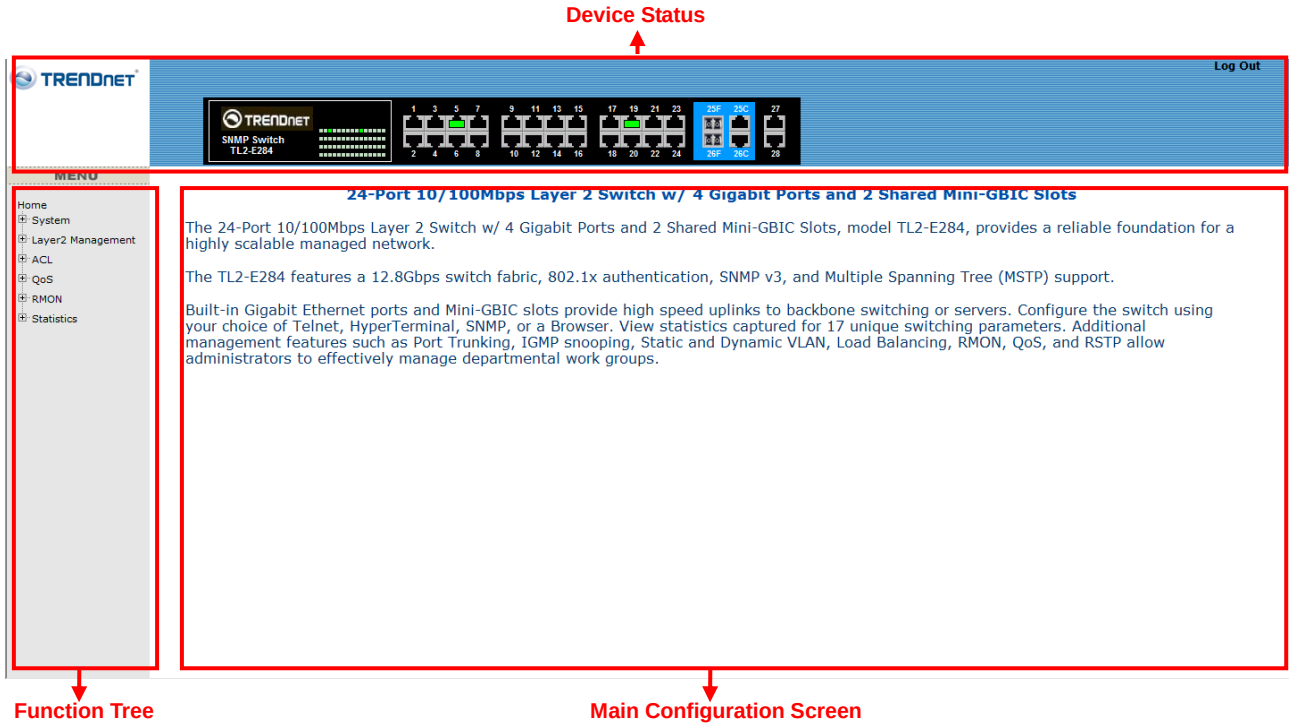


Figure 8 – Web User Interface

The three main areas are the **Device Status** on top, the **Function Tree**, and the

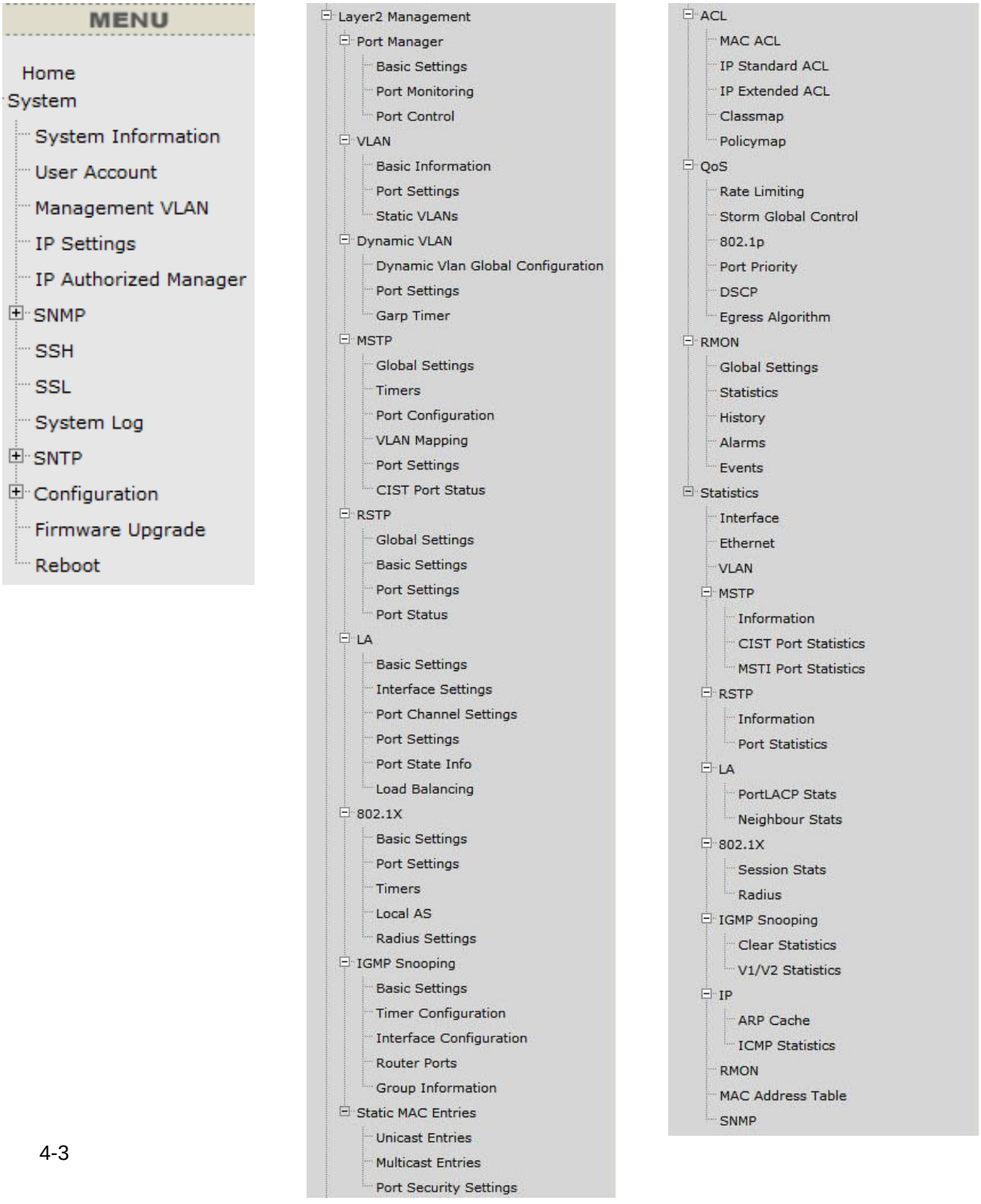
Main Configuration Screen.

The **Device Status** provides a real-time switch port link status.

By choosing different functions in the **Function Tree**, you can change all the settings in the **Main Configuration Screen**. The main configuration screen will show the current status of your Switch by clicking the model name on top of the function tree.

To terminate the web management session, click **Log Out** in the upper right comer.

Function Tree



Chapter 5
Configuring System Basic Functions

System Basic Function List

- **System Information**
- **User Account**
- **Management VLAN**
- **Management IP Settings**
- **IP Authorized Manager**
- **SNMP**
  - SNMP User/Group Table Configuration
  - SNMP Group Access Table Configuration
  - SNMP View Table Configuration
  - SNMP Community Settings
  - SNMP Host Table
  - SNMP Engine ID Configuration
- **SSH Configuration**
- **SSL Configuration**
- **System Log Configuration**
- **SNTP**
  - SNTP and Current Time Settings
  - SNTP Daylight Saving Time
- **Configuration**
  - Save Configuration
  - Restore Configuration
  - Erase Configuration
- **Firmware Upgrade**
- **Reboot**

System Information

This page is to display and edit relevant system information.

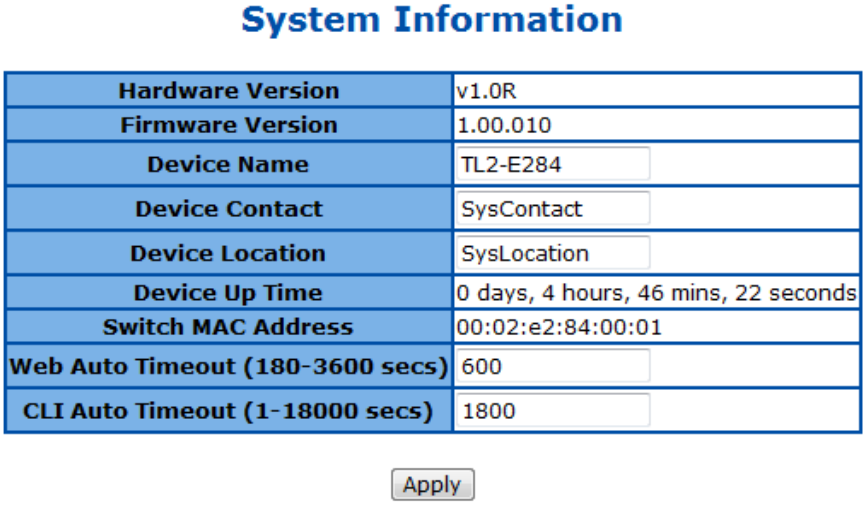


Figure 9 – System > System Information

Parameter	Description
Hardware Version	The hardware version of this device.
Firmware Version	The firmware version of the device.
Device Name	The name of the device. Default is *TL2-E284*.
Device Contact	The identification information of a contact person. Default is *SysContact*.
Device Location	Entering the device location description. Maximum of 50 characters is allowed and a null string is not accepted. Default is *SysLocation*.
Device Up Time	The time duration since the system has been up and running.
Switch MAC Address	The MAC address of the device.
Web Aut0 Timeout (180-3600 secs)	The duration that the device times out when no user activity occurs on the web interface. Default is *600* seconds.
CLI Auto Timeout (1-18000 secs)	The duration that the device times out when no user activity occurs on the web interface. Default is *1800* seconds.

Click **Apply** to submit the changes.

User Account

This page is to create and display user account information.

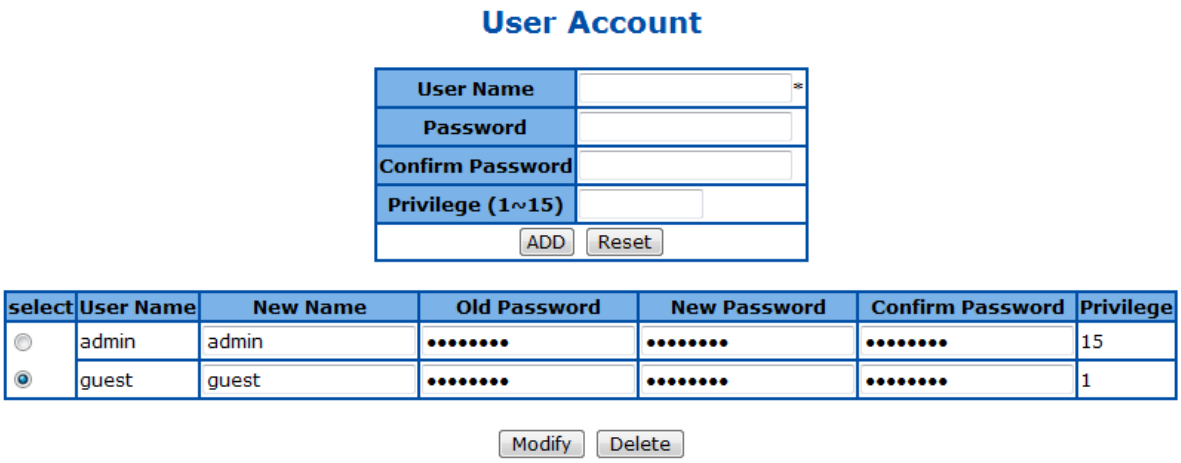


Figure 10 – System > User Account

Parameter	Description
User Name	Username of an account.
Password	Password of an account.
Privilege (1-15)	Privilege level that ranges from 1 to 15. 15 are the highest level.

Click **ADD** to submit the changes and the **Reset** button will clear the information. Select and click **Delete** to remove an existed account. The default accounts are *admin* (privilege 15) and *guest* (privilege 1).

Management VLAN

This page is to edit the management VLAN information.

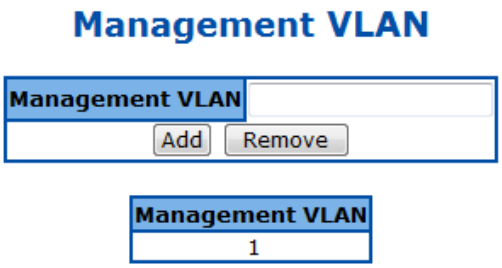


Figure 11 – System > Management VLAN

Parameter	Description
Management VLAN	The VLAN ID of management VLAN. It can be a single VLAN ID from 1 to 4094, a range of VLAN IDs separated by a hyphen (-) ,or a series of non-continuous numbers divided by a comma (,)

Click **ADD** to submit the changes and the **Remove** button will remove an existed VLAN ID.

Note There has to be at least one management VLAN ID exists.

Management IP Settings

This page is to edit the management IP settings.

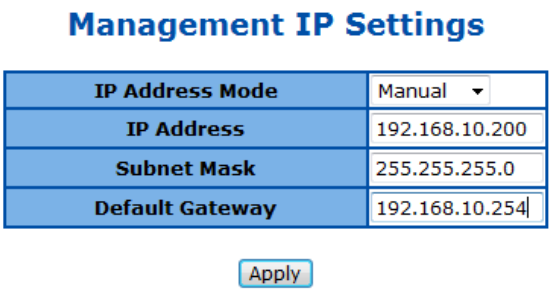


Figure 12 – System > IP Settings

Parameter	Description
IP Address Mode	To configure the mode that the IP address of default interface is assigned. You can choose **Manual** or **Dynamic**. Default is *Manual.*
IP Address	IP address of the management interface. Default is *192.168.10.200*.
Subnet Mask	Subnet mask of the management interface. Default is *255.255.255.0*.
Default Gateway	IP address of default gateway. Default is *192.168.10.254*.

Click **Apply** to submit the changes.

IP Authorized Manager

This page is to set an authorized administrator source IP address, and the services, interfaces, or VLANs that it is allowed to visit.

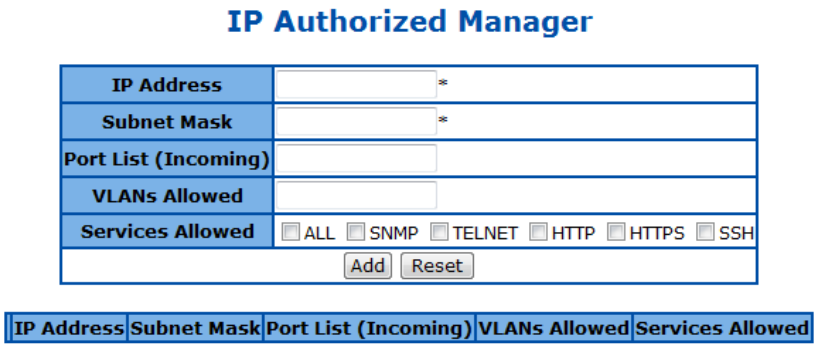


Figure 13 – System > IP Authorized Manager

Parameter	Description
IP Address	IP address of authorized manager
Subnet Mask	Subnet mask of the authorized IP address
Port List (Incoming)	Interface of the authorized administrator is allowed to connect to
VLANs Allowed	VLAN ID of the authorized administrator is allowed to connect to. It can be a single VLAN ID from 1 to 4094, a range of VLAN IDs separated by a hyphen (-) ,or a series of non-continuous numbers divided by a comma (,)
Service Allowed	Services that authorized administrator are allowed to access. It includes **SNMP**, **TELNET**, **HTTP** (Web), **HTTPS** (SSL), **SSH** services. Select **ALL** will cover all services.

Click **ADD** to submit the changes and the **Reset** button will clear the information. Select and click **Delete** to remove an existed account.

SNMP

SNMP User/Group Table Configuration

This page is to configure the SNMP user and group information.

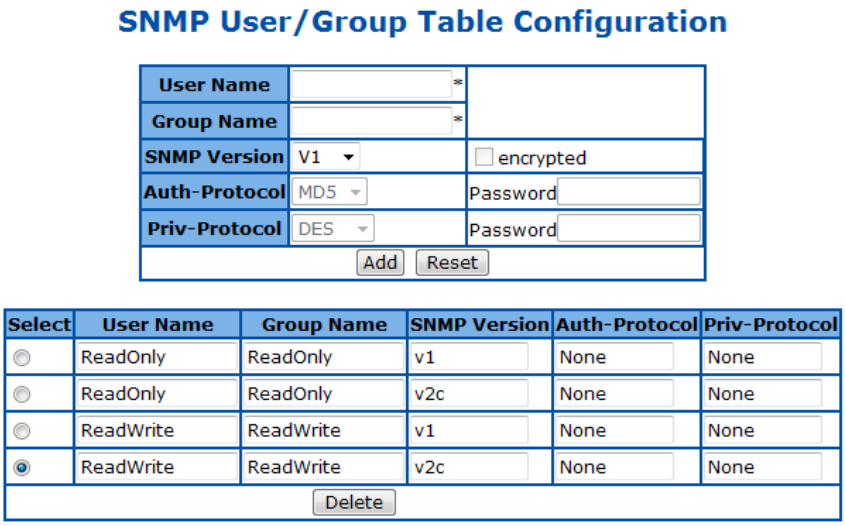


Figure 14 – System > SNMP > User/Group Table

Parameter	Description
User Name	SNMP user name
Group Name	SNMP group name

SNMP Version	Specify the SNMP version to be used, which can be **v1**, **v2c**, or **v3**. Select '**encrypted'** if the encryption for user authentication is needed. Once the encryption is enabled, then you can set the authentication and privilege algorithm and passwords.
Auth-Protocol	Specify the authentication algorithm from **MD5** or **SHA** algorithm, and the password.
Priv-Protocol	Specify the privilege encryption algorithm from **DES** or **none**, and the password.

Click **ADD** to submit the changes and the **Reset** button will clear the information. Select and click **Delete** to remove an existed entry.

SNMP Group Access Table Configuration

This page is to configure the access settings of a SNMP group.

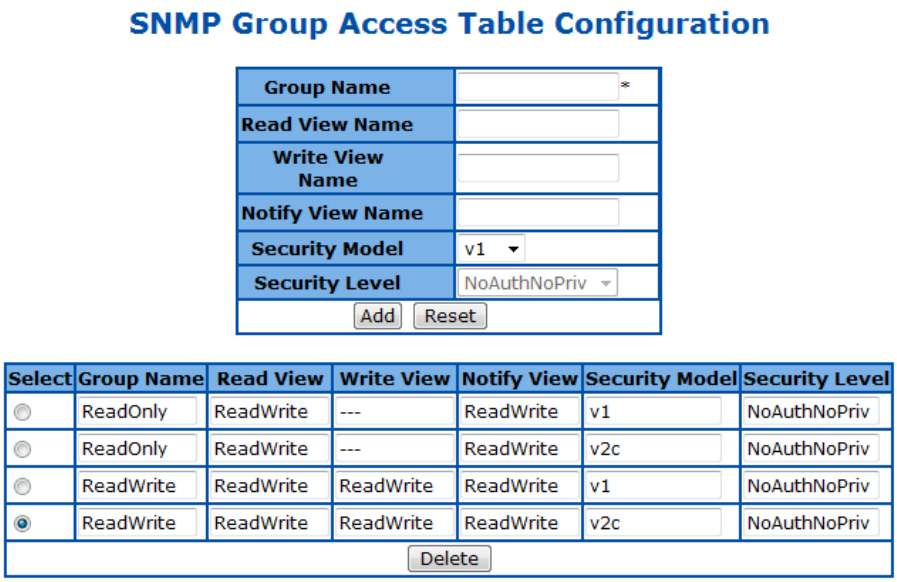


Figure 15 – System > SNMP > Group Access Table

Parameter	Description
Group Name	SNMP group name
Read View Name	The name of group (view) has read privilege and is allowed to access the specified MIB object groups.
Write View Name	The name of group (view) has write privilege and is allowed to access the specified MIB object groups.
Notify View Name	The name of group (view) can receive SNMP Trap messages and is allowed to access the specified MIB object groups.
Security Model	Specify the SNMP version to be used, which can be **v1**, **v2c**, or **v3**.
Security Level	Specify if authentication and encryption are needed for SNMP messages. **NoAuthNoPriv** – Neither authentication or encryption is needed. It is the default setting. **AuthNoPriv** - Authentication is required for the SNMP messages. It is selectable only when SNMPv3 is specified. **AuthPriv** – Both authentication and encryption are required for the SNMP messages. It is selectable only when SNMPv3 is specified.

Click **ADD** to submit the changes and the **Reset** button will clear the information. Select and click **Delete** to remove an existed entry.

SNMP View Table Configuration

This page is to create a SNMP view, which limits the range of MIB objects that a SNMP administrator can access to.

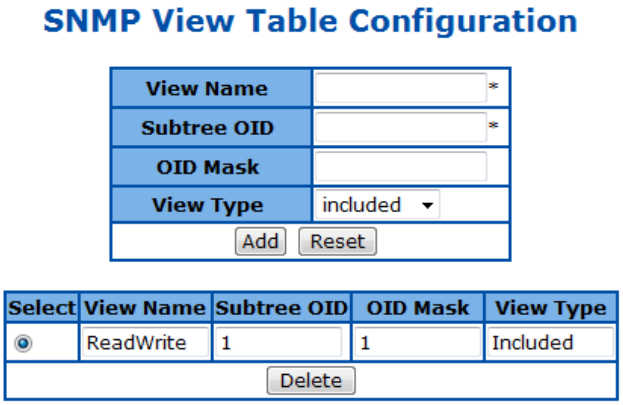


Figure 16 – System > SNMP > View Table

Parameter	Description
View Name	SNMP view name
Subtree OID	The object ID of MIB tree
OID Mask	The mask of OID
View Type	**included** – Includes the object in the list that the SNMP administrator can access. **excluded** – Excludes the object from the list that the SNMP administrator can access.

Click **ADD** to submit the changes and the **Reset** button will clear the information. Select and click **Delete** to remove an existed entry.

SNMP Community Settings

This page is to create and edit SNMP community information.

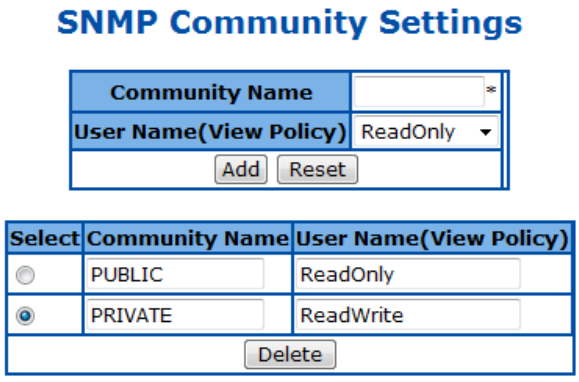


Figure 17 – System > SNMP > Community Table

Parameter	Description
Community Name	SNMP community name
User Name (View Policy)	ReadOnly – The community has read-only privilege. ReadWrite - The community has read write privilege.

Click **ADD** to submit the changes and the **Reset** button will clear the information. Select and click **Delete** to remove an existed entry.

SNMP Host Table

This page is to create a host that can access the device by SNMP protocol.

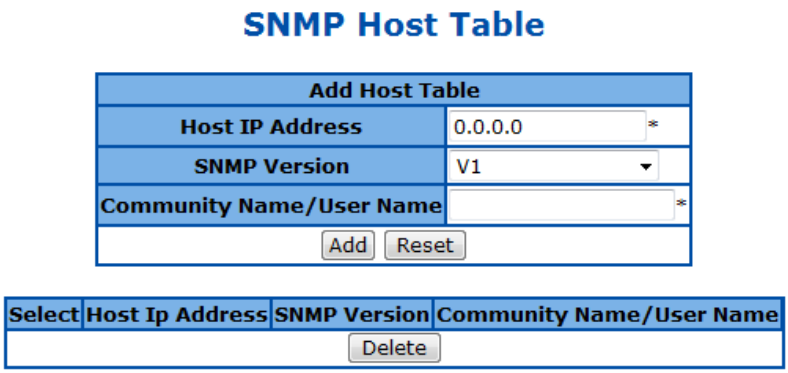


Figure 18 – System > SNMP > Trap Manager

Parameter	Description
Host IP Address	The IP address of a host that can access to the device by SNMP.
SNMP version	Specify the SNMP version to be used, which can be **v1**, **v2c**, or **v3**.
Community Name/User Name	The name of SNMP community/user that the host belongs to.

Click **ADD** to submit the changes and the **Reset** button will clear the information. Select and click **Delete** to remove an existed entry.

SNMP Engine ID Configuration

This page is to configure the SNMP engine identifier of the device.

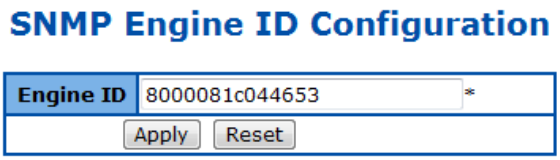


Figure 19 – System > SNMP > Engine ID

Parameter	Description
Engine ID	A string of between 5 and 32 octets expressed in hexadecimal. The default is *8000081c044653*.

Click **ADD** to submit the changes and the **Reset** button will clear the information.

SSH Configuration

This page is to configure the SSH server function on the device.

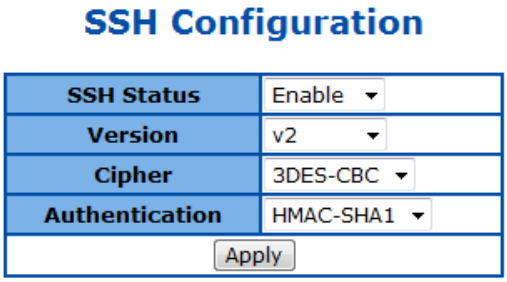


Figure 20 – System > SSH

Parameter	Description
SSH Status	Select **Enable** or **Disable** to turn on or off the SSH server function. Default is enabled.
Version	Specify the SSH version supported. **V2** – SSH v2 is supported. This is the default value. **V1 & V2** – Both SSH v1 and V2 are supported.
Cipher	To specify SSH Cipher algorithm. **3DES-CBC** - 3DES (Triple Data Encryption Standard) encryption algorithm in CBC (Cipher Blocking Chain). This is the default value. **DES-CBC** - DES (Data Encryption Standard) in CBC (Cipher Blocking Chain). **Both** – Both 3DES-CBC and DES-CBC are supported.
Authentication	To specify authentication encryption algorithm. **HMAC-SHA1** – Hash-based Message Authentication Codes (HMAC) and SHA1 (Secure Hash Algorithm). **HMAC-MD5** – Hash-based Message Authentication Codes (HMAC) and MD5 (Message-Digest algorithm 5). **Both** – Both HMAC-SHA1 and HMAC-MD5 are supported.

Click **Apply** to submit the changes.

SSL Configuration

This page is to configure the SSL server function on the device.

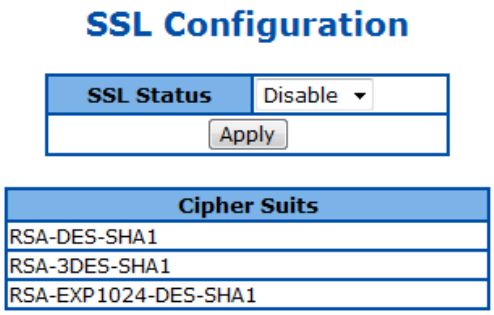


Figure 21 – System > SSL

Parameter	Description
SSL Status	Select **Enable** or **Disable** to turn on or off the SSH server function. Default is disabled. The cipher suite includes RSA-DES-SHA1, RSA-3DES-SHA1, and RSA-EXP1024-DES-SHA1 cipher algorithm.

Click **Apply** to submit the changes.

System Log Configuration

This page is to configure system log settings.

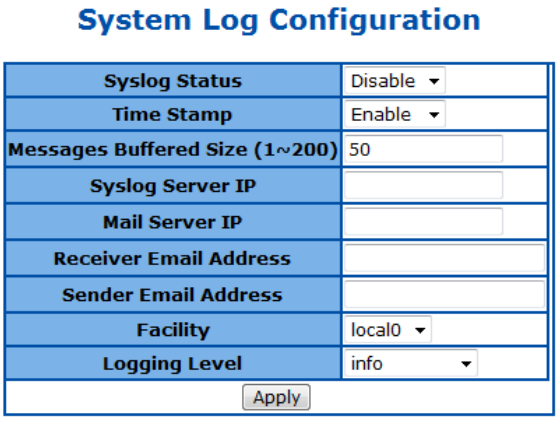


Figure 22 – System > System Log

Parameter	Description
Syslog Status	The status of syslog server function. Default is *enabled*.
Time Stamp	Specifies if time stamp is attached with syslog messages. Default is *enabled*.
Messages Buffered Size (1-200)	The size of internal logging buffer. Default is *50*.
Syslog Server IP	IP address of the external syslog server
Mail Server IP	Specify the IP address of mail server to be used for sending the email alerts messages.
Receiver Email Address	The email address of receiver that receives the alert messages.
Sender Email Address	The email address of sender that sends out the alert messages.
Facility	Specifies the facility that is indicated in the message. Possible values: **local0**, **local1**, **local2**, **local3**, **local4**, **local5**, **local6**, and **local7**. Default is *Local0*.
Logging Level	Specifies the severity level of messages. Possible values are: **Alert** level: action must be taken immediately. **Critical** level: Critical conditions. **Debug** level: Debug messages. **Emergency** level: System is unusable. **Error** level: Error conditions. **Informational** level: Informational messages. **Notification** level: Normal but significant condition. **Warning** level: Warning conditions. Default is *info*.

Click **Apply** to submit the changes.

SNTP

SNTP and Current Time Settings

This page is to configure SNTP and time settings.

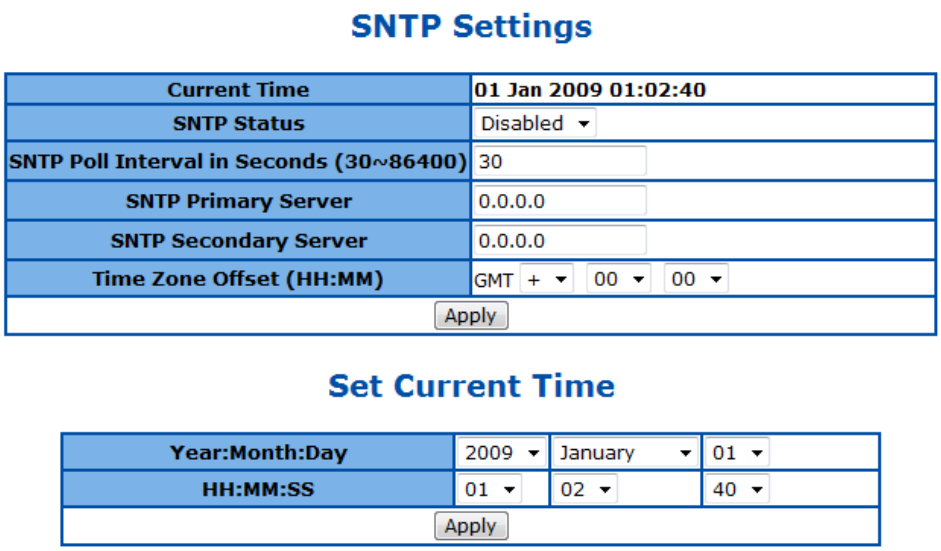


Figure 23 – System > SNTP > Time Settings

Parameter	Description
Current Time	Current system time.
SNTP Status	To enable/disable the Simple Network Time Protocol (SNTP) function. Default is *disabled*.
SNTP Poll Interval in Seconds (30-86400)	To set the time interval that SNTP synchronizes the time on SNTP server, and the range is from 30 to 86400 seconds. Default is *30*.
SNTP Primary Server	To set the primary SNTP server IP address.
SNTP Secondary Server	To set the secondary SNTP server IP address.
Time Zone Offset (HH:MM)	To specify the difference of current time zone relative to GMT.
Year:Month:Day	Specify current date
HH:MM:SS	Specify current system time.

Click **Apply** to submit the changes.

SNTP Daylight Saving Time

This page is to configure the daylight saving time function of system time setting.

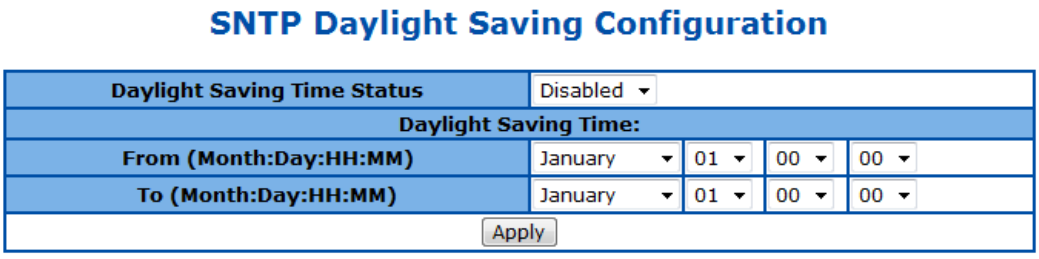


Figure 24 – System > SNTP > Daylight Saving Time

Parameter	Description
Daylight Saving Time Status	To enable/disable the DST function. Default is *disabled*.
Daylight Saving Time: From (Month:Day:HH:MM)	Specify the DST period in month:day:hour:minute.

To (Month:Day:HH:MM)	

Click **Apply** to submit the changes.

Configuration

Save Configuration

This page is used to save the running configuration.

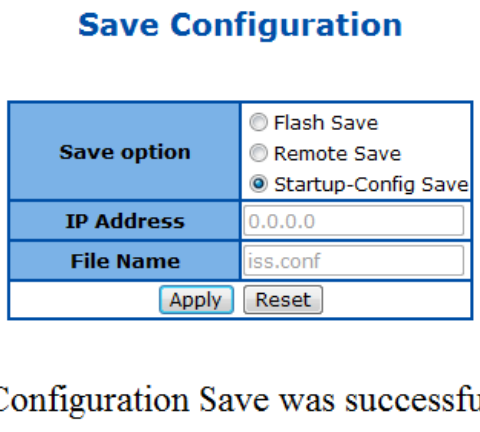


Figure 25 – System > Configuration > Save

Parameter	Description
Save option	Options to save the running configuration: **Flash Save**: Save to the device's flash memory with a designated file name. Saving the configuration to flash will back up the current configuration in the device's internal memory to be restored later if necessary but will not set the configuration as active after a device reboot or power cycle. **Remote Save**: Save to the remote TFTP server with a designated IP address and file name. This will back up the configuration to an external location. **Startup-Config Save**: Save to the device's startup configuration. Note: This will set the current configuration as the active configuration after a device reboot or power cycle.
IP Address	IP address of the remote TFTP server.
File Name	Specify the filename of the configuration to be saved.

Click **Apply** to submit the changes and the **Reset** button will clear the information.

Restore Configuration

This page is used to restore startup configuration from another configuration file in flash memory.

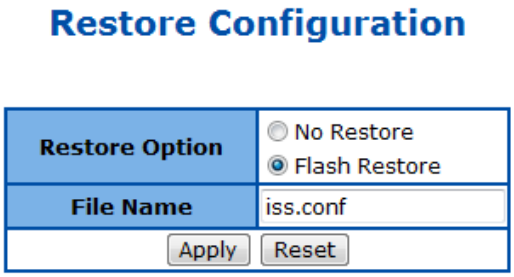


Figure 26 – System > Configuration > Restore

Parameter	Description
Restore Option	Options to restore the startup configuration: **No Restore**: Applying this option will reset the NV-RAM to default settings. Note: This will only reset the settings in NV-RAM, not the entire device configuration. After rebooting, only the default parameters in NV-RAM will be reset to defaults. Requires a manual device reboot for changes to take effect. Please reference the default NV-RAM parameters below. • Default IP Address : 192.168.10.200 • Default Subnet Mask: 255.255.255.0 • Default IP Address Config Mode: Manual • Default IP Address Allocation Protocol : DHCP • Default Interface Name: Fa0/1 • Default RM Interface Name: NONE • Config Restore Option: No restore • Config Save Option: Startup save • Config Save IP Address: 0.0.0.0 • Config Save Filename: iss.conf • Config Restore Filename: iss.conf • PIM Mode: Sparse Mode • IGS Forwarding Mode: MAC based • CLI Serial Console: Yes • SNMP EngineID: 80.00.08.1c.04.46.53 • SNMP Engine Boots: 1 • Default VLAN Identifier: 1 **Flash Restore**: Restore from a previously backed up configuration file in the device's flash memory to the startup-config. Note: After restoring configuration, requires a manual device reboot for changes to take effect.
File Name	Specify the file name of the configuration to be restored.

Click **Apply** to submit the changes and the **Reset** button will clear the information.

Erase Configuration

This page is used to reset the startup configuration, NV-RAM or the configuration file in flash to default value.

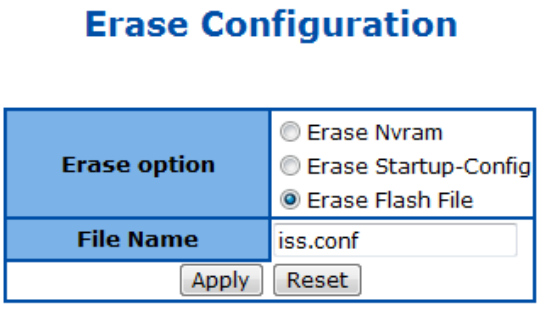


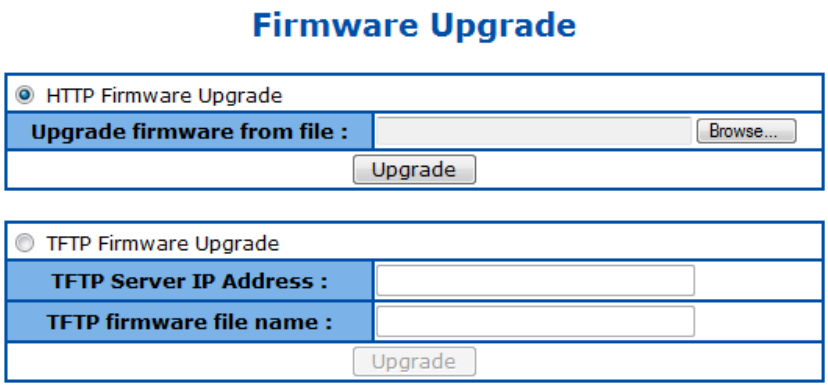
Figure 27 – System > Configuration > Erase

Parameter	Description
Erase option	Specify the configuration to be reset: **Erase Nvram**: Reset the NV-RAM to default settings and reset all previously saved configuration files to default that were stored flash memory. Note: This will only reset the settings in NV-RAM, not the entire device configuration. After rebooting, only the default parameters in NV-RAM will be

	reset to defaults. Requires a manual device reboot for changes to take effect. Please reference the default NV-RAM parameters below. • Default IP Address : 192.168.10.200 • Default Subnet Mask: 255.255.255.0 • Default IP Address Config Mode: Manual • Default IP Address Allocation Protocol : DHCP • Default Interface Name: Fa0/1 • Default RM Interface Name: NONE • Config Restore Option: No restore • Config Save Option: Startup save • Config Save IP Address: 0.0.0.0 • Config Save Filename: iss.conf • Config Restore Filename: iss.conf • PIM Mode: Sparse Mode • IGS Forwarding Mode: MAC based • CLI Serial Console: Yes • SNMP EngineID: 80.00.08.1c.04.46.53 • SNMP Engine Boots: 1 • Default VLAN Identifier: 1 **Erase Startup-Config**: Reset the all device configuration to default settings. Note: This will reset the startup device configuration to default. Any previously saved configuration files in flash memory will NOT be deleted or erased. After a device reboot or power cycle, the default device configuration will be loaded to the device. Requires a manual device reboot for changes to take effect. **Erase Flash File**: Reset the specified configuration file in the device's flash memory to default settings. Note: This will not reset the device's active configuration.
File Name	Specify the file name of the local configuration file.

Click **Apply** to submit the changes and the **Reset** button will clear the information.

Firmware Upgrade



Parameter	Description
HTTP Firmware Upgrade	Click *Browse* to locate the firmware file on the local hard drive and select it.
TFTP Firmware Upgrade	**TFTP Server IP Address:** Specify the IP address of the TFTP server. **TFTP firmware file name:** Specify the filename of the firmware file.

Click **Upgrade** to upgrade the device firmware.

Reboot

This page is to reboot the system.

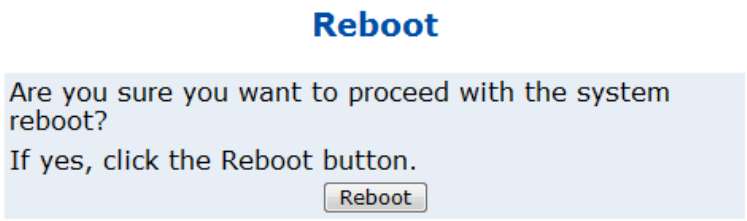


Figure 28 – System > Reboot

Click **Reboot** to warm start the device.

Note If the Switch reboots without write the running configurations, the last configuration wrote in NV-RAM will be loaded.

Chapter 6
Configuring Layer 2 Management Functions

Layer 2 Management Function List

- **Port Manager**
  - Port Basic Settings
  - Port Monitoring
  - Port Control
- **VLAN**
  - VLAN Basic Information
  - VLAN Port Settings
  - Static VLAN Configuration
- **Dynamic VLAN**
  - Dynamic VLAN Global Configuration
  - Dynamic VLAN Port Configuration
  - GARP Timers Configuration
- **MSTP**
  - MSTP Global Configuration
  - MSTP Timers Configuration
  - CIST Settings
  - MSTP VLAN Mapping
  - MSTP Port Settings
  - MSTP CIST Port Status
- **RSTP**
  - RSTP Global Configuration
  - RSTP Configuration
  - RSTP Port Status Configuration
  - RSTP Port Status
- **LA**
  - LA Basic Settings
  - PortChannel Interface Basic Settings
  - LA Port Channel Settings
  - LA Port Settings
  - LA Port StateMachine Information
  - LA Load Balancing Policy
- **802.1X**
  - 802.1X Basic Settings
  - 802.1X Port Settings
  - 802.1X Timer Configuration
  - 802.1X Local Authentication Server Configuration
  - RADIUS Server Configuration
- **IGMP Snooping**
  - IGMP Snooping Configuration
  - IGMP Snooping Timer Configuration
  - IGMP Snooping Interface Configuration
  - IGMP Snooping VLAN Router Ports
  - MAC Based Multicast Forwarding Table
- **Static MAC Entries**
  - Static MAC Address Configuration
  - Static Multicast Address Configuration
  - Port Security Settings

Port Manager

Port Basic Settings

This page is to configure basic settings of switch ports.

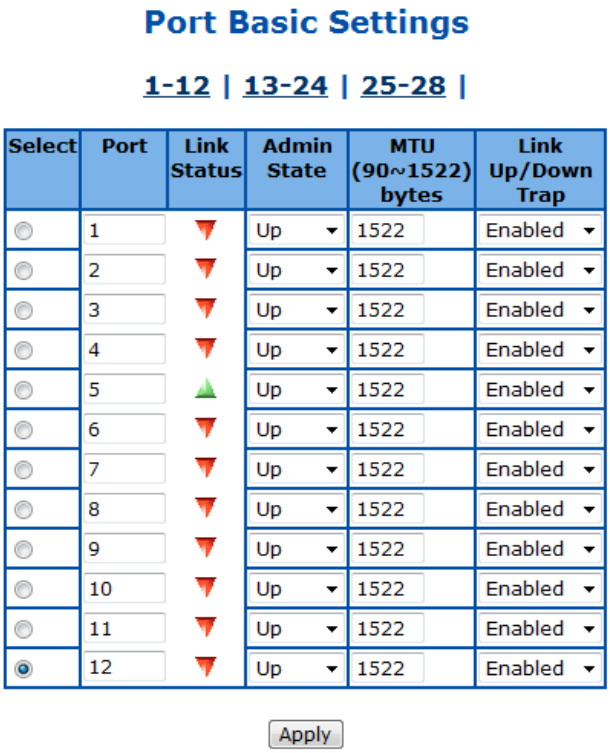


Figure 29 – Layer2 Management > Port Manager > Basic Settings

Parameter	Description
Port	Specify the switch port to be configured.
Link State	Display the physical connection states of the port.
Admin State	Specify the administrative status of the port. Default is *enabled*.
MTU (90-1522) bytes	To setup the Maximum Transmission Unit (MTU) frame size of the interface, and the range is from 90 to 1522 bytes. Default is *1500*.
Link Up/Down Trap	To enable/disable the link up/down trap information delivery. Default is *enabled*.

Click **Apply** to submit the changes.

Port Monitoring

This page is to configure the port monitoring function on the device.

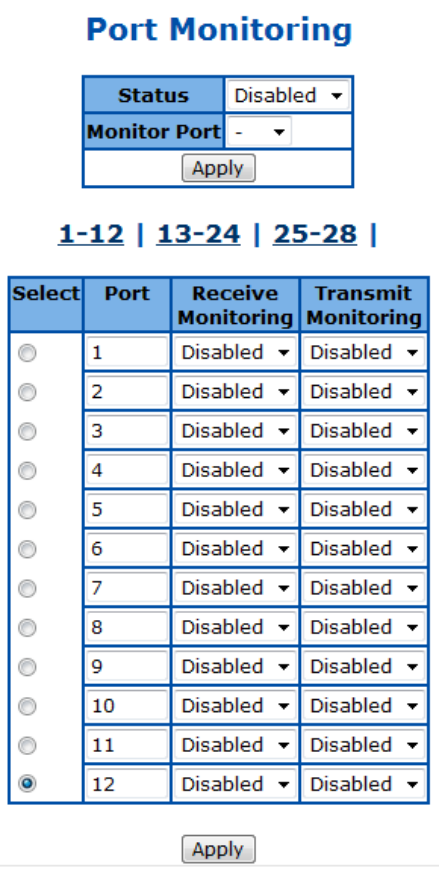


Figure 30 – Layer2 Management > Port Manager > Port Monitoring

Parameter	Description
Status	To enable/disable the port monitoring session on the device. Default is *disabled*.
Monitoring Port	Specify the source port of the mirror session.
Port	Specify the destination port of the mirror session.
Receive Monitoring	Monitoring the traffic received from the source port.
Transmit Monitoring	Monitoring the traffic transmitted from the source port.

Click **Apply** to submit the changes.

Port Control

This page is to configure the control parameters of interface.

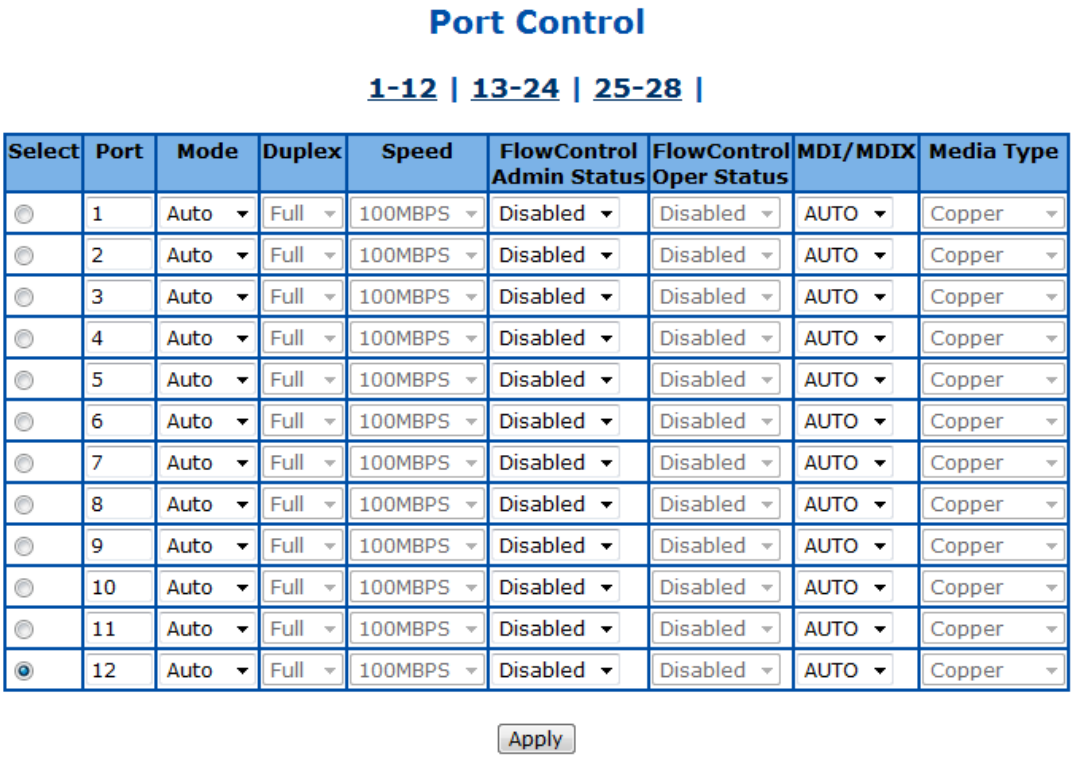


Figure 31 – Layer2 Management > Port Manager > Port Control

Parameter	Description
Port	Specify the switch port to be configured.
Mode	To enable/disable auto-negotiation function on ports. Default is *Auto*.
Duplex	To set the port duplex mode. Possible values are: **Full**: Port runs at full duplex mode. **Half**: Port runs at half duplex mode.
Speed	To set the port speed. Possible values are: **10MBPS**: Port runs at 10Mbps. **100MBPS**: Port runs at 100Mbps. **1GB**: Port runs at 1000Mbps. Only port 25-28 can run at 1000Mbps.
FlowControl Admin Status	To enable/disable 802.3x flow control on ports. Default is *Disabled*.
FlowControl Oper Status	To display the flow control operation status.
MDI/MDIX	To set MDI or MDIX mode for ports. Possible values are: **Auto**: Port performs the auto MDI/MDIX function. **MDI**: Port fixed at MDI mode. **MDIXB:** Port fixed at MDIX mode. Default is *Auto*.

Click **Apply** to submit the changes.

Note The port speed and duplex settings can only be configured when auto-negotiation disabled.

VLAN

VLAN Basic Information

This page is to configure the basic settings of virtual local area network (VLAN) on the device.

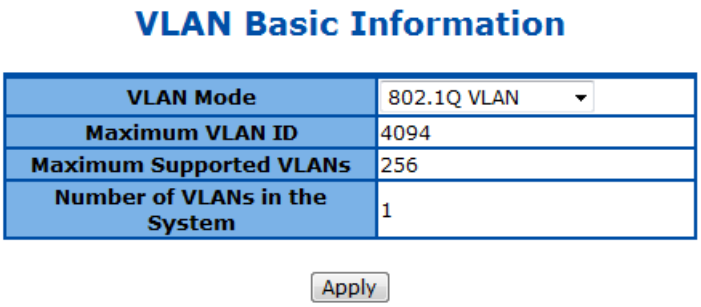


Figure 32 – Layer2 Management > VLAN > Basic Information

Parameter	Description
VLAN Mode	Choose from **802.1Q VLAN** or **Asymmetric VLAN** modes. Default is *802.1Q VLAN*.
Maximum VLAN ID	Display the maximum VLAN ID can be configured. Default is *4094*.
Maximum Supported VLANs	Display the maximum VLANs can be supported. Default is *256*.
Number of VLANs in the System	Display the current VLAN number in the system. Default is *1*.

Click **Apply** to submit the changes.

VLAN Port Settings

This page is to configure VLAN setting on physical port interfaces.

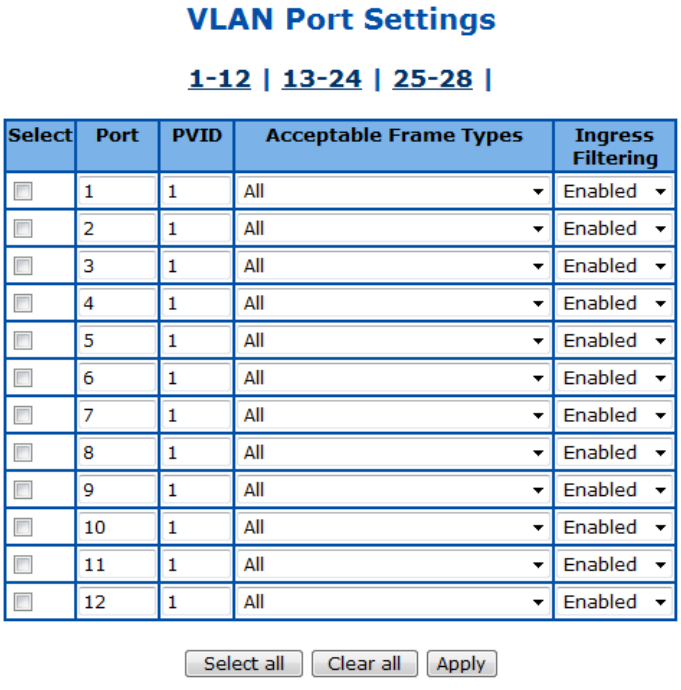


Figure 33 – Layer2 Management > VLAN > Port Settings

Parameter	Description
Port	Specifies the switch port which is to be configured.
PVID	To set the port VLAN ID of the port, all ingress untagged or priority tagged packet from this port will be assign to this VLAN. The range is from 1 to 4094.
Acceptable Frame Types	To configure the acceptable frame type of a port. **All**: Accepts all kinds of frames. **Tagged**: Accepts only tagged frames **UnTagged and Priority Tagged**: Accepts only untagged frames and frames with priority tag. Default is *All*.
Ingress Filtering	To enable/disable the filter of ingress packets not with the same VLAN tag as the VLAN membership of the port. Default is *Enabled*.

In the left-hand **Select** column, check all of the ports modified and click **Apply** to submit the changes.

Static VLAN Configuration

This page is to set up the static VLAN configuration.

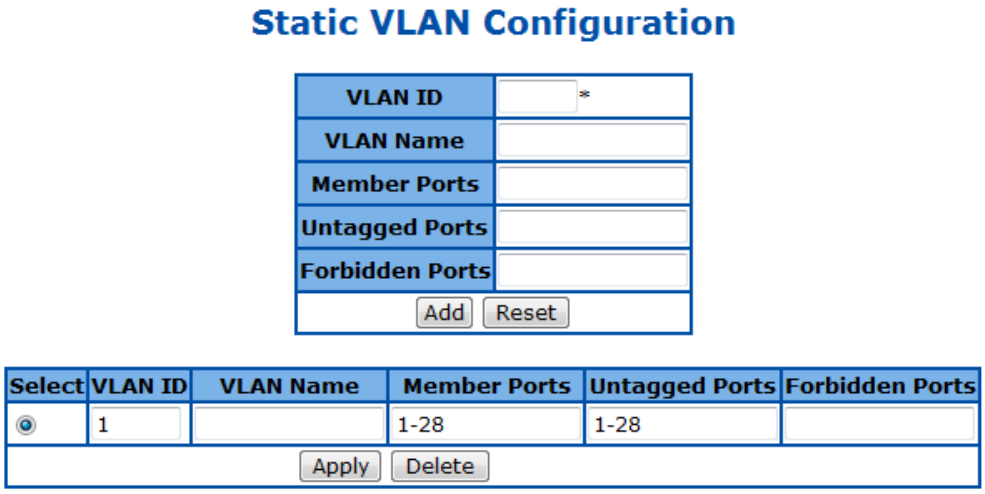


Figure 34 – Layer2 Management > VLAN > Static VLANs

Parameter	Description
VLAN ID	Specify the VLAN ID to be created.
VLAN Name	Specify the name of VLAN.
Member Ports	Specify the ports to apply the VLAN membership.
Untagged Ports	Specify the ports to be untagged interfaces.
Forbidden Ports	Specify the ports to be forbidden interfaces.

Click **Apply** to submit the changes and the **Reset** button will clear the information. Click **Delete** will remove an existed VLAN.

Note There has to be at least one VLAN in the system.

Dynamic VLAN

Dynamic VLAN Global Configuration

This page is to set the global dynamic VLAN configuration.

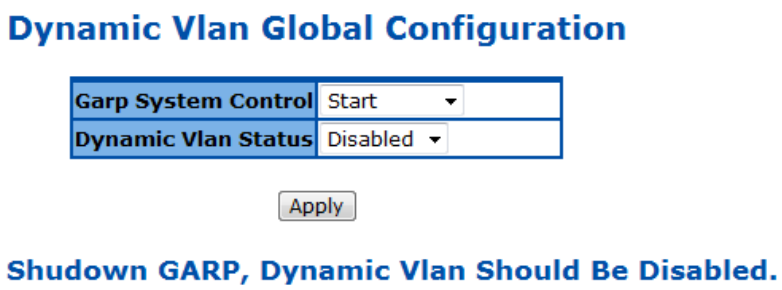


Figure 35 – Layer2 Management > Dynamic VLAN > Dynamic VLAN Global Configuration

Parameter	Description
Garp System Control	Choose **Start** to enable GARP function, and **Shutdown** to disable it. It is needed for using dynamic VLAN function. Default is *Start*.
Dynamic VLAN Status	To set the status of dynamic VLAN function from **Enabled** or **Disabled**. Default is *Disabled*.

Click **Apply** to submit the changes.

Dynamic VLAN Port Configuration

This page is to configure dynamic VLAN settings on switch ports.

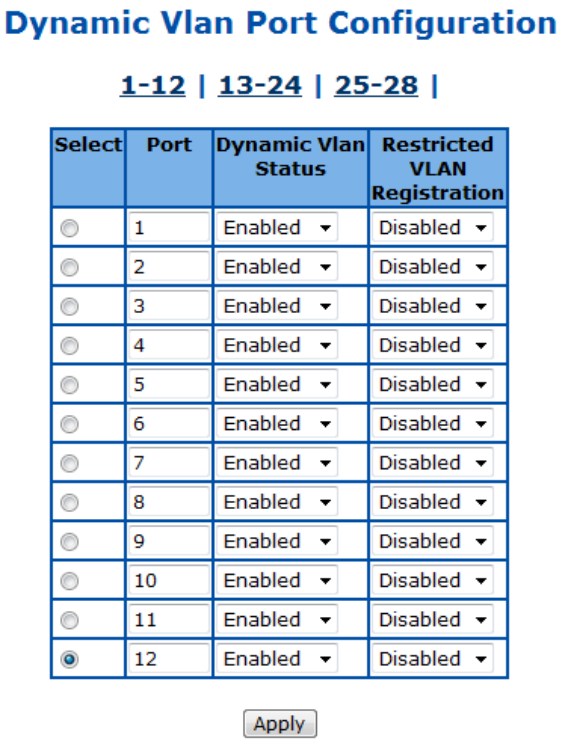


Figure 36 – Layer2 Management > Dynamic VLAN > Port Settings

Parameter	Description
Port	Specify the switch port to be configured.
Dynamic VLAN Status	To set the status of dynamic VLAN function from **Enabled** or **Disabled**.
Restricted VLAN Registration	To enable/disable the restricted VLAN on an interface.

Click **Apply** to submit the changes.

GARP Timers Configuration

This page is to set the GARP timers on an interface.

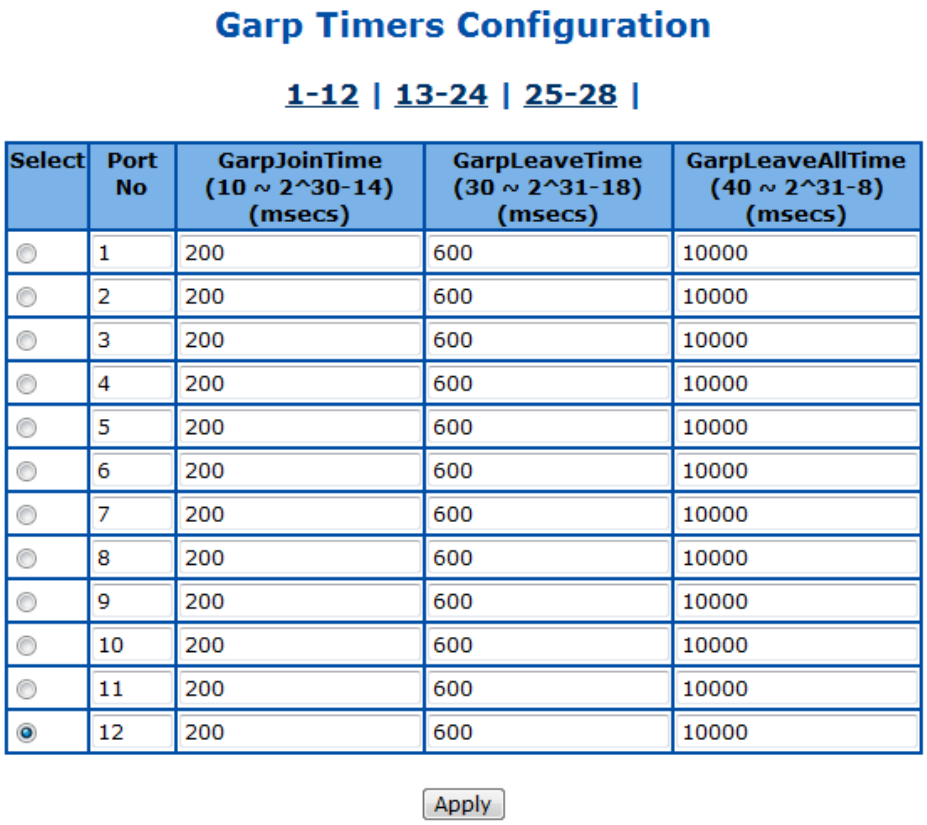


Figure 37 – Layer2 Management > Dynamic VLAN > Port Settings

Parameter	Description
Port No	Specify the switch port to be configured.
GarpJoinTime (10 ~ 2^30-14)(msecs)	Specify the join time of GARP. Default is *20* milliseconds.
GarpLeaveTime (30 ~ 2^31-18)(msecs)	Specify the leave time of GARP. Default is *60* milliseconds.
GarpLeaveAllTime (40 ~ 2^31-8)(msecs)	Specify the leave all time of GARP. Default is *100* milliseconds.

Click **Apply** to submit the changes.

MSTP

MSTP Global Configuration

This page is to configure the MSTP global settings of the Switch.

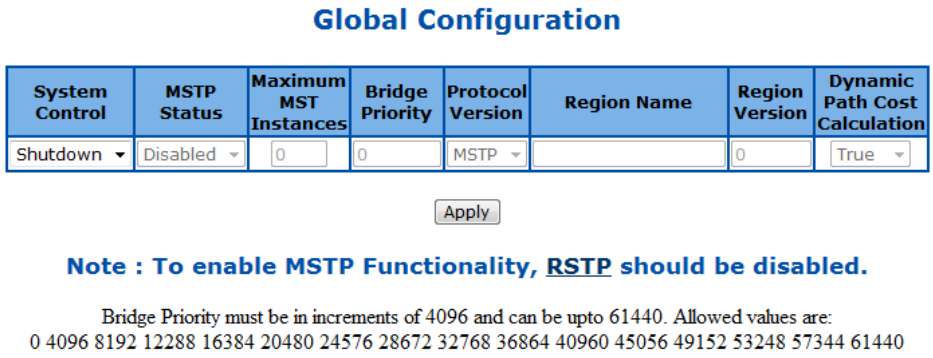


Figure 38 – Layer2 Management > MSTP > Global Configuration

Parameter	Description
System Control	To activate or shutdown the MSTP function. Select **Start** to activate the MSTP function, **Shutdown** to shutdown MSTP function.
MSTP Status	To enable or disable the MSTP. Select **Enabled t**o enable the MSTP function, **Disabled** to disable the MSTP function.
Maximum MSTP Instances	Specify the maximum number of MSTP instance allowed. The possible number is 1-64. Default is 64.
Bridge Priority	Specify the bridge priority of spanning tree. Default is 32768.
Protocol Version	Select the spanning tree compatibility version. The possible options are **STP**, **RSTP** and **MSTP**. Default is RSTP.
Region Name	Specify the region name of MST.
Region Version	Specify the MST region revision. The possible numbers are 0~65535, default is 0.
Dynamic Path Cost Calculation	Select the path cost calculation mode of spanning tree. Select **True** to enable dynamic path cost according to the port speed, **False** to disable it. Default if **False**.

Click **Apply** to submit the changes.

Note

1. RSTP function must be shutdown before activate MSTP.
2. MSTP status must be enabled before configure other MSTP details.

MSTP Timers Configuration

This page is to configure the MSTP timers of the Switch.

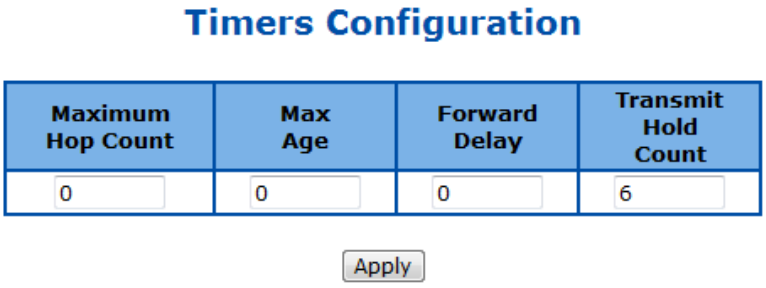


Figure 39 – Layer2 Management > MSTP > Timers Configuration

Parameter	Description
Maximum Hop Count	Specify the maximum hops permitted in MST. Possible value is 6-40. Default is 20.
Max Age	Specify the maximum age in second for STP information learned from the network on any port before it is discarded. The possible value is 6-40. Default

	is 20.
Forward Delay	Specify the time period in second that a port changes the STP state from blocking to forwarding. The possible value is 4-30. Default is 15.
Transmit Hold Count	Specify the hold counter to limit maximum transmission rate of the Switch. Default is 3.
Hello Time	Specify the time interval in second for a root bridge broadcasts the hello packets to other switches. Possible value is 1-2. Default is 2.

CIST Settings

This page is to configure the port related MSTP settings.

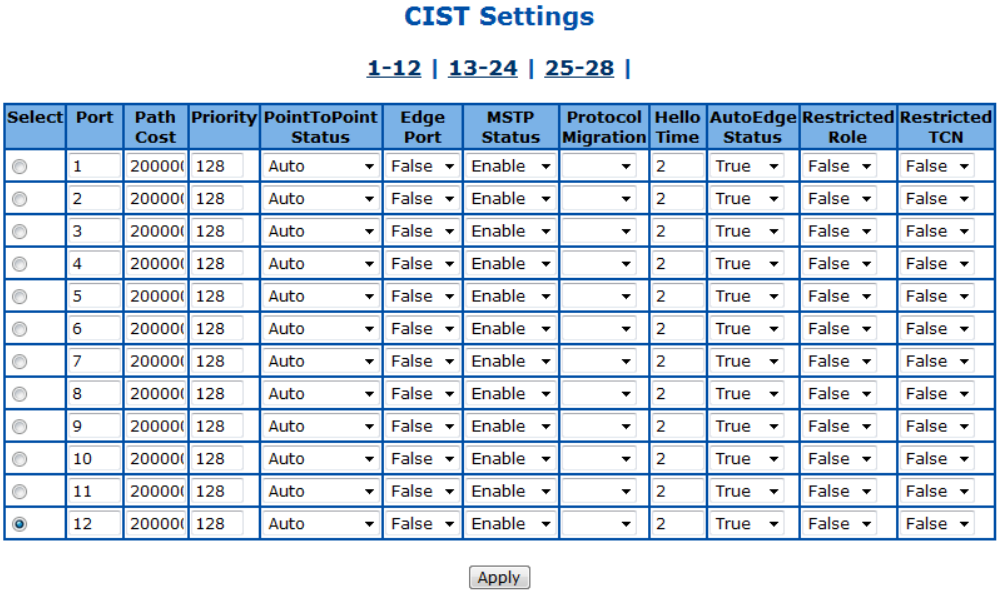


Figure 40 – Layer2 Management > MSTP > Port Configuration

Parameter	Description
Select	Select a port to apply the configuration changes.
Port	Port ID.
Path Cost	Specify the path cost of the port. Possible value is 0-200000000. Default 200000000
Priority	Specify the spanning tree port priority. Possible value is 0-240. Default is 128.
Point to Point Status	Specify the link type of this port. **ForceTrue** means link type is point to point; **ForceFalse** means it is shared; **Auto** means the decision will made automatically. Default is auto.
Edge Port	Specify if this port is edge port or not. Select **True** to enable the portfast function, **False** to disable it. Default is false.
MSTP Status	To enable or disable the MSTP on this port. Select **Enable** to enable MSTP on this port, **Disable** to disable it. Default is enabled.
Protocol Migration	To control if the port will migrate among MSTP, RSTP and STP automatically if another switch runs different protocol. Select **True** to enable the protocol migration function, **False** to disable it. Default is False.
Hello Time	Specify the hello time of this port. Possible value is 1-2. Default is 2.
AutoEdge Status	To enable or disable the auto edge detection of this port. Select **True** to enable the auto edge function, **False** to disable it. Default true.
Restricted Role	To enable or disable the root guard function to prevent the port becoming a root port. Select **True** to enable the root guard function, **False** to disable it. Default is false.
Restricted TCN	To enable the topology change guard function to prevent the topology change caused by this port. Select **True** to enable the topology change guard

	function, **False** to disable it. Default is false.

Click **Apply** to submit the changes.

MSTP VLAN Mapping

This page is to configure the MST Instance and VLAN mapping.

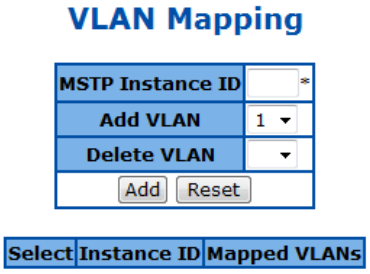


Figure 41 – Layer2 Management > MSTP > VLAN Mapping

Parameter	Description
MSTP Instance ID	Specify which MST instance to be mapped.
Add VLAN	Add a VLAN to the map list of this MST instance.
Delete VLAN	Delete a VLAN from the map list of this MST instance.

Click **Add** to submit the changes, **Reset** to clear the value.

MSTP Port Settings

This page is to configure the port related MSTP settings.

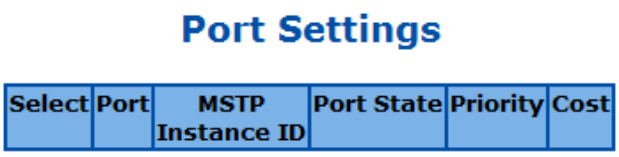
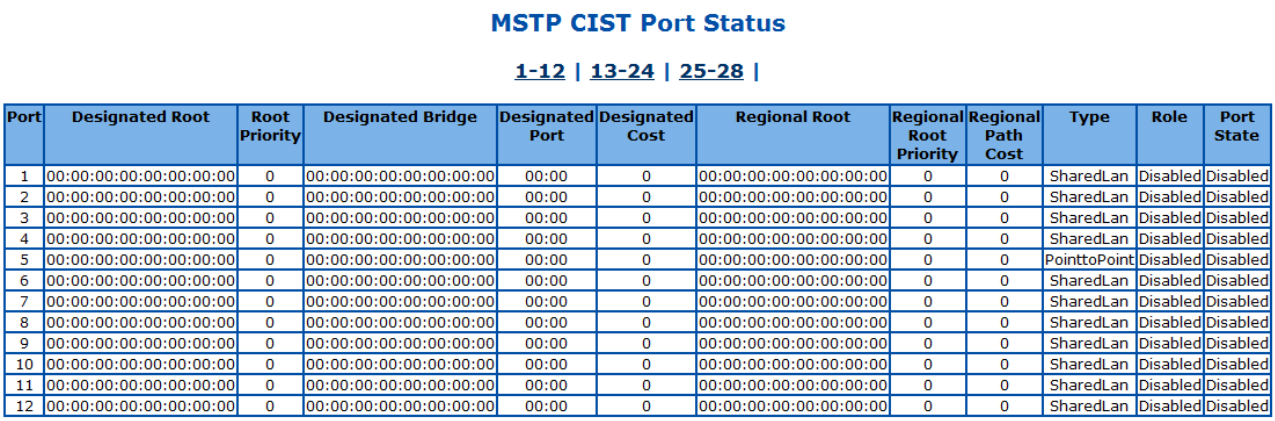


Figure 42 – Layer2 Management > MSTP > Port Settings

Parameter	Description
Select	Select a port to apply the changes.
Port	Port ID.
MSTP Instance ID	Specify the MST instance IP of this port.
Port State	Specify the current state of this port.
Priority	Specify the spanning tree port priority. Possible value is 0-240. Default is 128.
Cost	Specify the path cost of the port. Possible value is 0-200000000. Default 200000000

MSTP CIST Port Status

To display the current MSTP CIST port status.



MSTP CIST Port Status

1-12 | 13-24 | 25-28 |

Port	Designated Root	Root Priority	Designated Bridge	Designated Port	Designated Cost	Regional Root	Regional Root Priority	Regional Path Cost	Type	Role	Port State
1	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	00:00	0	00:00:00:00:00:00:00:00	0	0	SharedLan	Disabled	Disabled
2	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	00:00	0	00:00:00:00:00:00:00:00	0	0	SharedLan	Disabled	Disabled
3	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	00:00	0	00:00:00:00:00:00:00:00	0	0	SharedLan	Disabled	Disabled
4	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	00:00	0	00:00:00:00:00:00:00:00	0	0	SharedLan	Disabled	Disabled
5	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	00:00	0	00:00:00:00:00:00:00:00	0	0	PointtoPoint	Disabled	Disabled
6	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	00:00	0	00:00:00:00:00:00:00:00	0	0	SharedLan	Disabled	Disabled
7	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	00:00	0	00:00:00:00:00:00:00:00	0	0	SharedLan	Disabled	Disabled
8	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	00:00	0	00:00:00:00:00:00:00:00	0	0	SharedLan	Disabled	Disabled
9	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	00:00	0	00:00:00:00:00:00:00:00	0	0	SharedLan	Disabled	Disabled
10	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	00:00	0	00:00:00:00:00:00:00:00	0	0	SharedLan	Disabled	Disabled
11	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	00:00	0	00:00:00:00:00:00:00:00	0	0	SharedLan	Disabled	Disabled
12	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	00:00	0	00:00:00:00:00:00:00:00	0	0	SharedLan	Disabled	Disabled

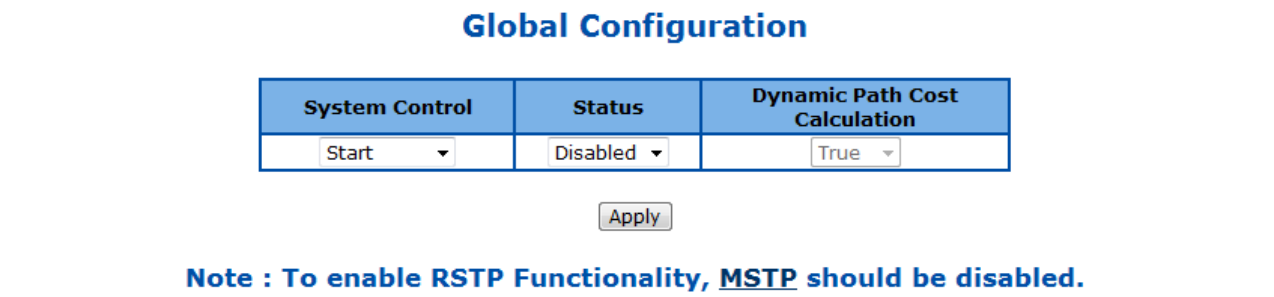
Figure 43 – Layer2 Management > MSTP > CIST Port Status

Click **1-12, 13-24, 25-28** to display the statistics for corresponding ports.

RSTP

RSTP Global Configuration

This page is to configure the RSTP global settings.



Global Configuration

System Control	Status	Dynamic Path Cost Calculation
Start	Disabled	True

Apply

Note : To enable RSTP Functionality, MSTP should be disabled.

Figure 44 – Layer2 Management > RSTP > Global Settings

Parameter	Description
System Control	To activate or shutdown the RSTP function. Select **Start** to activate the MSTP function, **Shutdown** to shutdown MSTP function.
Status	To enable or disable the MSTP. Select **Enabled** to enable the MSTP function, **Disabled** to disable it. Default is disabled.
Dynamic Path Cost Calculation	Select the path cost calculation mode of spanning tree. Select **True** to enable dynamic path cost according to the port speed, **False** to disable it. Default if **False**.

Click **Apply** to submit the changes.

Note

1. MSTP function must be shutdown before activate RSTP.
2. RSTP status must be enabled before configure other RSTP details.

RSTP Configuration

This page is to configure the timers and other details of RSTP functions.

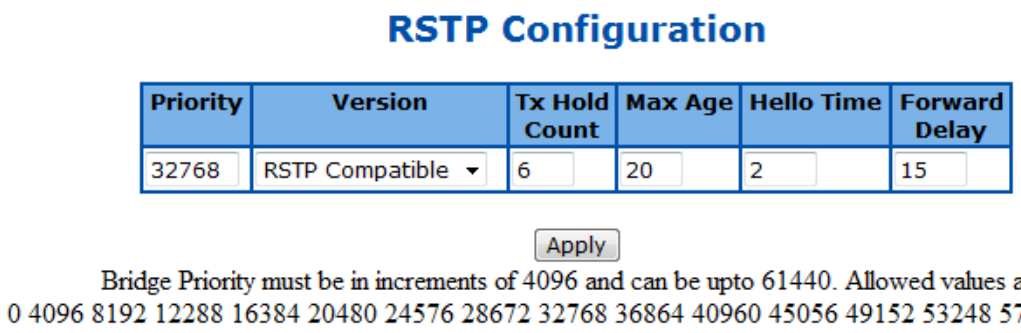


Figure 45 – Layer2 Management > RSTP > Basic Settings

Parameter	Description
Priority	Specify the bridge priority of spanning tree. Default is 32768.
Version	Select the spanning tree compatibility version. The possible options are **STP Compatible or RSTP Compatible**. Default is **RSTP Compatible**.
Tx Hold Count	Specify the hold counter to limit maximum transmission rate of the Switch. Default is 6.
Max Age	Specify the maximum age in second for STP information learned from the network on any port before it is discarded. The possible value is 6-40. Default is 20.
Help Time	Specify the time interval in second for a root bridge broadcasts the hello packets to other switches. Possible value is 1-2. Default is 2.
Forward Delay	Specify the time period in second that a port changes the STP state from blocking to forwarding. The possible value is 4-30. Default is 15.

Click **Apply** to submit the changes.

RSTP Port Status Configuration

This page is to configure the port related RSTP settings

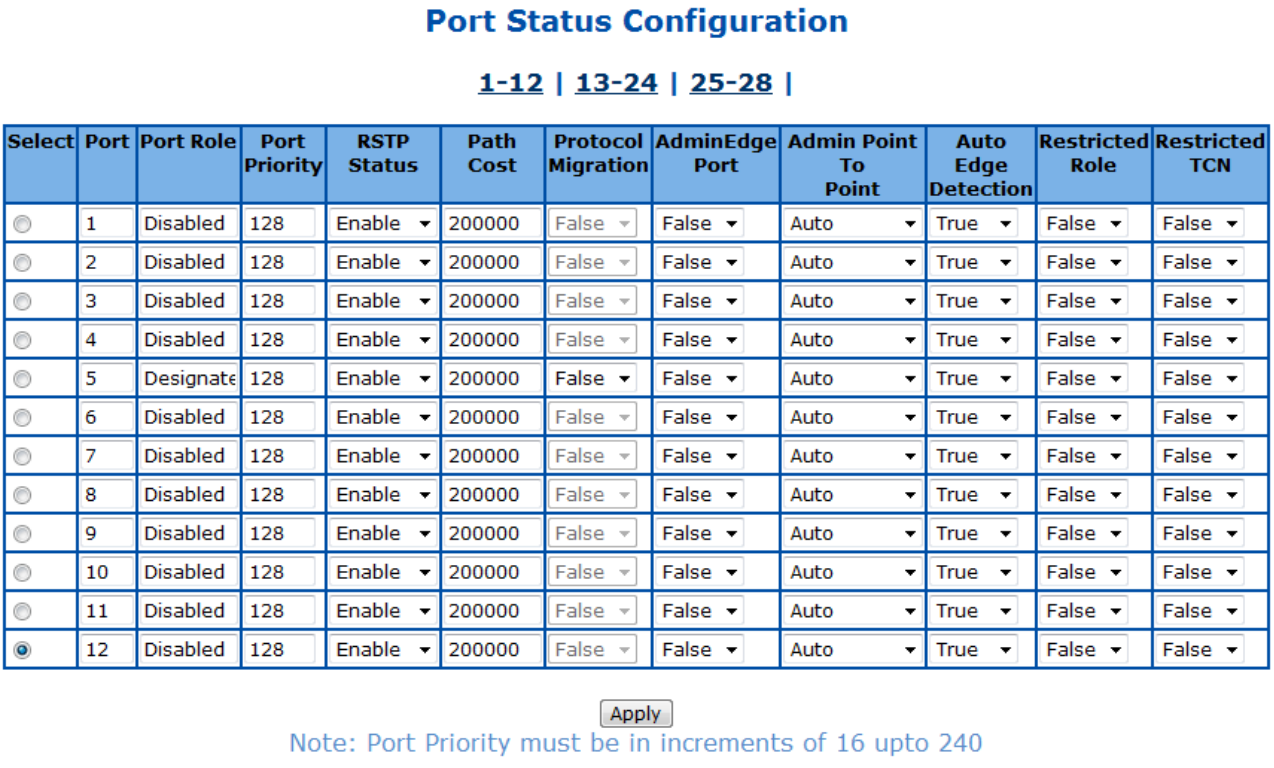


Figure 46 – Layer2 Management > RSTP > Port Settings

Parameter	Description
Select	Select a port to apply the changes.
Port	Port ID.
Port Role	Specify the current role of the port.
Port Priority	Specify the spanning tree port priority. Possible value is 0-240. Default is 128.
RSTP Status	To enable or disable the RSTP on this port. Select **Enable** to enable RSTP on this port, **Disable** to disable it. Default is enabled.
Path Cost	Specify the path cost of the port. Possible value is 0-200000000. Default 65535
Protocol Migration	To control if the port will migrate among MSTP, RSTP and STP automatically if another switch runs different protocol. Select **True** to enable the protocol migration function, **False** to disable it. Default is False.
Admin Edge Port	Specify if this port is edge port or not. Select **True** to enable the portfast function, **False** to disable it. Default is False.
Admin Point To Point	Specify the link type of this port. **ForceTrue** means link type is point to point; **ForceFalse** means it is shared; **Auto** means the decision will made automatically. Default is Auto.
AutoEdge Detection	To enable or disable the auto edge detection of this port. Select **True** to enable the auto edge function, **False** to disable it. Default True.
Restricted Role	To enable or disable the root guard function to prevent the port becoming a root port. Select **True** to enable the root guard function, **False** to disable it. Default is False.
Restricted TCN	To enable the topology change guard function to prevent the topology change caused by this port. Select **True** to enable the topology change guard function, **False** to disable it. Default is False.

RSTP Port Status

To display the current RSTP port status.

RSTP Port Status

1-12 | 13-24 | 25-28 |

Port	Designated Root	Designated Cost	Designated Bridge	Designated Port	Type	Role	Port State
1	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	00:00	SharedLan	Disabled	Blocking
2	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	00:00	SharedLan	Disabled	Blocking
3	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	00:00	SharedLan	Disabled	Blocking
4	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	00:00	SharedLan	Disabled	Blocking
5	80:00:00:02:e2:84:00:01	0	80:00:00:02:e2:84:00:01	80:05	Point-to-Point	Designated	Forwarding
6	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	00:00	SharedLan	Disabled	Blocking
7	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	00:00	SharedLan	Disabled	Blocking
8	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	00:00	SharedLan	Disabled	Blocking
9	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	00:00	SharedLan	Disabled	Blocking
10	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	00:00	SharedLan	Disabled	Blocking
11	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	00:00	SharedLan	Disabled	Blocking
12	00:00:00:00:00:00:00:00	0	00:00:00:00:00:00:00:00	00:00	SharedLan	Disabled	Blocking

Figure 47 – Layer2 Management > RSTP > Port Status

Click **1-12, 13-24, 25-28** to display the statistics for corresponding ports.

LA

LA Basic Settings

This page is to configure the link aggregation basic settings.

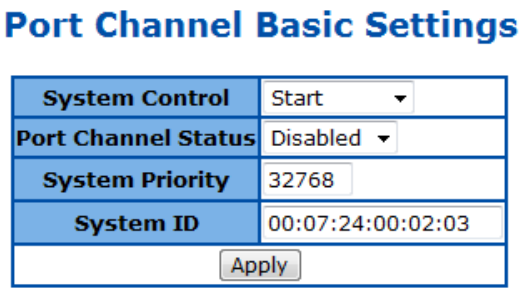


Figure 48 – Layer2 Management > LA > Basic Settings

Parameter	Description
System Control	To activate or shutdown link aggregation function of the Switch. Select **Start** to activate link aggregation function, **Shutdown** to shutdown it. Default is Start.
LA Status	To enable or disable the link aggregation function of the Switch. Select **Enabled** to enable the LA function, **Disabled** to disable it. Default is Disabled.
System Priority	To set the LACP priority of the Switch. Possible value is 0-65535. Default is 32768.
System ID	Specify the link aggregation system ID of the Switch.

Click **Apply** to submit the changes.

PortChannel Interface Basic Settings

This page is to configure details of a port channel.

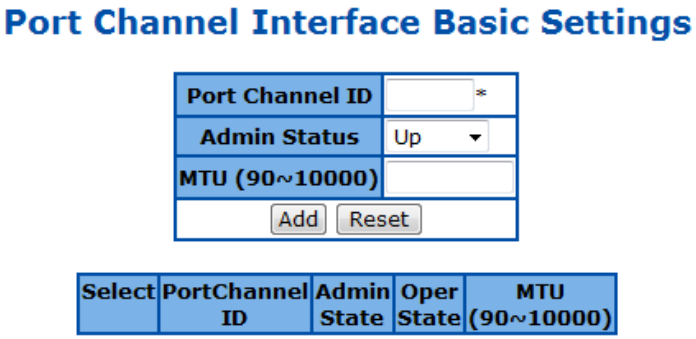


Figure 49 – Layer2 Management > LA > Interface Settings

Parameter	Description
Port Channel ID	Specify the ID of port channel that will apply the changes.
Admin Status	To activate or shutdown a port channel interface. Select **Up** to activate it, **Down** to shutdown it. Default is UP
MTU	Specify the Maximum Transmission Unit (MTU) frame size of the interface.

Click **Add** to submit the changes, **Reset** to clear the value.

LA Port Channel Settings

This page is to configure the details of a port channel.

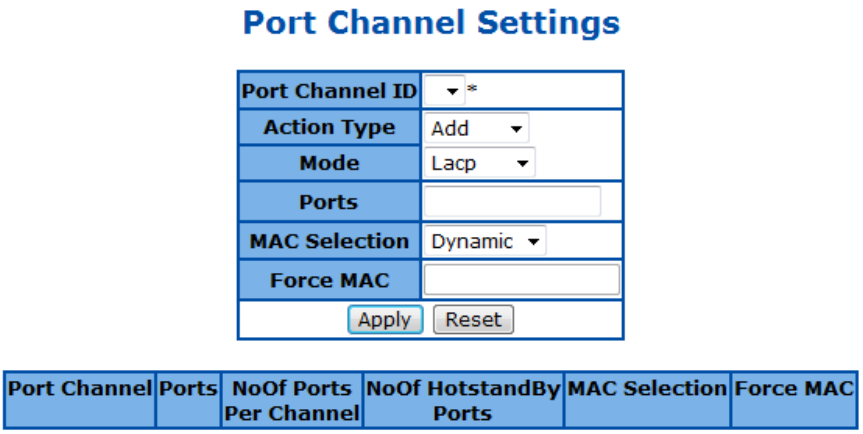


Figure 50 – Layer2 Management > LA > Port Channel Settings

Parameter	Description
Port Channel ID	Select a configured port channel group to submit the changes.
Action Type	To add or delete ports from/to a port channel. Select **Add** to add ports, **Delete** to delete one.
Mode	Specify the mode of this port channel. Possible options are **Lacp** and **Manual**. Default is Lacp
Ports	Specify which port to be included in this port channel.
MAC Selection	Specify the MAC address of the port channel. Select **Dynamic** to let system assign the MAC address to the port channel automatically, or select **Manual** to use a manual configured MAC address.
Force MAC	Specify the manual configured MAC address of this port channel.

Click **Apply** to submit the configurations, **Reset** to clear the value.

LA Port Settings

This page is to configure port related link aggregation settings.

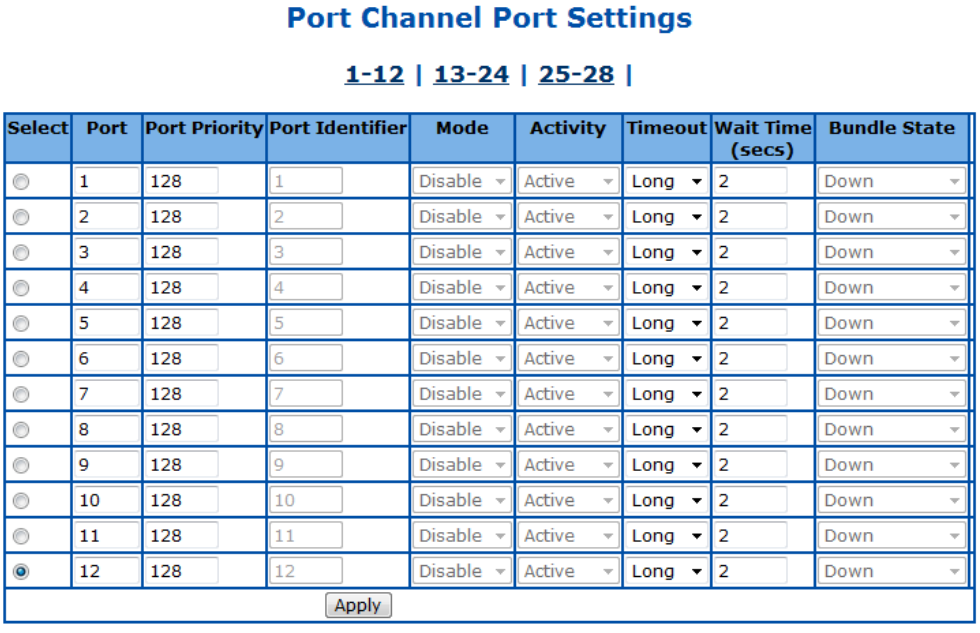


Figure 51 – Layer2 Management > LA > Port Settings

Parameter	Description
Select	Select a port to submit the changes.
Port	Port ID.
Port Priority	Specify the link aggregation port priority of this port. Possible values are 0-65535. Default is 128.
Port Identifier	Port ID.
Mode	Specify the mode of this port channel. Possible options are **Lacp**, **Manual** and **Disable**.
Activity	Specify the LACP mode of the port. Select **Active** to activate the LACP negotiation; select **Passive** that LACP negotiation starts only when LACP packet is received. Default is Active.
Timeout	To choose the LACP timeout period when no packet receive from peer. **Long** specifies a long time out value. LACP PDU will be sent every 30 seconds and LACP timeout value is 90 seconds. **Short** specifies a short time out value. LACP PDU will be sent every 1 seconds and LACP timeout value is 3 seconds
Wait Time (secs)	Specify the period that ports get aggregated after receiving LACP PDU. Possible value is 0-10 seconds. Default is 2.
Bundle State	Specify the current LA state of this port. And the states descriptions are: **Up in Bundle** - This port is an active member of a port channel. **Up Individual** - This port is not a member of any port channel but its operation state is Up. **Standby** - This port is a standby member of a port channel. **Down - T**his port operation state is down.

Click **Apply** to submit the changes.
Click **1-12, 13-24, 25-28** to configure LA port settings for corresponding ports.

LA Port StateMachine Information

This page is to display the LA state of each port.

Figure 52 – Layer2 Management > LA > Port State Info

LA Load Balancing Policy

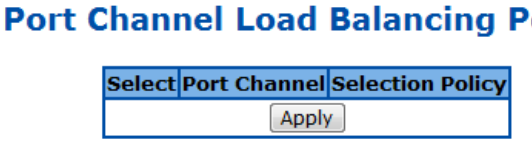


Figure 53 – Layer2 Management > LA > Load Balancing

Parameter	Description
Select	Select a port channel to apply the configuration change.
Port Channel	Port Channel ID.
Selection Policy	Select a load balancing algorithm for the port channel. The traffic will hash between the member ports of a port channel based on the rule selected. The options are **MAC Source**, **MAC Destination**, **MAC Source and Destination**, **IP Source**, **IP Destination**, **and IP Source and Destination**. Default is MAC Source and Destination.

Click **Apply** to submit the changes.

802.1X

802.1X Basic Settings

This page is used to configure the 802.1X authentication global settings.

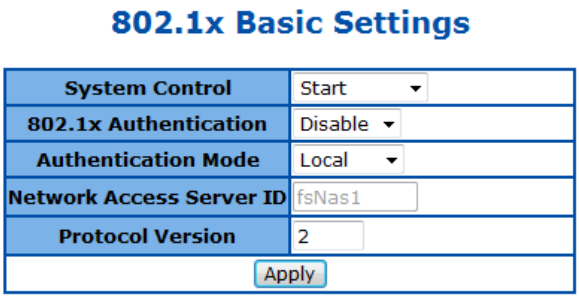


Figure 54 – Layer2 Management > 802.1X > Basic Settings

Parameter	Description
System Control	To activate or shutdown 802.1X function of the Switch. Select **Start** to activate the function, **Shutdown** to shutdown it. Default is Start.
802.1X Authentication	To enable or disable the 802.1X authentication of the Switch. Select **Enabled** to enable the function, **Disabled** to disable it. Default is Disabled.
Authentication Mode	Select the authentication database for 802.1X. **Remote** is to use the RADIUS server; **Local** will use the local database. Default is Local.
Network Access Server ID	Specify the remote RADIUS server authenticator ID.
Protocol Version	Specify the protocol version of 802.1X.

Click **Apply** to submit the changes.

802.1X Port Settings

This page is to configure the port related setting of 802.1X.

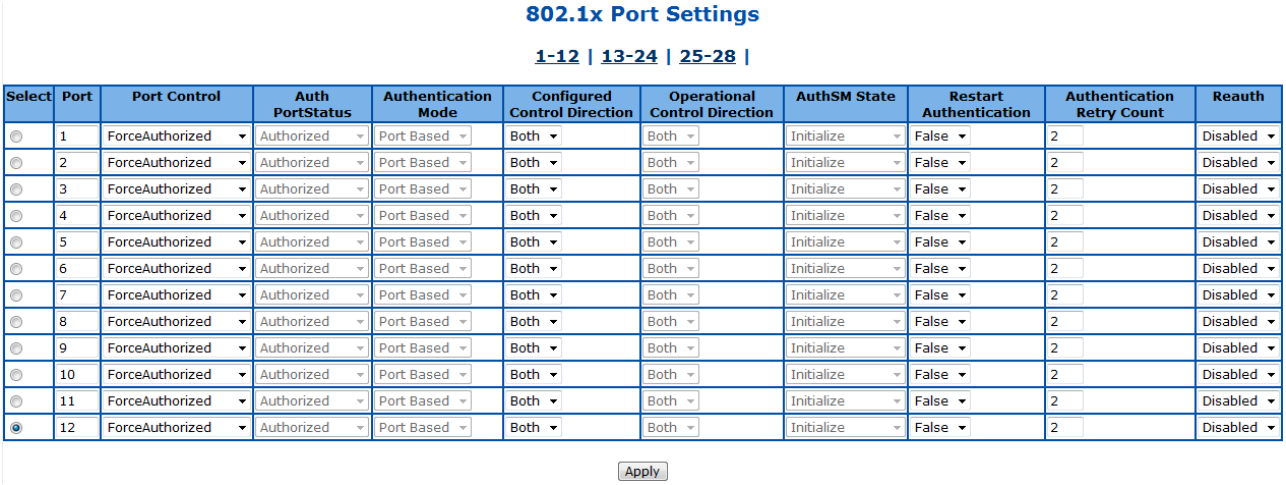


Figure 55 – Layer2 Management > 802.1X > Port Settings

Parameter	Description
Select	Select a port to apply the configuration changes.
Port	Port ID.
Port Control	To set the authenticator control on this port. The possible options are: **ForceUnauthorized** - All traffic is blocked to the port. **Auto** - Enable the 802.1X authentication on this port, and the port authorized or unauthorized will based on the 802.1X authentication result. **ForceAuthorized** - All traffic is transparent to the port. Default is ForceAuthorized.
Auth PortStatus	Current authentication status of this port.
Authentication Mode	The authentication mode of this port. Only Port-based mode is supported currently.
Configured Control Direction	To choose the authentication control direction on this port. **In** - Authentication control is only for ingress packets. **Both** - Authentication control is for both ingress and egress packets. Default is Both.
Operational Control Direction	The current authentication direction on this port.
AuthSM State	The current authentication state of this port.
Restart Authentication	To enable periodic re-authentication on this port.
Authentication Retry Count	To set the maximum 802.1X Extensible Authentication Protocol (EAP) retries of the client before restarting authentication process.
Reauth	To enable or disable the authentication retry function. Default is Disabled.

Click **Apply** to submit the changes.
Click **1-12, 13-24, 25-28** to configure 802.1X port settings for corresponding ports.

802.1X Timer Configuration

This page is to configure the 802.1X timers of the device.

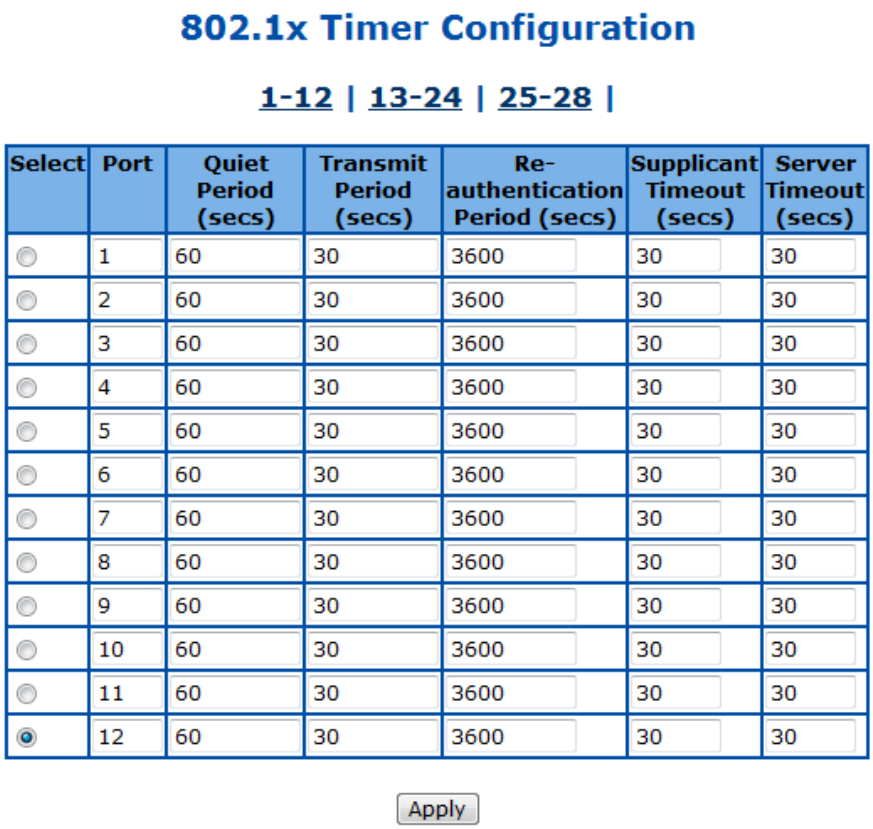


Figure 56 – Layer2 Management > 802.1X > Timers

Parameter	Description
Select	Select a port to apply the configuration changes.
Port	Port ID.
Quiet Period (secs)	The period that Switch will not do anything after a failed authentication. Possible value is 0-65535 seconds. Default is 60.
Transmit Period (secs)	The period that Switch waits for a response to an EAP-request/identity frame from the client before retransmitting the request. Possible values are 1-65535 seconds. Default is 30.
Re-authentication Period (secs)	The period between re-authentication attempts. Possible value is 1-65535 seconds. Default is 3600.
Supplicant Timeout (secs)	The period that Switch waits for the re-transmission to the client. Possible value is 1-65535 seconds. Default is 30.
Server Timeout (secs)	The period that Switch waits for the re-transmission to the RADIUS server. Possible value is 1-65535 seconds. Default is 30.

Click **Apply** to submit the changes.
Click **1-12, 13-24, 25-28** to configure 802.1X timer settings for corresponding ports.

802.1X Local Authentication Server Configuration

This page is to configure the 802.1X local user database.

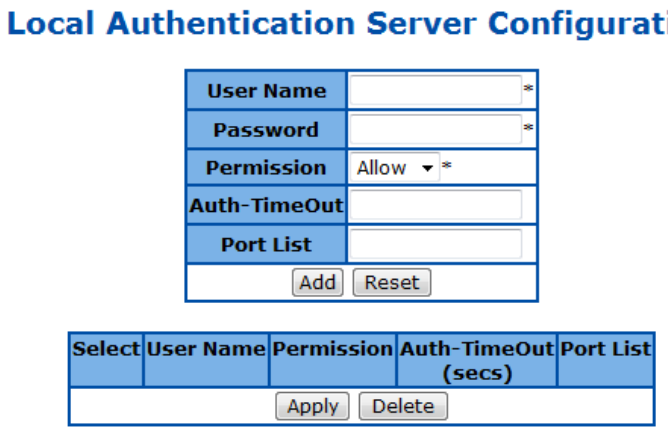


Figure 57 – Layer2 Management > 802.1X > Local AS

Parameter	Description
User Name	Specify the user name of the new user entry.
Password	Specify the password of the new user entry.
Permission	Specify if the new user is allowed to access the network.
Auth-TimeOut	Specify the authentication timeout for the new user.
Port List	Specify which port that the new user is allowed to access.

Click **Add** to add a new user entry, **Reset** to clear the value.

Parameter	Description
Select	Select an existing user entry to apply new settings.
User Name	The user ID.
Permission	Specify if the user is allowed to access the network.
Auth-TimeOut	Specify the authentication timeout for the user.
Port List	Specify which port that the user is allowed to access.

Click **Apply** to submit the changes to existing user account, **Delete** to delete one.

RADIUS Server Configuration

This page is to configure the details of RADIUS server.

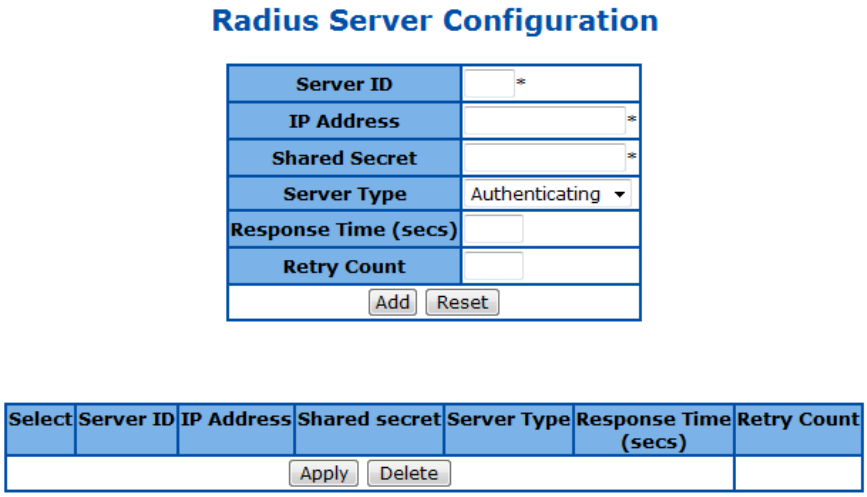


Figure 58 – Layer2 Management > 802.1X > Radius Settings

Parameter	Description
Server ID	Specify the new RADIUS server ID. The possible ID is 1-10.
IP Address	Specify the IP address of the new RADIUS server.
Shared Secret	Specify the encryption key between RADIUS server and clients.
Server Type	Specify the server type of the RADIUS server. The options are: **Authenticating** – This server is only for RADIUS authentication. **Accounting** - This server is only for RADIUS accounting. **Both** - This RADIUS server support both authentication and accounting.
Response Time (secs)	Specify the time period that a client waits for the response from the RADIUS server before re-sending the request. The possible number is 1-120 seconds.
Retry Count	The maximum number that a client re-sends the request when there is no response from RADIUS server. The possible number is 1-254 times.

Click **Add** to add a new RADIUS server, **Reset** to clear the value.

Parameter	Description
Select	
Server ID	The RADIUS server ID.
IP Address	Specify the IP address of the RADIUS server.
Shared Secret	Specify the encryption key between RADIUS server and clients.
Server Type	Specify the server type of the RADIUS server. The options are: **Authenticating** – This server is only for RADIUS authentication. **Accounting** - This server is only for RADIUS accounting. **Both** - This RADIUS server support both authentication and accounting.
Response Time (secs)	Specify the time period that a client waits for the response from the RADIUS server before re-sending the request. The possible number is 1-120 seconds.
Retry Count	The maximum number that a client re-sends the request when there is no response from RADIUS server. The possible number is 1-254 times.

Click **Apply** to submit the changes the setting of an existing RADIUS server, **Delete** to delete one.

IGMP Snooping

IGMP Snooping Configuration

This page is to configure the IGMP Snooping global settings.

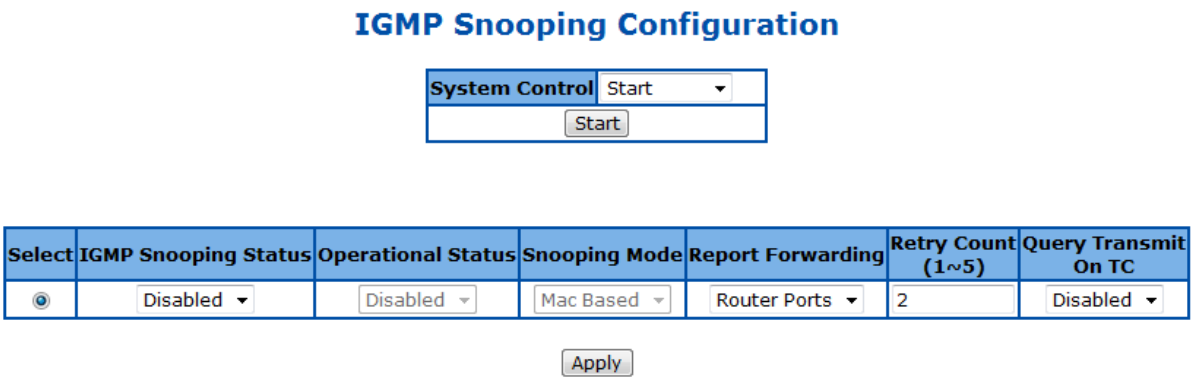


Figure 59 – Layer2 Management > IGMP Snooping > Basic Settings

Parameter	Description
System Control	To activate or shutdown IGMP snooping of the Switch. Select **Start** to activate the function, **Shutdown** to shutdown it. Default is Start.

Click **Start** to start or shutdown the IGMP Snooping globally.

Parameter	Description
Select	Select a line to change the configuration.
IGMP Snooping Status	To enable or disable IGMP Snooping globally. Default is enabled.
Operational Status	Specify the operational status of IGMP snooping function.
Snooping Mode	Specify the Snooping mode of IGMP snooping function.
Report Forwarding	Specify which port to forward the IGMP report. Select **All Ports** to forward the report to all ports, **Router Ports** to forward the reports to IGMP router ports only. Default is Router Ports.
Retry Count (1~5)	To set the maximum retries for group specific queries which sent to a port received an IGMPv2 leave message. The possible number is 1-5 times. Default is 2.
Query Transmit On TC	Specify if the IGMP queries will still be sent when STP topology change happens. Select **Enable** to transmit the queries, **Disable**d not to transmit. Default is Disabled.

Click **Apply** to submit the changes.

IGMP Snooping Timer Configuration

This page is to configure the IGMP Snooping timers.

Note: When configured as querier in a VLAN, the Group-Member Port Purge Interval will be calculated by the program automatically as (Group-Member Port Purge Interval = Retry Count * Querier Query Interval + Max. Response Time). When configured as non-querier in a VLAN, the Group-Member Port Purge Interval will be as the configured value in the above field.

Figure 60 – Layer2 Management > IGMP Snooping > Timer Configuration

Parameter	Description
Router Port Purge Interval (60~600 Secs)	To set the time-out period that an IGMP multicast router port hasn't received IGMP router control packet, it will be deleted. Default is 125 seconds.
Group-Member Port Purge Interval (130~2335 Secs)	To set the purge interval that an IGMP member port hasn't' received IGMP report packet, it will be deleted. Default is 260 seconds.
Report Forward Interval (1~25 Secs)	To set the time interval that IGMPv2 report of the same group will not be forwarded to the router ports. Default is 5 seconds.
Group Query Interval (1~5 Secs)	To set up the time interval to send the group specific query. Default is 2 seconds.
Querier Query Interval (60~600 Secs)	To set up the time interval to send the IGMP general query. Default is 125 seconds.

Click **Apply** to submit the changes, **Reset** to clear the values.

IGMP Snooping Interface Configuration

This page is used to configure the VLAN basis IGMP snooping settings.

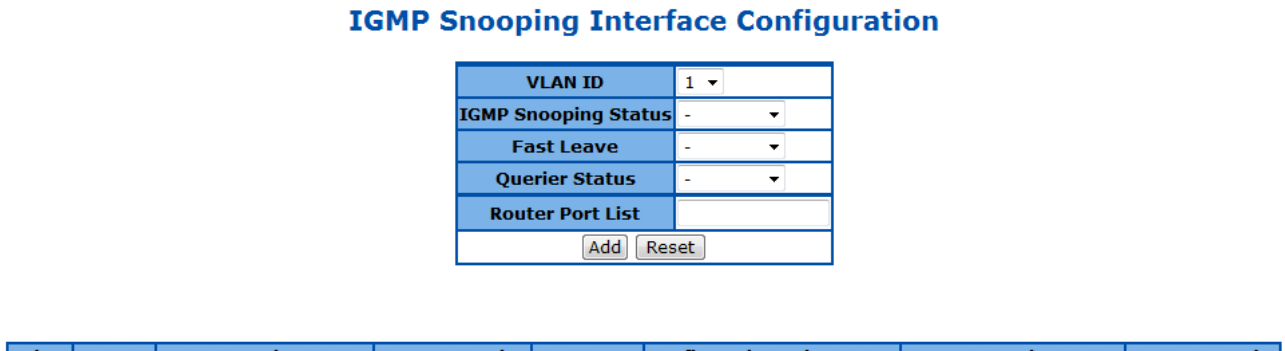


Figure 61 – Layer2 Management > IGMP Snooping > Interface Configuration

Parameter	Description
VLAN ID	Specify which VLAN to add to the IGMP snooping interface list below.
IGMP Snooping Status	Enable or disable the IGMP Snooping on this VLAN.
Fast Leave	Enable or disable the fast leave function on this VLAN.
Querier Status	Enable or disable the IGMP querier function on this VLAN.
Router Port List	Specify the IGMP router ports of this VLAN.

Click **Add** to add a new VLAN to the list, **Reset** to clear the value.

Parameter	Description
Select	Select which VLAN to apply the configuration changes.
VLAN ID	VLAN ID of this VLAN.
IGMP Snooping Status	Enable or disable the IGMP Snooping on this VLAN.
Current Version	Specify the IGMP version of this VLAN.
Fast Leave	Enable or disable the fast leave function on this VLAN.
Querier Status	Enable or disable the IGMP querier function on this VLAN.
Router Port List	Specify the IGMP router ports of this VLAN.

Click **Apply** to submit the changes the IGMP snooping setting of an existing VLAN, **Delete** to delete one VLAN from the list.

IGMP Snooping VLAN Router Ports

This page is to display the static and dynamic learned IGMP router ports of each VLAN.

Figure 62 – Layer2 Management > IGMP Snooping > Router Ports

MAC Based Multicast Forwarding Table

This page is to display the IGMP group MAC address was learned.

Figure 63 – Layer2 Management > IGMP Snooping > Group Information

Static MAC Entries

Static MAC Address Configuration

This page is to create or configure static unicast MAC address in the L2 forwarding database.

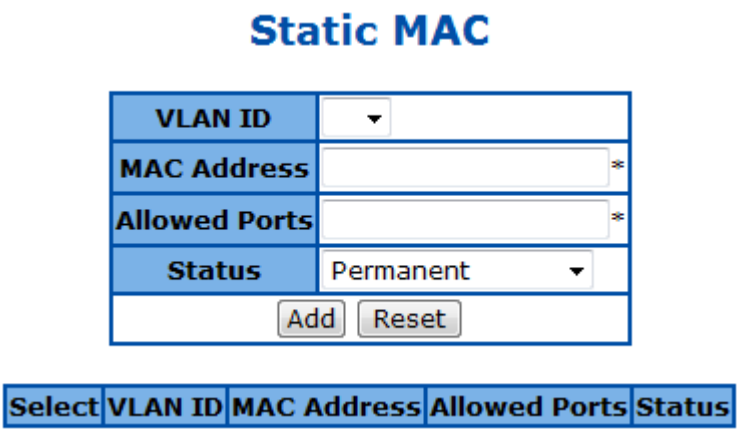


Figure 64 – Layer2 Management > Static MAC Entries > Unicast Entries

Parameter	Description
VLAN ID	Specify the VLAN ID of the new MAC address entry.
MAC Address	Specify the MAC address if this new entry.
Allowed Port	Specify the port allowed to forward the MAC address.
Status	Specify the attribute of this static MAC. The options are: **Permanent** - The static multicast will keep alive. **DeleteOnReset** - The static multicast will be deleted after switch reset. **DeleteOnTimeout** - The static multicast will be deleted when aging time out. Default is Permanent.

Click **Add** to create a new static MAC, **Reset** to clear the value.

Parameter	Description
Select	Select which MAC address to apply the configuration changes.
VLAN ID	VLAN ID of this MAC address belongs to.
MAC Address	The MAC address.
Allowed Port	Specify the port allowed to forward the MAC address.
Status	Specify the attribute of this static MAC. The options are: **Permanent** - The static multicast will keep alive. **DeleteOnReset** - The static multicast will be deleted after switch reset. **DeleteOnTimeout** - The static multicast will be deleted when aging time out. Default is Permanent.

Click **Apply** to submit the changes the static MAC, **Delete** to delete it from the FDB.

Static Multicast Address Configuration

This page is to create/configure a static multicast MAC address in the L2 forwarding database.

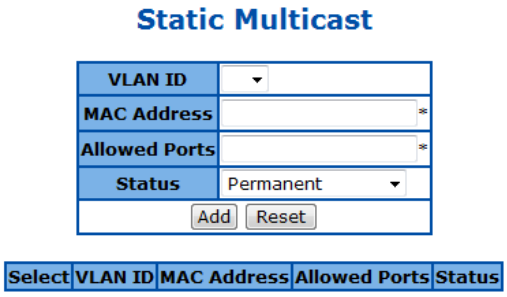


Figure 65 – Layer2 Management > Static MAC Entries > Multicast Entries

Parameter	Description
VLAN ID	Specify the VLAN ID of the new MAC address entry.
MAC Address	Specify the MAC address if this new entry.
Allowed Ports	Specify the port allowed to forward the MAC address.
Status	Specify the attribute of this static MAC. The options are: **Permanent** - The static multicast will keep alive. **DeleteOnReset** - The static multicast will be deleted after switch reset. **DeleteOnTimeout** - The static multicast will be deleted when aging time out. Default is Permanent.

Click **Add** to create a new static MAC, **Reset** to clear the value.

Parameter	Description
Select	Select which MAC address to apply the configuration changes.
VLAN ID	VLAN ID of this MAC address belongs to.
MAC Address	The MAC address.
Allowed Ports	Specify the port allowed to forward the MAC address.
Status	Specify the attribute of this static MAC. The options are: **Permanent** - The static multicast will keep alive. **DeleteOnReset** - The static multicast will be deleted after switch reset. **DeleteOnTimeout** - The static multicast will be deleted when aging time out. Default is Permanent.

Click **Apply** to submit the changes the static MAC, **Delete** to delete it from the FDB.

Port Security Settings

This page is to configure the port security function for each port.

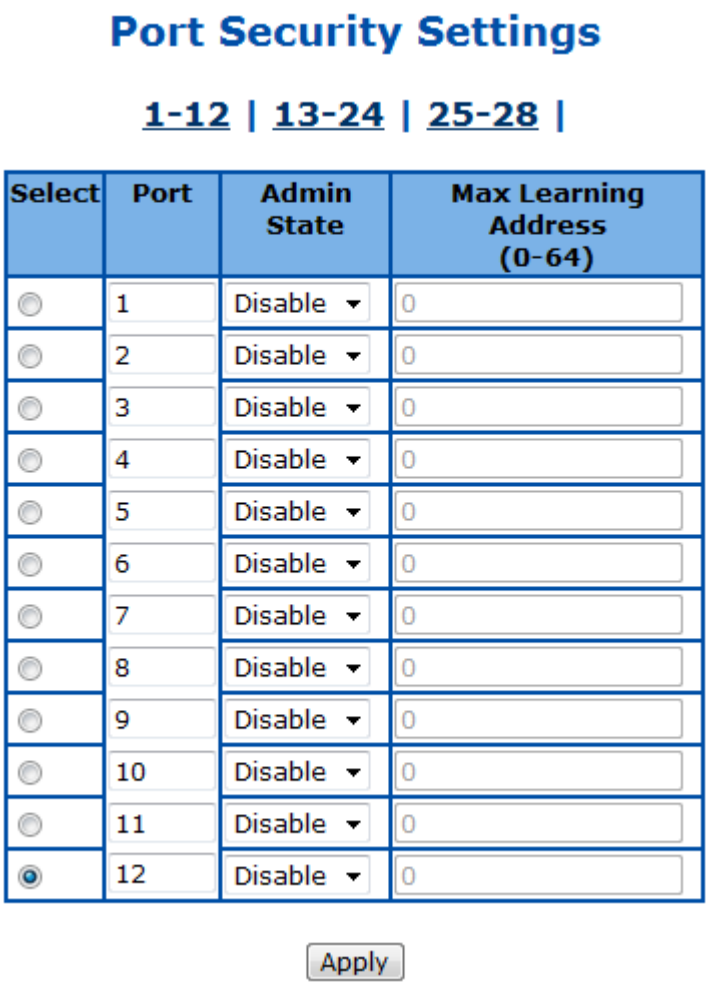


Figure 66 – Layer2 Management > Static MAC Entries > Port Security Settings

Parameter	Description
Select	Select a port to apply the configuration changes.
Port	Port ID.
Admin State	To enable or disable the port security function. Default is disable.
Max Learning Address (0-64)	Specify the maximum MAC address number of this port.

Click **Apply** to submit the changes.
Click **1-12, 13-24, 25-28** to configure port security function for corresponding ports.

Chapter 7
Configuring ACL Functions

ACL Function List

- **MAC ACL Configuration**
- **IP Standard ACL Configuration**
- **IP Extended ACL Configuration**
- **Classmap Settings**
- **Policymap Settings**

MAC ACL Configuration

This page is to create/configure a rule to MAC Access Control List.

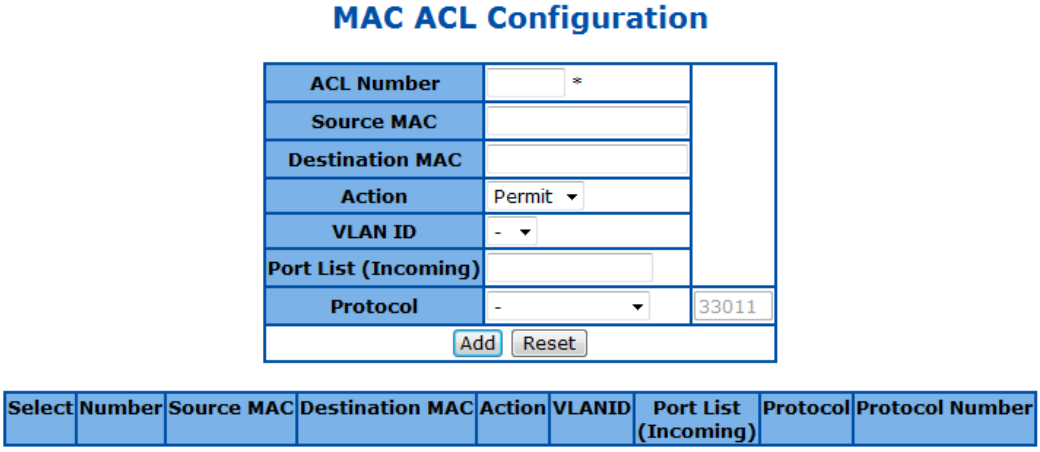


Figure 67 – ACL > MAC ACL

Parameter	Description
ACL Number	Specify the ACL ID of this rule. The possible ID of MAC ACL is 1-65535.
Source MAC	Matching packets with a specific source MAC address.
Destination MAC	Matching packets with a specific destination MAC address.
Action	Specify the action for packet matched. Select **Permit** to process the packets, **Deny** to discard them.
VLAN ID	Matching packets with a specific VLAN ID.
Port List (Incoming)	Specify the ports to apply this ACL rule.
Protocol	Matching packet with specific protocol (Ether type). The options are: **Protocol** — **Ether Type** **aarp** — 0x80F3(33011). **amber** — 0x6008(24584). **dec-spanning** — 0x8138(33080). **decnet**-iv — 0x6003(24579). **diagnostic** — 0x6005(24581). **dsm** — 0x8309(32825). **etype-6000** — 0x6000(24576). **etype-8042** — 0x8042(32834). **lat** — 0x6004(24580).

	lavc-sca	0x6007(24583).
	mop-console	0x6002(24578).
	mop-dump	0x6001(24577).
	msdos	0x8041(32833).
	mumps	0x6009(24585).
	netbios	0x8040(32832).
	vines-echo	0x0BAF(2991).
	vines-ip	0x0BAD(2989).
	xns-id	0x0807(2055).
	others	Insert a custom Ether type (0-65535) to the right column.

Click **Add** to create a new ACL rule, **Reset** to clear the value.

Parameter	Description
Select	Select an ACL rule to apply the configuration changes.
ACL Number	Specify the ACL ID of this rule.
Source MAC	Matching packets with a specific source MAC address.
Destination MAC	Matching packets with a specific destination MAC address.
Action	Specify the action for packet matched. Select **Permit** to process the packets, **Deny** to discard them.
VLAN ID	Matching packets with a specific VLAN ID.
Port List (Incoming)	Specify the ports to apply this ACL rule.
Protocol	Matching packet with specific protocol (Ether type). The options are: **Protocol** **Ether Type** **aarp** 0x80F3(33011). **amber** 0x6008(24584). **dec-spanning** 0x8138(33080). **decnet**-iv 0x6003(24579). **diagnostic** 0x6005(24581). **dsm** 0x8309(32825). **etype-6000** 0x6000(24576). **etype-8042** 0x8042(32834). **lat** 0x6004(24580). **lavc-sca** 0x6007(24583). **mop-console** 0x6002(24578). **mop-dump** 0x6001(24577). **msdos** 0x8041(32833). **mumps** 0x6009(24585). **netbios** 0x8040(32832). **vines-echo** 0x0BAF(2991). **vines-ip** 0x0BAD(2989). **xns-id** 0x0807(2055). **others**
Protocol Number	Specify the Ether type for the protocol.

Click **Apply** to submit the changes to the ACL rule, **Delete** to delete it.

IP Standard ACL Configuration

This page is to create/configure a rule to IP standard Access Control List.

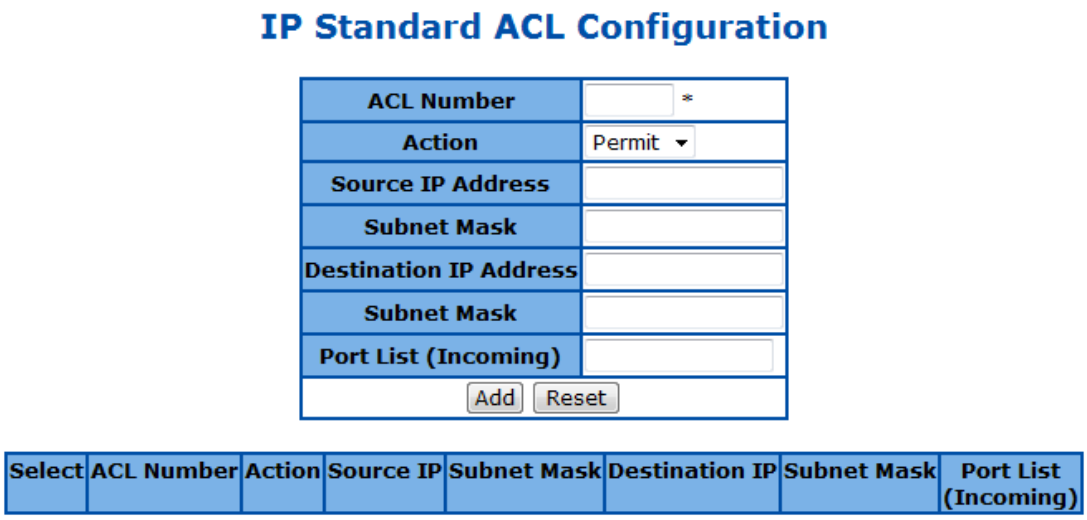


Figure 68 – ACL > IP Standard ACL

Parameter	Description
ACL Number	Specify the ACL ID of this rule. The possible ID of IP Standard ACL is 1-1000.
Action	Specify the action for packet matched. Select **Permit** to process the packets, **Deny** to discard them.
Source IP Address	Matching packet with a specific source IP address.
Subnet Mask	Matching packet with a range of source IP address. For example 172.17.5.1 with mask 255.255.255.0 means 172.15.5.0~255.
Destination IP Address	Matching packet with a specific destination IP address.
Subnet Mask	Matching packet with a range of destination IP address. For example 172.17.5.1 with mask 255.255.255.0 means 172.15.5.0~255.
Port List (Incoming)	Specify the ports to apply this ACL rule.

Click **Add** to create a new ACL rule, **Reset** to clear the value.

Parameter	Description
Select	Select an ACL rule to apply the configuration changes.
ACL Number	Specify the ACL ID of this rule.
Action	Specify the action for packet matched. Select **Permit** to process the packets, **Deny** to discard them.
Source IP Address	Matching packet with a specific source IP address.
Subnet Mask	Matching packet with a range of source IP address. For example 172.17.5.1 with mask 255.255.255.0 means 172.15.5.0~255.
Destination IP Address	Matching packet with a specific destination IP address.
Subnet Mask	Matching packet with a range of destination IP address. For example 172.17.5.1 with mask 255.255.255.0 means 172.15.5.0~255.
Port List (Incoming)	Specify the ports to apply this ACL rule.

Click **Apply** to submit the changes to the ACL rule, **Delete** to delete it.

IP Extended ACL Configuration

This page is to create/configure a rule to IP Extended Access Control List.

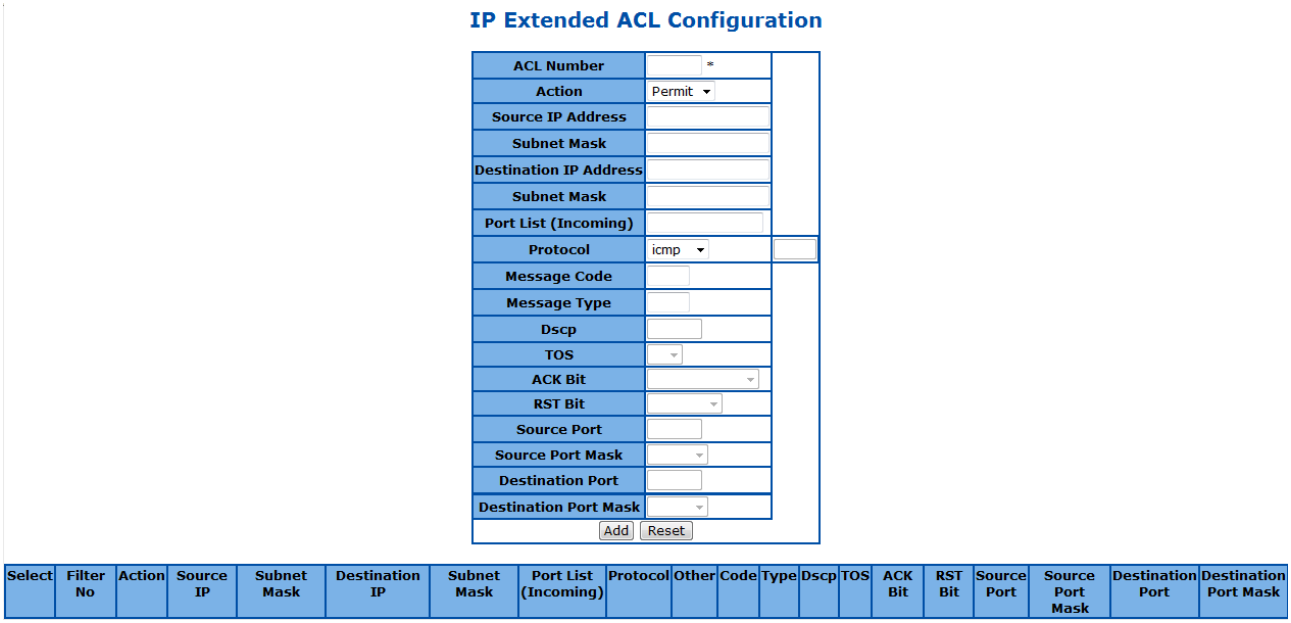


Figure 69 – ACL > IP Extended ACL

Parameter	Description
ACL Number	Specify the ACL ID of this rule. The possible ID of IP Standard ACL is 1001-65535.
Action	Specify the action for packet matched. Select **Permit** to process the packets, **Deny** to discard them.
Source IP Address	Matching packet with a specific source IP address.
Subnet Mask	Matching packet with a range of source IP address. For example 172.17.5.1 with mask 255.255.255.0 means 172.15.5.0~255.
Destination IP Address	Matching packet with a specific destination IP address.
Subnet Mask	Matching packet with a range of destination IP address. For example 172.17.5.1 with mask 255.255.255.0 means 172.15.5.0~255.
Port List (Incoming)	Specify the ports to apply this ACL rule.
Protocol	Matching the L4 protocol type of the packet. The options are: **icmp**, **ip**, **tcp**, **udp**, **ospf**, **pim** and **other**. When selecting others, insert the protocol ID in the right column.
Message Code	Matching ICMP packets with specific message type. The possible code is 0-255.
Message Type	Matching ICMP packets with specific message code. The possible type is 0-255.
Dscp	Matching packets with specific DSCP type. The possible value is 0-63.
TOS	Matching packets with specific ToS value. The possible value is 0-7
ACK Bit	Matching packets with a specific TCP acknowledge flag. The options are: **Establish** – TCP ACK packet. **Not Establish** - TCP ACK-not packet. **Any** - Any kind of TCP acknowledge packet.
RST Bit	Matching packets with a specific TCP reset flag. The options are: **Set** - TSP reset packet. **Not Set** - TCP reset-not packet. **Any** - Any kind of TCP reset packet.
Source Port	Matching packets with a specific L4 source port.
Source Port Mask	Matching packet with a range of source port. For example source port 23 with mask FFFE means 22~23. The mask options are: **8000**, **C000**, **E000**, **F000**, **F800**, **FC00**, **FE00**, **FF00**, **FF80**, **FFC0**, **FFE0**, **FFF0**, **FFF8**, **FFFC**, **FFFE**, **FFFF**.
Destination Port	Matching packets with a specific L4 destination port.

Destination Port Mask	Matching packet with a range of destination port. For example source port 23 with mask FFFE means 22~23. The mask options are: **8000**, **C000**, **E000**, **F000**, **F800**, **FC00**, **FE00**, **FF00**, **FF80**, **FFC0**, **FFE0**, **FFF0**, **FFF8**, **FFFC**, **FFFE**, **FFFF**.

Click **Add** to create a new ACL rule, **Reset** to clear the value.

Parameter	Description
Select	Select an ACL rule to apply the configuration changes.
ACL Number	Specify the ACL ID of this rule.
Action	Specify the action for packet matched. Select **Permit** to process the packets, **Deny** to discard them.
Source IP Address	Matching packet with a specific source IP address.
Subnet Mask	Matching packet with a range of source IP address. For example 172.17.5.1 with mask 255.255.255.0 means 172.15.5.0~255.
Destination IP Address	Matching packet with a specific destination IP address.
Subnet Mask	Matching packet with a range of destination IP address. For example 172.17.5.1 with mask 255.255.255.0 means 172.15.5.0~255.
Port List (Incoming)	Specify the ports to apply this ACL rule.
Protocol	Matching the L4 protocol type of the packet. The options are: **icmp**, **ip**, **tcp**, **udp**, **ospf**, **pim** and **other**. When selecting others, insert the protocol ID in the right column.
Message Code	Matching ICMP packets with specific message type. The possible code is 0-255.
Message Type	Matching ICMP packets with specific message code. The possible type is 0-255.
Dscp	Matching packets with specific DSCP type. The possible value is 0-63.
TOS	Matching packets with specific ToS value. The possible value is 0-7
ACK Bit	Matching packets with a specific TCP acknowledge flag. The options are: **Establish** – TCK ACK packet. **Not Establish** - TCP ACK-not packet. **Any** - Any kind of TCP acknowledge packet.
RST Bit	Matching packets with a specific TCP reset flag. The options are: **Set** - TSP reset packet. **Not Set** - TCP reset-not packet. **Any** - Any kind of TCP reset packet.
Source Port	Matching packets with a specific L4 source port.
Source Port Mask	Matching packet with a range of source port. For example source port 23 with mask FFFE means 22~23. The mask options are: **8000**, **C000**, **E000**, **F000**, **F800**, **FC00**, **FE00**, **FF00**, **FF80**, **FFC0**, **FFE0**, **FFF0**, **FFF8**, **FFFC**, **FFFE**, **FFFF**.
Destination Port	Matching packets with a specific L4 destination port.
Destination Port Mask	Matching packet with a range of destination port. For example source port 23 with mask FFFE means 22~23. The mask options are: **8000**, **C000**, **E000**, **F000**, **F800**, **FC00**, **FE00**, **FF00**, **FF80**, **FFC0**, **FFE0**, **FFF0**, **FFF8**, **FFFC**, **FFFE**, **FFFF**.

Click **Apply** to submit the changes to the ACL rule, **Delete** to delete it.

Classmap Settings

This page is to create/configure a Classmap.

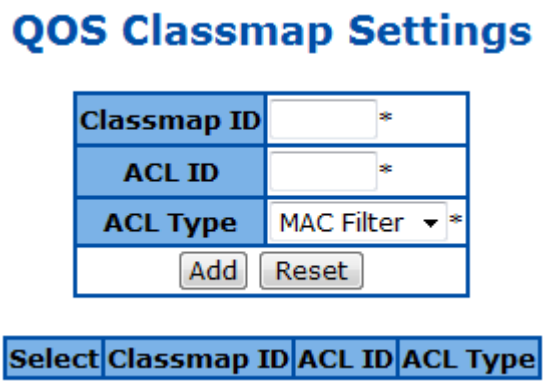


Figure 70 – ACL > Classmap

Parameter	Description
Classmap ID	Specify the classmap ID. The possible value is 1-65535.
ACL ID	Specify the ACL rule ID to bind.
ACL Type	Specify the type of the ACL rule.

Click **Add** to create a new classmap, **Reset** to clear the value.

Parameter	Description
Select	Select a classmap to delete
Classmap ID	The classmap ID.
ACL ID	The ID of binding ACL rule.
ACL Type	The type of binding ACL rule.

Click **Delete** to delete selected classmap.

Policymap Settings

This page is to create/configure a policymap.

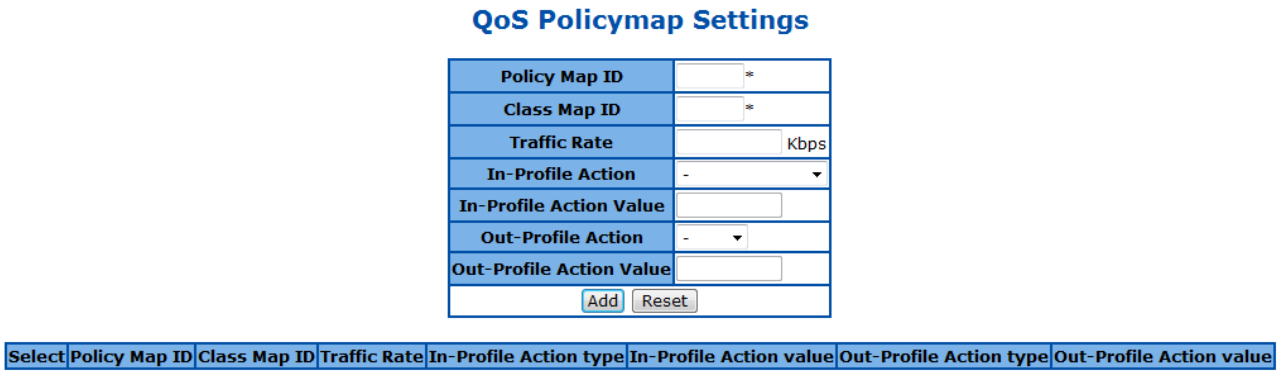


Figure 71 – ACL > Pokicymap

Parameter	Description
Policy Map ID	Specify the policymap ID. The possible value is 1-65535.
Classmap ID	Specify which classmap to bind.
Traffic Rate	Set the traffic rate threshold in Kbps for the class map.
In-Profile Action	Specify the action to packets do not exceed the rate threshold. The options are:

	Policed-DSCP - Assign a new DSCP value to the packets. **Policed-Priority** - Assign a new 802.1p priority to the packets.
In-Profile Action Value	Specify the new value of above. When rewriting DSCP tag, the possible value is 0-63; when rewriting the 802.1p priority, the possible value is 0-7.
Out-Profile Action	Specify the action to packets exceed the rate threshold. The options are: **Drop** - Drop the packets. **Policy DSCP** - Assign a new DSCP value to the packets.
Out-Profile Action Value	Specify the new value of DSCP tag. The possible value is 0-63.

Click **Add** to create a new policymap, **Reset** to clear the value.

Parameter	Description
Policy Map ID	Specify the policymap ID. The possible value is 1-65535.
Classmap ID	Specify which classmap to bind.
Traffic Rate	Set the traffic rate threshold in Kbps for the class map.
In-Profile Action	Specify the action to packets do not exceed the rate threshold. The options are: **Policed-DSCP** - Assign a new DSCP value to the packets. **Policed-Priority** - Assign a new 802.1p priority to the packets.
In-Profile Action Value	Specify the new value of above. When rewriting DSCP tag, the possible value is 0-63; when rewriting the 802.1p priority, the possible value is 0-7.
Out-Profile Action	Specify the action to packets exceed the rate threshold. The options are: **Drop** - Drop the packets. **Policy DSCP** - Assign a new DSCP value to the packets.
Out-Profile Action Value	Specify the new value of DSCP tag. The possible value is 0-63.

Click **Apply** to submit the changes to the policymap, **Delete** to delete it.

Chapter 8
Configuring QoS Functions

QoS Function List

- **Rate Limiting**
- **Storm Control Settings**
- **802.1p Queue Mapping**
- **802.1p Port Priority**
- **DSCP Queue Mapping**
- **Egress Queue Scheduling Settings**

Rate Limiting

This page is to configure the rate limiting function on each port.

Rate Limiting

1-12 | 13-24 | 25-28 |

Select	Port	Ingress RateLimit (0,64~1000000 Kbps)	Egress RateLimit (0,64~1000000 Kbps)
○	1	0	0
○	2	0	0
○	3	0	0
○	4	0	0
○	5	0	0
○	6	0	0
○	7	0	0
○	8	0	0
○	9	0	0
○	10	0	0
○	11	0	0
◉	12	0	0

Note 1: It means Ingress / Egress rate limit disable if Ingress / Egress RateLimit is 0.
Note 2: The multiple of 1850 Kbits/sec will be set automatically because the resolution of Giga-port Egress RateLimit is 1850 Kbits/sec.
Note 3: In fastethernet ports, the Ingress / Egress RateLimit support to 100000 Kbps.

Apply

Figure 72 – QoS > Rate Limiting

Parameter	Description
Select	Select a port to configure rate limiting function.
Port	Port ID.
Ingress RateLimit (0,64~1000000 Kbps)	Specify the traffic Kbit per second is allowed to be transmitted for an ingress port. 0 means no limit.
Egress RateLimit (0,64~1000000 Kbps)	Specify the traffic Kbit per second is allowed to be transmitted for an egress port. 0 means no limit.

Click **Apply** to submit the changes.
Click **1-12, 13-24, 25-28** to configure rate limiting for corresponding ports.

Storm Control Settings

This page is to configure the storm control function of the device.

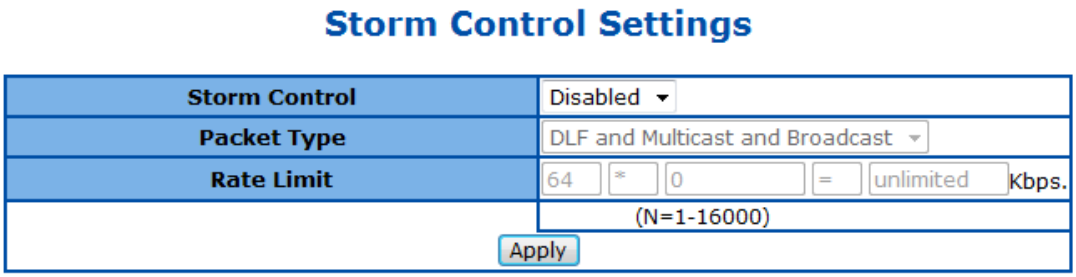


Figure 73 – QoS > Storm Global Settings

Parameter	Description
System Control	To activate or shutdown storm control function of the Switch. Select **Enable** to activate link aggregation function, **Disabled** to shutdown it. Default is Start.
Packet Type	Specify which kind of packets to be controlled. The options are: **Broadcast only** - Control broadcast packets only. **Multicast and Broadcast** - Control both multicast and broadcast packets. **DLF and Multicast and Broadcast** - Control Destination Lookup Failed unicast, multicast and broadcast packets.
Rate Limit	Specify the maximum packet rate is allowed per second.

802.1p Queue Mapping

This page is to configure the 802.1p priority and queue mapping.

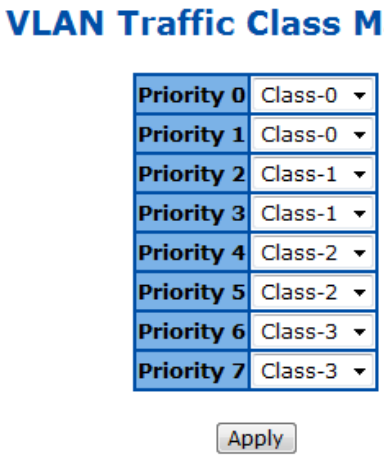


Figure 74 – QoS > 802.1p

Parameter	Description
Priority 0~7	Specify which switch queue to map. The options are **Class-0**, **Class-1**, **Class-2** and **Class-3**.

Click **Apply** to submit the changes.

802.1p Port Priority

This page is to configure the 802.1p priority for untagged packets receive from each port.

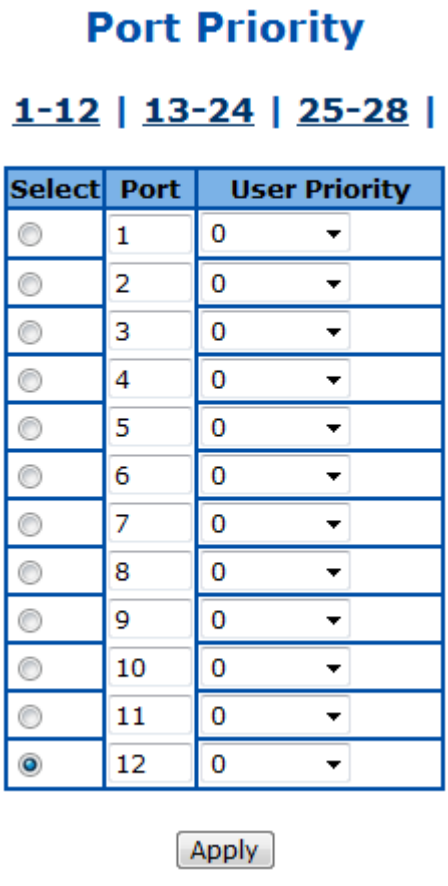


Figure 75 – QoS > Port Priority

Parameter	Description
Select	Select a port to submit the configuration changes.
Port	Port ID.
User Priority	Specify 802.1p priority of untagged packets.

Click **Apply** to submit the changes.
Click **1-12, 13-24, 25-28** to configure port priority for corresponding ports.

DSCP Queue Mapping

This page is to enable/configure the DSCP and queue mapping.

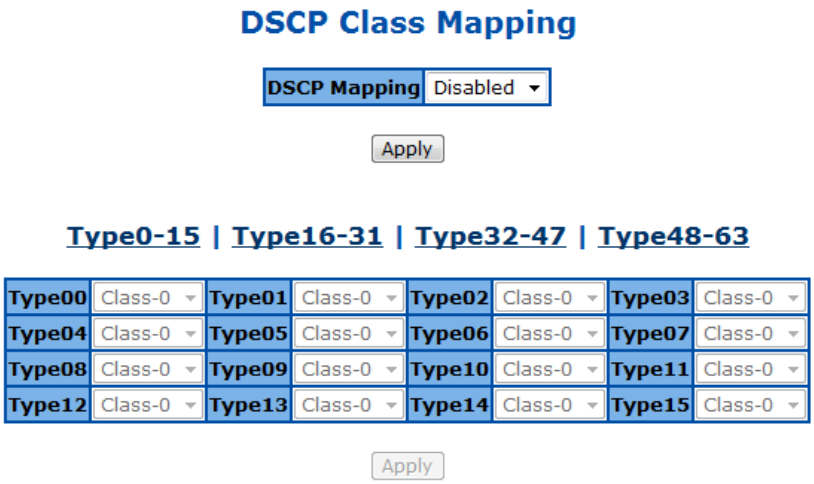


Figure 76 – QoS > DSCP

Parameter	Description
DSCP Mapping	To enable the DSCP queue mapping. When disabled, Switch will map queue with 802.1p priority.

Click **Apply** to submit the changes.

Parameter	Description
Type00~63	Specify which switch queue to map. The options are **Class-0**, **Class-1**, **Class-2** and **Class-3**.

Click **Type0-15, 16-31, 32-47, 48-63** to configure queue mapping for corresponding DSCP levels.
Click **Apply** to submit the changes.

Egress Queue Scheduling Settings

This page is to configure the scheduling algorithm for switch queues.

Figure 77 – QoS > Egress Algorithm

Parameter	Description
Scheduling Algorithm	Select the algorithm of queue scheduling. The options are: **Strict Priority** - The traffic in highest queue always process first. **Weighted RoundRobin** - Using weighted round-robin algorithm to handle packets in priority queues. Default is Strict Priority.

Click **Apply** to submit the changes.

Chapter 9
Configuring RMON Functions

RMON Function List

- **RMON Basic Settings**
- **RMON Statistics Configuration**
- **RMON History Configuration**
- **RMON Alarms Configuration**
- **RMON Events Configuration**

RMON Basic Settings

This page is to enable or disable RMON function

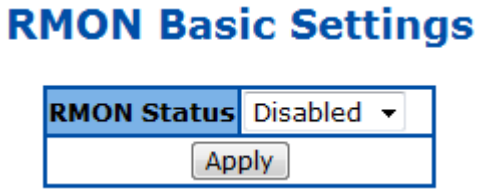


Figure 78 – RMON > Global Settings

Parameter	Description
RMON Status	To enable or disable RMON function. Default is Disabled.

Click **Apply** to submit the changes.

RMON Statistics Configuration

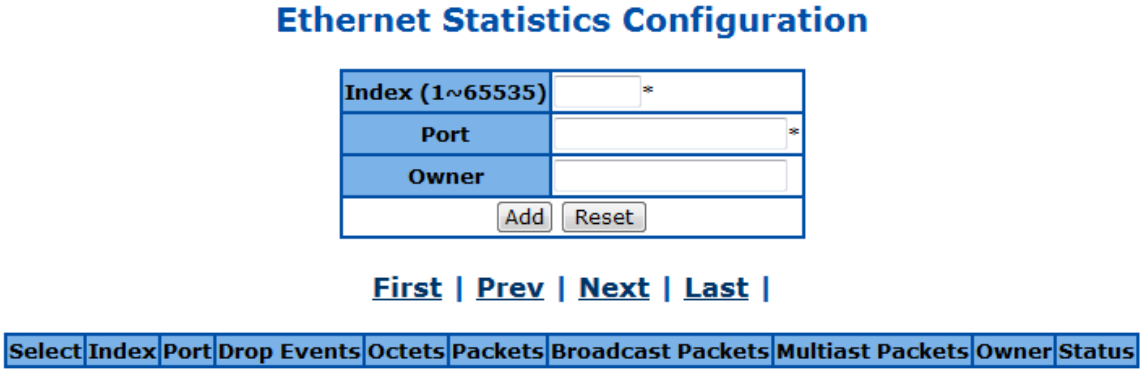


Figure 79 – RMON > Statistics

Parameter	Description
Index (1~65535)	Specify the index of the RMON statistics collection.
Port	Specify which port to enable the RMON statistics collection.
Owner	Specify the owner of the statistics entry.

Click **Add** to create a new statistics entry, **Reset** to clear the value.

Parameter	Description
Select	Select a RMON statistics entry to apply the
Index	The index of the RMON statistics collection.
Port	The port of the RMON statistics collection.
Drop Events	The number of events was dropped due to lack of resources.
Octets	The total number of octets received from this port.
Packets	The total number of packets received from this port.
Broadcast Packets	The total number of broadcast packets received from this port.
Multicast Packets	The total number of multicast packets received from this port.
Owner	Specify the owner of the statistics.
Status	Specify the status of this statistics entry. The options are: **Valid** - The statistics entry is valid. **Under Creation** - **Invalid** - The statistics entry is invalid and will be deleted.

Click **Apply** to submit the changes.

RMON History Configuration

This page is to configure the RMON history settings on ports.

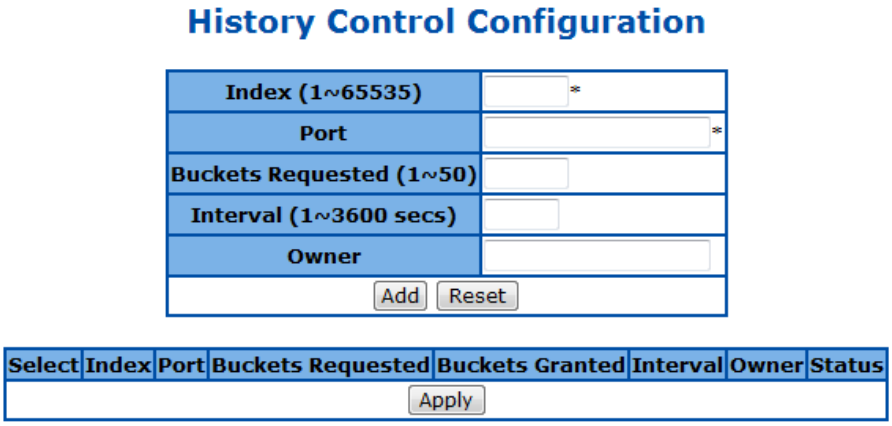


Figure 80 – RMON > History

Parameter	Description
Index (1~65535)	Specify the index of the RMON history collection.
Port	Specify which port to enable the RMON history collection.
Buckets Requested (1~50)	Specify the maximum number of RMON history collection.
Interval (1~3600 secs)	Specify the time interval for the history collection.
Owner	Specify the owner of the history entry.

Click **Add** to create a new history entry, **Reset** to clear the value.

Parameter	Description
Select	Select a RMON history entry to apply the
Index	The index of the RMON history collection.
Port	The port of the RMON history collection.
Buckets Requested	Specify the maximum number of RMON history collection.
Buckets Granted	The number of bucket granted for collecting the RMON history.

Interval	Specify the time interval for the history collection.
Owner	Specify the owner of the history entry.
Status	Specify the status of this history entry. The options are: **Valid** - The history entry is valid. **Under Creation** - **Invalid** - The history entry is invalid and will be deleted.

Click **Apply** to submit the changes.

RMON Alarms Configuration

To set a RMON alarm to a MIB object.

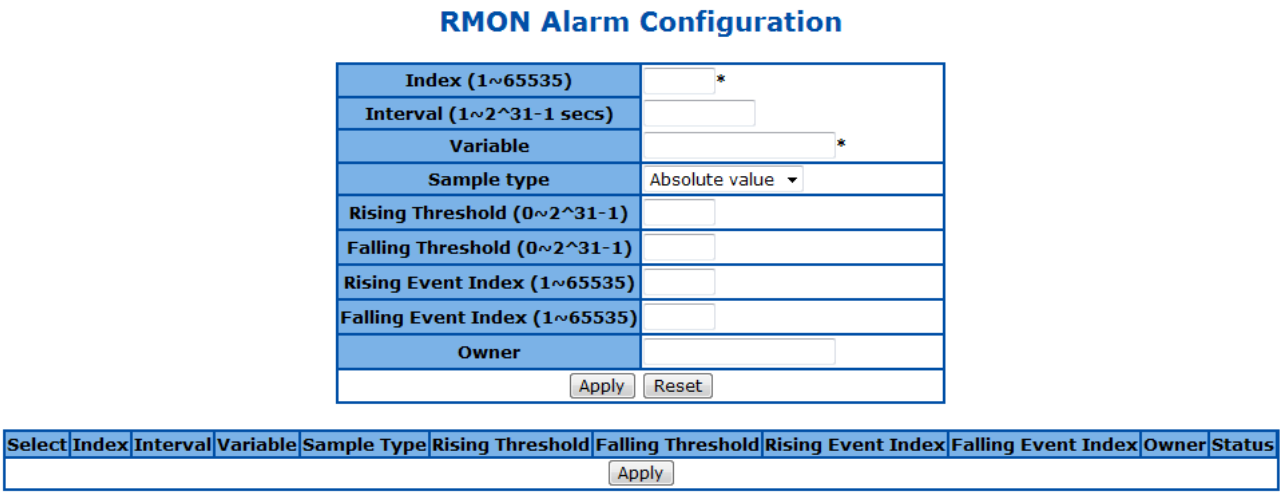


Figure 81 – RMON > Alarms

Parameter	Description
Index (1~65535)	Specify the index of the RMON alarm.
Interval (1~2^31-1 secs)	The time interval in seconds that alarm monitors the MIB variable.
Variable	The MIB OID to set alarm.
Sample type	The type of the alarm sampling. The options are: **Absolute value** - To test the MIB variable directly. **Delta value** - To test the change between samples of a MIB variable.
Rising Threshold (0~2^31-1)	The threshold value to trigger alarm when the number of sample exceeds.
Falling Threshold (0~2^31-1)	The threshold value to reset alarm when the number of sample exceeds.
Rising Event Index (1~65535)	The number of event to trigger when rising threshold is exceeded.
Falling Event Index (1~65535)	The number of event to trigger when falling threshold is exceeded.
Owner	Specify the owner of the alarm entry.

Click **Add** to create a new RMON alarm, **Reset** to clear the value.

Parameter	Description
Select	Select a RMON alarm entry to apply the configuration changes.
Index	Specify the index of the RMON alarm.

Interval	The time interval in seconds that alarm monitors the MIB variable.
Variable	The MIB OID of this alarm entry.
Sample type	The type of the alarm sampling. The options are: **Absolute value** - To test the MIB variable directly. **Delta value** - To test the change between samples of a MIB variable.
Rising Threshold	The threshold value to trigger alarm when the number of sample exceeds.
Falling Threshold	The threshold value to reset alarm when the number of sample exceeds.
Rising Event Index	The number of event to trigger when rising threshold is exceeded.
Falling Event Index	The number of event to trigger when falling threshold is exceeded.
Owner	Specify the owner of the alarm entry.
Status	Specify the status of this alarm entry. The options are: Valid - The alarm entry is valid. Under Creation - Invalid - The alarm entry is invalid and will be deleted.

Click **Apply** to submit the changes.

RMON Events Configuration

This page is to add an event to RMON event table.

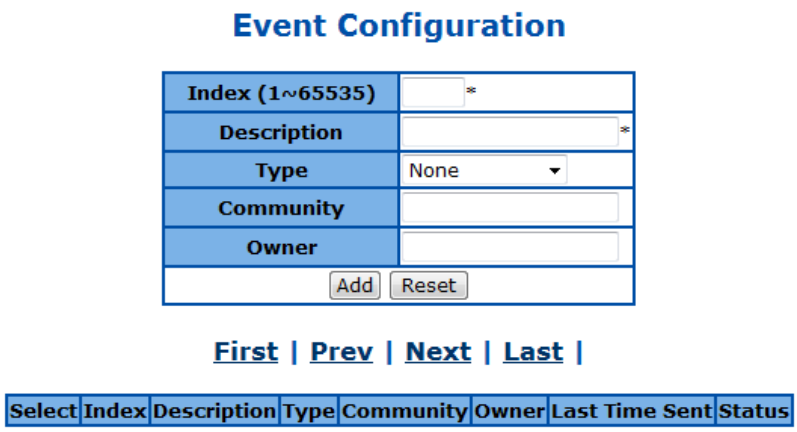


Figure 82 – RMON > Events

Parameter	Description
Index (1~65535)	Specify the index of the RMON event.
Description	Specify the description of the event.
Type	Specify the action type of the event. The options are: **Log** - Generating syslog when event is triggered. **SNMP Trap** - Generating a trap message when event is triggered. **Log and Trap** - Generating both log and trap message when event is triggered.
Community	Specify the SNMP community string used for the traps.
Owner	Specify the owner of the event entry.

Click **Add** to create a new RMON event, **Reset** to clear the value.

Parameter	Description
Index	Specify the index of the RMON event.
Description	Specify the description of the event.
Type	Specify the action type of the event. The options are: **Log** - Generating syslog when event is triggered.

	SNMP Trap - Generating a trap message when event is triggered. **Log and Trap** - Generating both log and trap message when event is triggered.
Community	Specify the SNMP community string used for the traps.
Owner	Specify the owner of the alarm entry.
Status	Specify the status of this event entry. The options are: **Valid** - The event entry is valid. **Under Creation** - **Invalid** - The events entry is invalid and will be deleted.

Click **Apply** to submit the changes.

Chapter 10
Switch Statistics

Switch Statistics List

- **Interface Statistics**
- **Ethernet Statistics**
- **VLAN Statistics**
- **MSTP**
  - MSTP Information
  - MSTP CIST Port Statistics
  - MSTP MSTI Port Statistics
- **RSTP**
  - RSTP Information
  - RSTP Port Statistics
- **LA**
  - LA Port Statistics
  - LA Neighbour Statistics Information
- **802.1X**
  - 802.1X Session Statistics
  - RADIUS Server Statistics
- **IGMP Snooping**
  - IGMP Snooping Clear Statistics
  - IGMP Snooping V1/V2 Statistics
- **IP**
  - ARP Cache
  - ICMP Statistics
- **RMON**
- **MAC Address Table**
- **SNMP**

Interface Statistics

This page is to display the traffic statistics of each port.

Interface Statistics

1-12 | 13-24 | 25-28 |

Index	MTU	Speed (Bits Per Second)	Received Octets	Received Unicast Packets	Received Nunicast Packets	Received Discards	Received Errors	Received Unknown Protocols	Transmitted Octets	Transmitted Unicast Packets	Transmitted Nunicast Packets	Transmitted Discards	Transmitted Errors
1	1522	100000000	0	0	0	0	0	0	0	0	0	0	0
2	1522	100000000	0	0	0	0	0	0	0	0	0	0	0
3	1522	100000000	0	0	0	0	0	0	0	0	0	0	0
4	1522	100000000	0	0	0	0	0	0	0	0	0	0	0
5	1522	100000000	35128600	75047	769	0	0	0	22039641	58369	49572	0	0
6	1522	100000000	0	0	0	0	0	0	0	0	0	0	0
7	1522	100000000	0	0	0	0	0	0	0	0	0	0	0
8	1522	100000000	0	0	0	0	0	0	0	0	0	0	0
9	1522	100000000	0	0	0	0	0	0	0	0	0	0	0
10	1522	100000000	0	0	0	0	0	0	0	0	0	0	0
11	1522	100000000	0	0	0	0	0	0	0	0	0	0	0
12	1522	100000000	0	0	0	0	0	0	0	0	0	0	0

Figure 83 – Statistics > Interface

Click **1-12, 13-24, 25-28** to display the Ethernet related statistics of corresponding ports.

Ethernet Statistics

This page is to display the Ethernet related statistics of each port.

Ethernet Statistics

1-12 | 13-24 | 25-28 |

Index	Alignment Errors	FCS Errors	Single Collision Frames	Multiple Collision Frames	SQE Test Errors	Deferred Transmissions	Late Collisions	Excess Collisions	Transmitted Internal MAC Errors	Carrier Sense Errors	Frame Too Long	Received Internal MAC Errors	Ether ChipSet	Symbol Errors	Duplex Status
1	0	0	0	0	1096427445	0	0	0	0	0	0	0	1	0	Half-Duplex
2	0	0	0	0	1096427445	0	0	0	0	0	0	0	1	0	Half-Duplex
3	0	0	0	0	1096427445	0	0	0	0	0	0	0	1	0	Half-Duplex
4	0	0	0	0	1096427445	0	0	0	0	0	0	0	1	0	Half-Duplex
5	0	0	0	0	1096427445	0	0	0	0	0	0	0	1	0	Full-Duplex
6	0	0	0	0	1096427445	0	0	0	0	0	0	0	1	0	Half-Duplex
7	0	0	0	0	1096427445	0	0	0	0	0	0	0	1	0	Half-Duplex
8	0	0	0	0	1096427445	0	0	0	0	0	0	0	1	0	Half-Duplex
9	0	0	0	0	1096427445	0	0	0	0	0	0	0	1	0	Half-Duplex
10	0	0	0	0	1096427445	0	0	0	0	0	0	0	1	0	Half-Duplex
11	0	0	0	0	1096427445	0	0	0	0	0	0	0	1	0	Half-Duplex
12	0	0	0	0	1096427445	0	0	0	0	0	0	0	1	0	Half-Duplex

Figure 84 – Statistics > Ethernet

Click **1-12, 13-24, 25-28** to display the Ethernet related statistics of corresponding ports.

VLAN Statistics

This page is to display current VLAN and its member port information of the Switch.

VLAN Current Database

VLAN ID	VLAN FDB ID	Member Ports	Untagged Ports	Status
1	1	1-28	1-28	Permanent

Figure 85 – Statistics > VLAN

MSTP

MSTP Information

This page is to display current MSTP settings and states of the Switch.

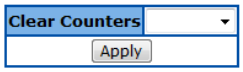
MSTP Information

Context Id	Bridge Address	CIST Root	Regional Root	CIST Root Cost	Regional Root Cost	Root Port	Hold Time	Max Age	Forward Delay	Config Digest	CIST Time Since Topology Change	Topology Changes
0	00:00:00:00:00:00	00:00:00:00:00:00:00:00	00:00:00:00:00:00:00:00	0	0	0	1	20	15		0	0

Figure 86 – Statistics > MSTP > MSTP Information

MSTP CIST Port Statistics

This page is to display the MSTP traffic statistics of ports.



MSTP CIST Port Statistics

1-12 | 13-24 | 25-28 |

Port	Received MST BPDUs	Received RST BPDUs	Received Config BPDUs	Received TCN BPDUs	Transmitted MST BPDUs	Transmitted RST BPDUs	Transmitted Config BPDUs	Transmitted TCN BPDUs	Received Invalid MST BPDUs	Received Invalid RST BPDUs	Received Invalid Config BPDUs	Received Invalid TCN BPDUs	Protocol Migration Count

Figure 87 – Statistics > MSTP > CIST Port Statistics

Parameter	Description
Clear Counters	**Update** – To display the latest statistics information. **Clear** – To reset all MSTP traffic counters.

Click **Apply** to update or clear the statistics of the Swtich.
Click **1-12, 13-24, 25-28** to display the MSTP traffic statistics of corresponding ports.

MSTP MSTI Port Statistics

This page is to display the MSTP traffic statistics of different instances in each port.

MSTP MSTI Port Statistics

Instance	Port	Designated Root	Designated Bridge	Designated Port	State	Forward Transitions	Received BPDUs	Transmitted BPDUs	Invalid Received BPDUs	Designated Cost	Role

Figure 88 – Statistics > MSTP > MSTI Port Statistics

RSTP

RSTP Information

This page is to display current RSTP setting and states of the Switch.

RSTP Information

Context Id	Protocol Specification	Time Since Topology Change	Designated Root	Root Brg Priority	Root Cost	Root Port	Max Age	Hello Time	Hold Time	Forward Delay
0	3	3	00.00.00.00.00.00.00.00	0	0	0	20	2	1	15

Figure 89 – Statistics > RSTP > RSTP Information

RSTP Port Statistics

This page is to display the RSTP traffic statistics of ports.

RSTP Port Statistics

1-12 | 13-24 | 25-28 |

Clear Counters [ ] Apply

Port	Received RST BPDUs	Received Configuration BPDUs	Received TCN	Transmitted RST BPDUs	Transmitted Configuration BPDUs	Transmitted TCN	Received Invalid RST BPDUs	Received Invalid Configuration BPDUs	Received Invalid TCN BPDUs	Protocol Migration Count	Effective Port State	EdgePort Oper Status	Link Type
1	0	0	0	0	0	0	0	0	0	0	Disable		

Figure 90 – Statistics > RSTP > Port Statistics

Parameter	Description
Clear Counters	**Update** – To display the latest statistics information. **Clear** – To reset all RSTP traffic counters.

Click **Apply** to update or clear the statistics of the Switch.
Click **1-12, 13-24, 25-28** to display the Link Aggregation neighbours information of corresponding ports.

LA

LA Port Statistics

This page is to display the traffic statistics of Link Aggregation ports.

Port Channel Port Statistics

1-12 | 13-24 | 25-28 |

Port	Received PDUs	Received Unknown PDUs	Received Illegal PDUs	Transmitted PDUs
1	0	0	0	0
2	0	0	0	0
3	0	0	0	0
4	0	0	0	0
5	0	0	0	0
6	0	0	0	0
7	0	0	0	0
8	0	0	0	0
9	0	0	0	0
10	0	0	0	0
11	0	0	0	0
12	0	0	0	0

Figure 91 – Statistics > LA > Port LACP Stats

Click **1-12, 13-24, 25-28** to display the Link Aggregation neighbours information of corresponding ports.

LA Neighbour Statistics Information

This page is to display the information of Link Aggregation neibubours.

Port Channel Neighbour Statistics Information

1-12 | 13-24 | 25-28 |

Port	Partner SystemID	Oper Key	Partner Port Priority
1	00:00:00:00:00:00	0	0
2	00:00:00:00:00:00	0	0
3	00:00:00:00:00:00	0	0
4	00:00:00:00:00:00	0	0
5	00:00:00:00:00:00	0	0
6	00:00:00:00:00:00	0	0
7	00:00:00:00:00:00	0	0
8	00:00:00:00:00:00	0	0
9	00:00:00:00:00:00	0	0
10	00:00:00:00:00:00	0	0
11	00:00:00:00:00:00	0	0
12	00:00:00:00:00:00	0	0

Figure 92 – Statistics > LA > Neighbour Stats

Click **1-12, 13-24, 25-28** to display the Link Aggregation neighbours information of corresponding ports.

802.1X

802.1X Session Statistics

This page is to display the statistics and status of current authenticated users.

802.1x Session Statistics

1-12 | 13-24 | 25-28 |

Port	Session ID	Received Frames	Transmitted Frames	Session Time (secs)	Session Terminate Cause	User Name
1	1-0	0	0	1980400	Admin Disabled	No User
2	2-0	0	0	1980400	Admin Disabled	No User
3	3-0	0	0	1980400	Admin Disabled	No User
4	4-0	0	0	1980400	Admin Disabled	No User
5	5-0	76797	109486	1980400	Admin Disabled	No User
6	6-0	0	0	1980400	Admin Disabled	No User
7	7-0	0	0	1980400	Admin Disabled	No User
8	8-0	0	0	1980400	Admin Disabled	No User
9	9-0	0	0	1980400	Admin Disabled	No User
10	10-0	0	0	1980400	Admin Disabled	No User
11	11-0	0	0	1980400	Admin Disabled	No User
12	12-0	0	0	1980400	Admin Disabled	No User

Figure 93 – Statistics > 802.1X > Session Stats

Click **1-12, 13-24, 25-28** to display the statistics for corresponding ports.

RADIUS Server Statistics

This page is to display the traffic statistics to RADIUS server.

Radius Server Statistics

Index	Radius Server Address	UDP Port Number	Round Trip Time	No of Request Packets	No of Retransmitted Packets	No of Access-Accept Packets	No of Access-Reject Packets	No of Access-Challenge Packets	No of Malformed Access Responses	No of Bad Authenticators	No of Pending Requests	No of Time Outs	No of Unknown Types

Figure 94 – Statistics > 802.1X > Radius

IGMP Snooping

IGMP Snooping Clear Statistics

This page is to reset the IGMP Snooping traffic counters.

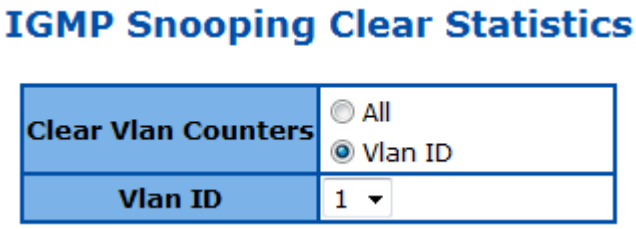


Figure 95 – Statistics > IGMP Snooping > Clear Statistics

Parameter	Description
Clear Vlan Counters	**All** – Reset all IGMP Snooping traffic counters. **VLAN ID** – Reset the IGMP Snooping traffic counter of a VLAN.
Vlan ID	Choose a VLAN to reset the IGMP Snooping Counters.

Click **Apply** to clear the counters.

IGMP Snooping V1/V2 Statistics

This page is to display the IGMP traffic statistics snooped by the Switch.

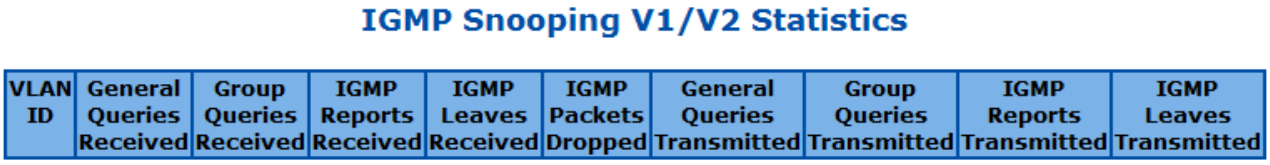


Figure 96 – Statistics > IGMP Snooping > V1/V2 Statistics

IP

ARP Cache

This page is to display the ARP information of direct connected hosts learned by the Switch.

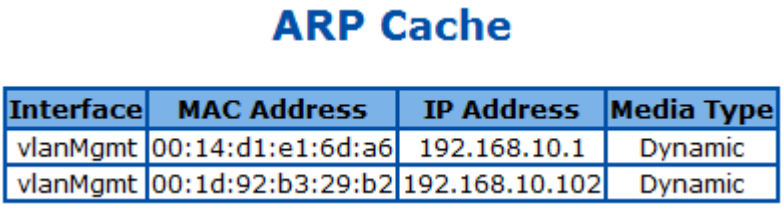
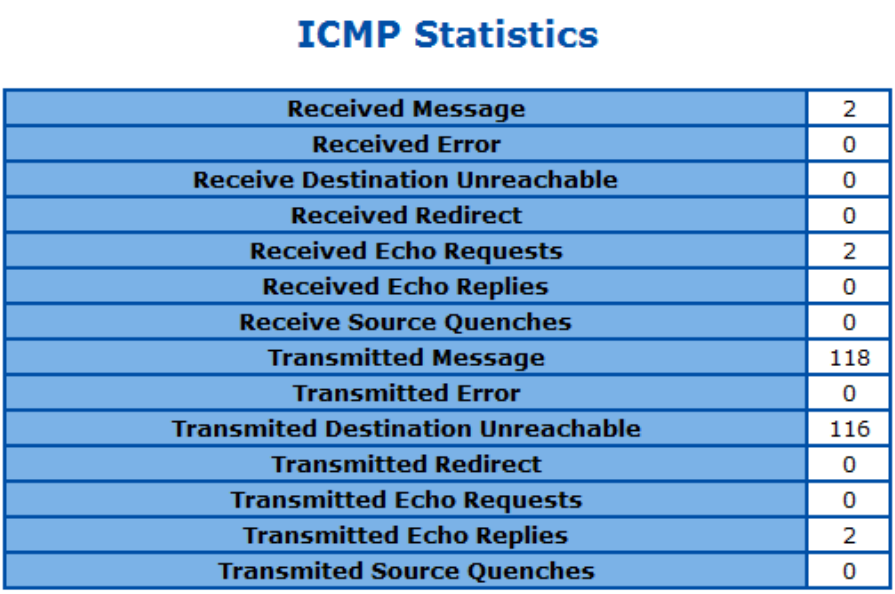


Figure 97 – Statistics > IP > ARP Cache

ICMP Statistics

This page is to display the ICMP traffic statistics of the Switch.



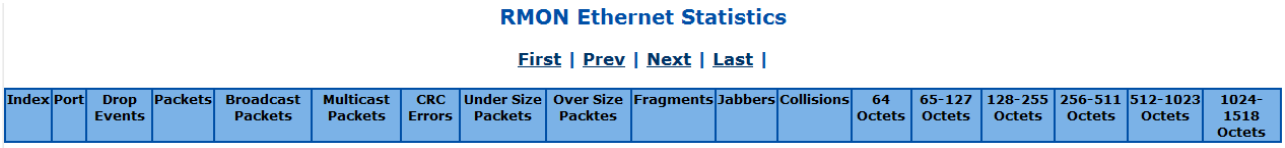
ICMP Statistics

Received Message	2
Received Error	0
Receive Destination Unreachable	0
Received Redirect	0
Received Echo Requests	2
Received Echo Replies	0
Receive Source Quenches	0
Transmitted Message	118
Transmitted Error	0
Transmited Destination Unreachable	116
Transmitted Redirect	0
Transmitted Echo Requests	0
Transmitted Echo Replies	2
Transmited Source Quenches	0

Figure 98 – Statistics > IP > ICMP Statistics

RMON

This page is to display the RMON Statistics of the Switch.



RMON Ethernet Statistics

First | Prev | Next | Last |

Index	Port	Drop Events	Packets	Broadcast Packets	Multicast Packets	CRC Errors	Under Size Packets	Over Size Packtes	Fragments	Jabbers	Collisions	64 Octets	65-127 Octets	128-255 Octets	256-511 Octets	512-1023 Octets	1024-1518 Octets

Figure 99 – Statistics > RMON

Click **First, Prev, Next, Last** to see the first, previous, next or last page of the RMON Statistics.

MAC Address Table

This page is to show the MAC addresses learned in L2 forwarding database.

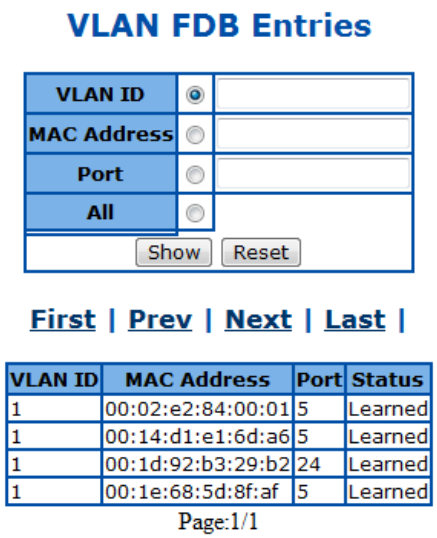


Figure 100 – Statistics > MAC Address Table

Parameter	Description
VLAN ID	Display the MAC addresses under a given VLAN.
MAC Address	Display a specific MAC address in FDB.
Port	Display the MAC addresses learned under a given port.
All	Display all MAC addresses in FDB.

Click **Show** to display the MAC addresses in FDB with given parameter and click **Reset** to reset the parameter input.
Click **First, Prev, Next, Last** to see the first, previous, next or last page of the MAC addresses list discovered.

SNMP

This page is to show the SNMP traffic statistics of the Switch.

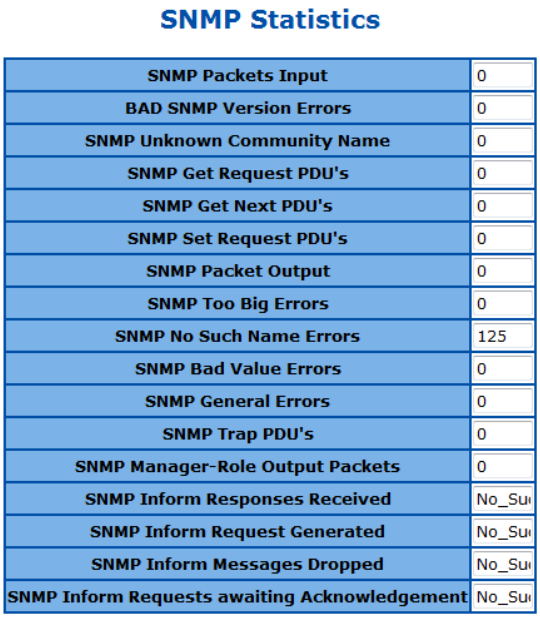


Figure 101 – Statistics > SNMP

Chapter 11
Using the Command-Line Interface

Accessing the Switch

This system may be managed out-of-band through the console port on the front panel or in-band using Telnet. The user may also choose the web-based management, accessible through a web browser. (See Web UI Reference Guide for details). Each Switch must be assigned its own IP Address, which is used for communication with an SNMP network manager or other TCP/IP application (for example BOOTP, TFTP). The Switch's default IP address is 192.168.10.1. The user can change the default Switch IP address to meet the specification of your networking address scheme

Connecting the Console Port

The Switch provides an RS-232 serial port that enables a connection to a computer or terminal for monitoring and configuring the Switch. This port is a male DB-9 connector, implemented as data communication terminal equipment (DCE) connection.

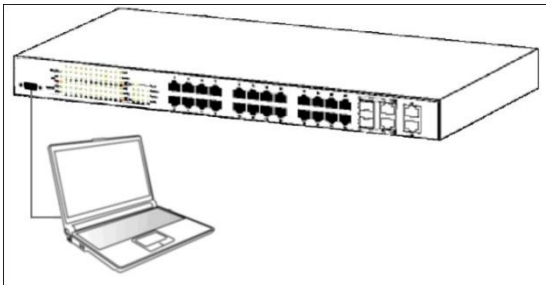


Figure 102 –Connected to an end node via console cable

To connect a terminal to the console port

1. Connect the female connector of the RS-232 cable directly to the console port on the Switch, and tighten the captive retaining screws.
2. Connect the other end of the cable to a terminal or to the serial connector of a computer running terminal emulation software. Set the terminal emulation software as follows:
3. Select the appropriate serial port (COM port 1 or COM port 2).
4. Set the data rate to 115200.
5. Set the data format to 8 data bits, 1 stop bit, and no parity.
6. Set flow control to none.
7. Under Properties, select VT100 for Emulation mode.
8. Select Terminal keys for Function, Arrow, and Ctrl keys. Ensure that you select Terminal keys (not Windows keys).
9. After you have correctly set up the terminal, plug the power cable into the power receptacle on the back of the Switch. The boot sequence appears in the terminal.
10. After the boot sequence completes, the console login screen displays.
11. If you have not logged into the command line interface (CLI) program, press the Enter key at the User name and password prompts. There is no default user name and password for the Switch. The administrator must firstly create user names and passwords. If you have previously set up user accounts, log in and continue to configure the Switch.
12. Enter the commands to complete your desired tasks. Many commands require administrator-level access privileges.
13. When you have completed your tasks, exit the session with the logout

command or close the emulator program.

Telnet Management

Users may also access the switch console through Telnet using your PC's Command Prompt. To access it from your computer, users must first ensure that a valid connection is made through the Ethernet port of the Switch and your PC, and then click **Start > Programs > Accessories > Command Prompt** on your computer. Once the console window opens, enter the command **telnet 192.168.10.1** (depending on configured IP address) and press Enter on your keyboard. You should be directed to the opening console screen for the Command Line Interface of the switch, press the Enter key at the User name and password prompts.

There are two user names and passwords by default.

	User Name	**Password**
User EXEC Mode	guest	guest123
Privileged EXEC Mode	admin	admin

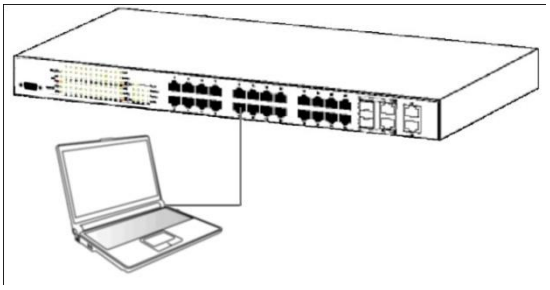


Figure 103 –Connected to an end node via Ethernet cable

Privilege Levels

TL2-E284 support 15 user privilege levels for commands, the default setting as below.

Privilege Levels	1	2~14	15
Description	User EXEC Mode	Not Defined	Privileged EXEC Mode

You may use enable command to entering different privilege level, or use disable command back to last privilege.

CLI Command Modes

To execute commands correctly, you have to enter corresponding command mode. Each command mode has its own system prompt. See following chart to understand the relationship between the command modes and the commands to enter/exit the command modes.

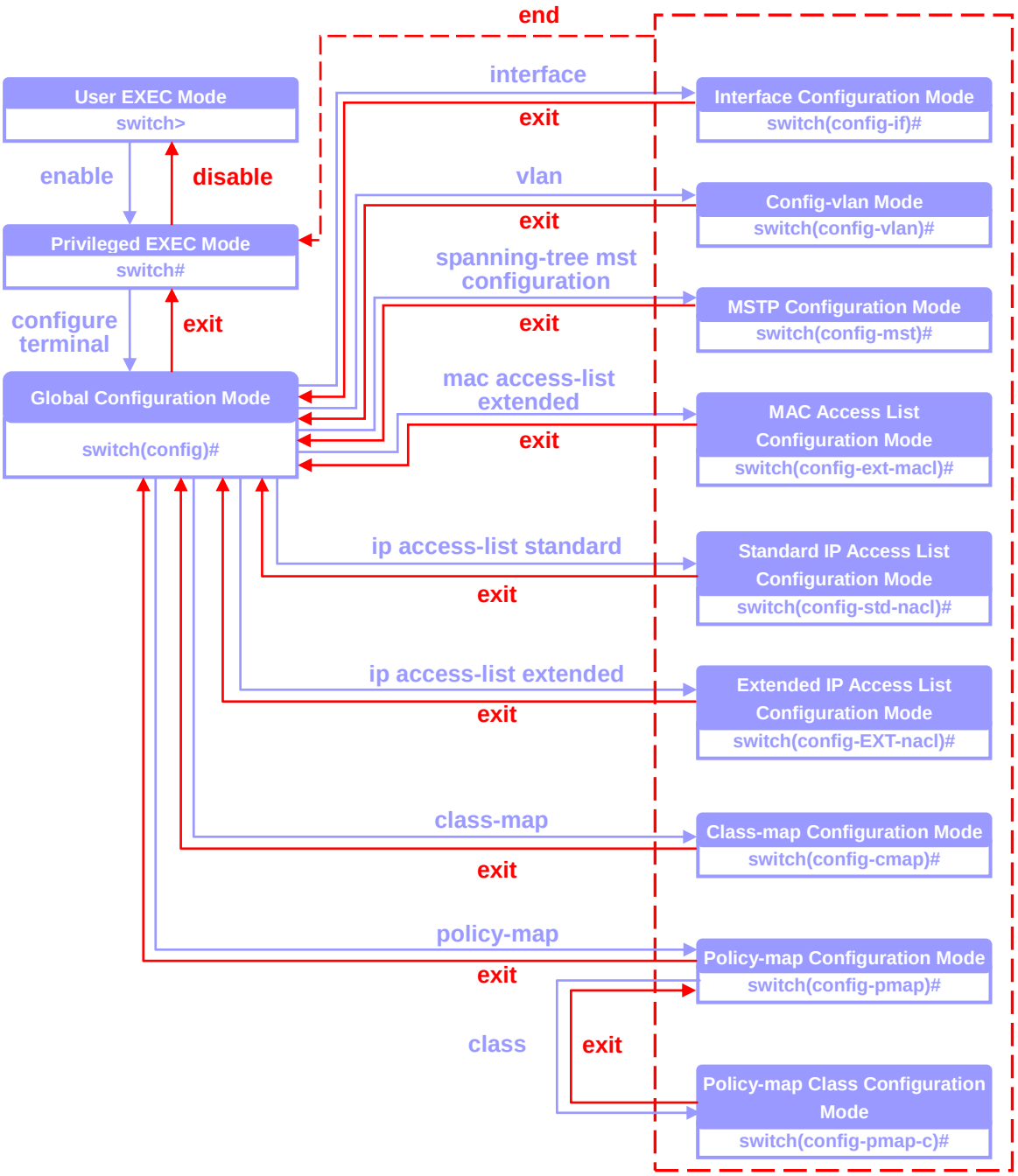


Figure 104 –Relationship of Command Modes

User EXEC Mode	When login the .Switch using privilege level 1 accounts, user will entering User EXEC Mode automatically. User EXEC mode is used to do the basic operation such as show commands.
Privileged EXEC Mode	When login the .Switch using privilege level 15 accounts, user will entering Privileged EXEC Mode automatically. A password is required to enable Privileged EXEC Mode, default is **password**.
Global Configuration Mode	The Global Configuration Mode is used to configure the global commands which will take effect to whole system and all interfaces.
Interface	The Interface Configuration Mode is used to configure the commands for physical

Configuration Mode	interfaces.
Config-vlan Mode	The VLAN Configuration Mode is used to configure the commands for VLAN interfaces.
MSTP Configuration Mode	The MSTP Configuration Mode is used to configure multiple spanning tree specific commands.
MAC Access List Configuration Mode	The MAC Access List Configuration Mode is used to configure L2 access rules including content such as MAC address, VLAN, or specific Ether type.
Standard IP Access List Configuration Mode	The Standard IP Access List Configuration Mode is used to configure L3 access rules with specific source/destination IP address.
Extended IP Access List Configuration Mode	The Standard IP Access List Configuration Mode is used to configure L3/4 access rules with specific IP address, protocol type or port number.
Class-map Configuration Mode	The Class-map Configuration Mode is used to configure class rules and access lists mapping.
Policy-map Configuration Mode	The Policy-map Configuration Mode is used to configure policy mapping for class rules.
Policy-map Class Configuration Mode	The Policy-map Class Configuration Mode is used to configure the actions of policies.

Conventions

This publication uses these conventions to convey instructions and information:
Command descriptions use these conventions:
- Commands and keywords are in **bold** text.
- Arguments for which you supply values are in *italic*.
- Square brackets ([ ]) means optional elements.
- Braces ({}) group required choices, and vertical bars (|) separate the alternative elements.
- Braces and vertical bars within square brackets ([{ | }]) mean a required choice within an optional element.

Chapter 12
System Information Command

System Information Command List

- **system name**
- **system contact**
- **system location**
- **system web-timeout**
- **system cli-timeout**
- **default ip address**
- **default ip address allocation protocol**
- **default mode**
- **default restore**
- **default restore-file**
- **default vlan id**
- **set ip http**
- **ip http port**
- **show system information**
- **show nvram**
- **show http server status**
- **show ip information**
- **show line console**

system name

To define the name of the Switch

Command

system name *<identify info>*

Syntax Description

identify info	A maximum of 15 characters is allowed. A NULL string is not accepted.

Default Settings

SysName

Command Modes

Global Configuration Mode

User Guidelines

This command defines the name of the Switch.

Example

```
switch(config)# system name trendnet
```

Command History

Version	History
1.00.001	This command was introduced.

system contact

To enter identification information of a contact person.

Command

system contact *<contact info>*

Syntax Description		
	contact info	A maximum of 50 characters is allowed. A NULL string is not accepted.

Default Settings

SysContact

Command Modes

Global Configuration Mode

User Guidelines

Use this command to provide the name and/or other information to identify a contact person who is responsible for the Switch.

Example

```
switch(config)# system contact TechSupport
```

Command History	Version	History
	1.00.001	This command was introduced.

system location

To enter a description of the location of the Switch.

Command

system location *<location info>*

Syntax Description		
	location info	A maximum of 50 characters is allowed. A NULL string is not accepted.

Default Settings

SysLocation

Command Modes

Global Configuration Mode

User Guidelines

This command enters a description of the location of the Switch.

Example

```
switch(config)# system location 5F east
```

Command History	Version	History
	1.00.001	This command was introduced.

system web-timeout

To define the amount of time the device times out when no user activity occurs on the web interface.

Command **system web-timeout** *<180-3600 seconds>*

Syntax Description		
	180-3600 seconds	The web interface logs out the current user when no user activity input for 180-3600 seconds.

Default Settings 600 seconds

Command Modes Global Configuration Mode

User Guidelines This command defines the amount of time the device times out when no user activity occurs on the web interface.

Example

```
switch(config)# system web-timeout 3600
```

Command History	Version	History
	1.00.001	This command was introduced.

system cli-timeout

To define the amount of time the device times out when no user activity occurs on the CLI interface.

Command **system cli-timeout** *<1-18000 seconds>*

Syntax Description		
	1-18000 seconds	The cli interface logs out the current user when no user activity input for 1-18000 seconds.

Default Settings 1800 seconds

Command Modes Global Configuration Mode

User Guidelines This command defines the amount of time the device times out when no user activity occurs on the web interface.

Example

```
switch(config)# system cli-timeout 18000
```

Command History	Version	History
	1.00.001	This command was introduced.

default ip address

To configure the default IP interface.

Command

default ip address *<ip-address>* **[subnet-mask** *<subnet mask>* **]**
[interface *<interface-type> <interface-id>* **]**

Syntax Description

ip-address	IP address of the default interface
subnet-mask *subnet mask*	Subnet mask of the default interface
interface *interface-type interface-id*	Interface-type including *Fa* (Fast Ethernet) or *Gi* (Gigabit Ethernet). Interface-id is slot/port number.

Default Settings

IP address - 192.168.10.200
Subnet mask - 255.255.255.0

Command Modes

Global Configuration Mode

User Guidelines

This command is to configure the IP address and subnet mask of default interface.

Example

```
switch(config)# default ip address 10.0.0.250 subnet-mask
255.0.0.0
```

Command History

Version	History
1.00.001	This command was introduced.

default ip address allocation protocol

To configure the protocol that the IP address of default interface is assigned.

Command

default ip address allocation protocol {bootp | rarp | dhcp}

Syntax Description

bootp	Bootp protocol
rarp	RARP protocol
dhcp	DHCP protocol

Default Settings

DHCP

Command Modes

Global Configuration Mode

User Guidelines

This command is to configure the protocol that the IP address of default interface is assigned.

Example

```
switch(config)# default ip address allocation protocol bootp
```

Command History

Version	History
1.00.001	This command was introduced.

Note Default mode must be dynamic to make this command effective.

default mode

To configure the mode that the IP address of default interface is assigned.

Command

```
default mode { manual | dynamic }
```

Syntax Description

manual	Manual mode. The ip address of default interface is the one configured by 'default ip address' command.
dynamic	Dynamic mode. The ip address of default interface is got through the protocol configured by 'default ip address allocation protocol' command.

Default Settings

Manual

Command Modes

Global Configuration Mode

User Guidelines

This command is to configure the mode that the IP address of default interface is assigned.

Example

```
switch(config)# default mode dynamic
```

Command History

Version	History
1.00.001	This command was introduced.

default restore

To enable or disable the default mode of configuration restoration.

Command

```
default restore {enable | disable}
```

Syntax Description

enable	To enable the configuration restoration option.
disable	To disable the configuration restoration.

Default Settings

Disable

Command Modes

Global Configuration Mode

User Guidelines

This command is to adjust the default mode of configuration restoration.

Example

```
switch(config)# default restore enable
```

Command History	Version	History
	1.00.001	This command was introduced.

default restore-file

To configure the default restoration file.

Command

`default restore-file` *<filename>*

Syntax Description	*filename*	The name of restoration file.

Default Settings

Iss.conf

Command Modes

Global Configuration Mode

User Guidelines

This command is to configure the default restoration file.

Example

```
switch(config)# default restore-file restore1.conf
```

Command History	Version	History
	1.00.001	This command was introduced.

Note Default mode must be dynamic to make this command effective.

default vlan id

To configure the default VLAN ID.

Command

`default vlan id <`*count(1-4094)***`>`**

Syntax Description	*count(1-4094)*	Change default VLAN from 1 to 4094.

Default Settings

1

Command Modes

Global Configuration Mode

Example

```
switch(config)#default vlan id 100
```

Command History	Version	History
	1.00.001	This command was introduced.

set ip http

To enable or disable HTTP server.

Command

`set ip http {enable | disable}`

Syntax Description

`enable`	To enable the embedded HTTP server.
`disable`	To disable the embedded HTTP server.

Default Settings

Enable

Command Modes

Global Configuration Mode

Example

```
switch(config)#set ip http enable
```

Command History

Version	History
1.00.001	This command was introduced.

ip http port

To configure the TCP port for HTTP server connection.

Command

`ip http port` *`<port-number(1-65535)>`*

`no ip http port`

Syntax Description

`port-number(1-65535)`	TCP port number.

Default Settings

80

Command Modes

Global Configuration Mode

User Guidelines

The no form resets the HTTP port to default.

Example

```
switch(config)#ip http port 8080
```

Command History

Version	History
1.00.001	This command was introduced.

show system information

To display system information.

Command **show system information**

Command Modes Privileged EXEC mode

Example

```
switch# show system information

Hardware Version                : Rev.A1
Firmware Version                : 1.00.002
Switch Name                     : SysName
System Contact                  : SysContact
System Location                 : SysLocation
Logging Option                  : Console Logging
Login Authentication Mode       : Local
Config Save Status              : Not Initiated
Remote Save Status              : Not Initiated
Config Restore Status           : Successful
Web Timeout Interval            : 600
Cli Timeout Interval            : 18000
```

Command History

Version	History
1.00.001	This command was introduced.

show nvram

To display the current information stored in NVRAM.

Command **show nvram**

Command Modes Privileged EXEC mode

Example

```
switch# show nvram

Default IP Address                  : 192.168.10.200
Default Subnet Mask                 : 255.255.255.0
Default IP Address Config Mode      : Manual
Default IP Address Allocation Protocol : DHCP
Switch Base MAC Address             : 00:74:24:00:02:00
Default Interface Name              : Fa0/1
Default RM Interface Name           : NONE
Config Restore Option               : Restore
Config Save Option                  : Startup save
Config Save IP Address              : 0.0.0.0
Config Save Filename                : iss.conf
Config Restore Filename             : iss.conf
PIM Mode                            : Sparse Mode
IGS Forwarding Mode                 : MAC based
Cli Serial Console                  : Yes
SNMP EngineID                       : 80.00.08.1c.04.46.53
SNMP Engine Boots                   : 2
Default VLAN Identifier             : 1
```

Command History

Version	History
1.00.001	This command was introduced.

show http server status

To display the HTTP server status.

Command

show http server status

Command Modes

Privileged EXEC mode

Example

```
switch# show http server status

HTTP server status            : Enabled
HTTP port is                 : 80
```

Command History

Version	History
1.00.001	This command was introduced.

show ip information

To display the IP information.

Command

show ip information

Command Modes

Privileged EXEC mode

Example

```
switch# show http server status

HTTP server status            : Enabled
HTTP port is                 : 80
switch# show ip information

Global IP Configuration:
------------------------
 IP routing is enabled
 Default TTL is 64
 ICMP redirects are always sent
 ICMP unreachables are always sent
 ICMP echo replies are always sent
 ICMP mask replies are always sent
 Number of aggregate routes is 10
 Number of multi-paths is 2
 Load sharing is disabled
 Path MTU discovery is disabled
```

Command History

Version	History
1.00.001	This command was introduced.

show line console

To display the information of current session.

Command

```
show line console
```

Command Modes

Privileged EXEC mode

Example

```
switch# show line console
Current Session Timeout (in secs) = 18000
```

Command History

Version	History
1.00.001	This command was introduced.

Chapter 13
User Account Command

User Account Command List

username

To configure a user account information

Command

username *<user-name>* **[password** *<passwd>***] [privilege** *<1-15>***]**

no username *<user-name>*

Syntax Description

username *user-name*	Username
password *passwd*	Password
privilege *1-15*	Privilege level. It is from 1 to 15.

Command Modes

Global Configuration Mode

User Guidelines

The no form deletes the user.

Example

```
switch(config)# username user password user privilege 1
```

Command History

Version	History
1.00.001	This command was introduced.

show users

To display the information of current users.

Command

show users

Command Modes

Privileged EXEC mode

Example

```
switch# show users

 Line          User           Peer-Address
0 con          root           Local Peer
```

Command History

Version	History
1.00.001	This command was introduced.

listuser

To display all existing user information.

Command

```
listuser
```

Command Modes

Privileged EXEC mode

Example

```
switch# listuser

USER                  PRIVILEGE
root                  15
guest                 1
user                  1
```

Command History

Version	History
1.00.001	This command was introduced.

Chapter 14
Management VLAN Command

Management VLAN Command List

management vlan-list

To set the VLAN ID for the management VLAN.

Command

```
management vlan-list <vlan-list>
no management vlan-list <vlan-list>
```

Syntax Description

vlan-list	It can be a single VLAN ID from 1 to 4094, a range of VLAN IDs separated by a hyphen (-), or a series of non-continuous numbers divided by a comma (,).

Command Modes

Global Configuration Mode

Example

```
switch(config)# management vlan-list 100
```

Command History

Version	History
1.00.001	This command was introduced.

show management vlan

To display the management VLAN ID.

Command

```
show management vlan
```

Command Modes

Privileged EXEC mode

Example

```
switch# show management vlan
Management VLAN-List
100,
```

Command History

Version	History
1.00.001	This command was introduced.

Chapter 15
IP Settings Command

IP Settings Command List

release dhcp vlanMgmt

To release the DHCP lease of management VLAN interface.

Command

```
release dhcp vlanMgmt
```

Command Modes

Privileged EXEC mode

Example

```
switch# release dhcp vlanMgmt
```

Command History

Version	History
1.00.001	This command was introduced.

Note The IP address of Management VLAN interface must be assigned by a DHCP server.

renew dhcp vlanMgmt

To renew the DHCP lease of management VLAN interface.

Command

```
renew dhcp vlanMgmt
```

Command Modes

Privileged EXEC mode

Example

```
switch# renew dhcp vlanMgmt
```

Command History

Version	History
1.00.001	This command was introduced.

Note The IP address of Management VLAN interface must be assigned by a DHCP server.

ip arp max-retries

To set the maximum number of ARP request retries.

Command

ip arp max-retries *<value (2-10)>*

no ip arp max-retries

Syntax Description

value (2-10)	Number of ARP request retries.

Default Settings

3

Command Modes

Global Configuration Mode

User Guidelines

The no form resets the number of retries to default value.

Example

```
switch(config)# ip arp max-retries 4
```

Command History

Version	History
1.00.001	This command was introduced.

arp

To add a static entry in the switch ARP table.

Command

arp *<ip address> <hardware address>* **{Vlan** *<vlan-id(1-4094)>* **|** *<interface-type> <interface-id>* **| Linuxvlan** *<interface-name>***| Cpu0}**

no arp *<ip address>*

Syntax Description

ip address	IP address of the network node.
hardware address	MAC address of the network node.
Vlan *vlan-id(1-4094)*	VLAN id
interface-type interface-id	Interface type and id of the interface connects to the ARP entry. Interface-type including *Fa* (Fast Ethernet) or *Gi* (Gigabit Ethernet). Interface-id is slot/port number.
Linuxvlan *interface-name*	Interface name of Linux VLAN interface.
Cpu0	Out-of-band management interface.

Command Modes Global Configuration Mode

User Guidelines The no form is to remove the entry.

Example

```
switch(config)# arp 10.90.90.100 11:22:33:44:55 vlan 1
```

Command History

Version	History
1.00.001	This command was introduced.

arp timeout

To set the ARP table timeout.

Command

arp timeout *<seconds (30-86400)>*

no arp timeout

Syntax Description

seconds (30-86400)	ARP entry timeout period

Default Settings 300

Command Modes Global Configuration Mode

User Guidelines The no form is to reset to default value.

Example

```
switch(config)# arp timeout 3600
```

Command History

Version	History
1.00.001	This command was introduced.

ip address

To configure the IP address of interface.

Command

ip address *<ip-address> <subnet-mask> <gw-address>*

no ip address *<ip-address>*

Syntax Description

ip-address	IP address of the interface
subnet-mask	Subnet mask of the interface
gw-address	IP address of the gateway

Command Modes Interface Configuration Mode

User Guidelines The no form will delete the configured IP address.

Example

```
switch(config-if)# ip address 20.0.0.1 255.0.0.0 20.0.0.254
```

Command History

Version	History
1.00.001	This command was introduced.

ip address dhcp

To set the IP address of interface to be assigned by DHCP server.

Command

```
ip address dhcp
```

Command Modes Interface Configuration Mode

Example

```
switch(config-if)#ip address dhcp
```

Command History

Version	History
1.00.001	This command was introduced.

debug ip dhcp client

To enable the debug mode of DHCP client.

Command

```
debug ip dhcp client { all | event | packets | errors | bind }
no debug ip dhcp client { all | event | packets | errors | bind }
```

Syntax Description

all	Information of all DHCP client activities
event	Information of DHCP client events.
packets	Information of DHCP client packets
errors	Information of errors.
bind	Information of DHCP client binding.

Default Settings Disabled

Command Modes Privileged EXEC mode

User Guidelines This command is to enable the debug mode of DHCP client, and the no form is to disable it.

Example

```
switch#debug ip dhcp client all
```

Command History

Version	History
1.00.001	This command was introduced.

show ip interface

To display the IP interface information.

Command

show ip interface

Command Modes

Privileged EXEC mode

User Guidelines

This command is to display the IP interface information.

Example

```
switch#show ip interface

vlanMgmt is up, line protocol is down
Internet Address is 0.0.0.0/0
Broadcast Address  255.255.255.255
IP address allocation method is dynamic
IP address allocation protocol is dhcp
```

Command History

Version	History
1.00.001	This command was introduced.

show ip route

To display the IP route information.

Command

show ip route [{ *<ip-address>* **[***<mask>***] | bgp | connected | ospf | rip | static | summary }]**

Syntax Description

<ip-address> *<mask>*	Network address and subnet mask of IP route.
bgp	BGP routes.
connected	Directly connected routes.
ospf	OSPF routes.
rip	RIP routes.
static	Static routes.
summary	Summary of all IP routes.

Command Modes

Privileged EXEC mode

Example

```
switch#show ip route summary

Route Source    Routes
connected        0
static           0
rip              0
bgp              0
ospf             0
Total            0
```

Command History

Version	History
1.00.001	This command was introduced.

Chapter 16
IP Authorized Manager Command

IP Authorized Manager Command List

authorized-manager

To set an authorized administrator source IP address, and the services, interfaces, or VLANs that it is allowed to visit.

Command

authorized-manager ip-source *<ip-address>* **[{***<subnet-mask>* **| /** *<prefix-length(1-32)>***}] [interface [***<interface-type <0/a-b, 0/c, ...>***] [***<interface-type <0/a-b, 0/c, ...>***]] [vlan** *<a,b or a-b or a,b,c-d>***] [cpu0] [service [snmp] [telnet] [http] [https] [ssh]]**

no authorized-manager ip-source *<ip-address>* **[{***<subnet-mask>* **| /** *<prefix-length(1-32)>***}]**

Syntax Description

ip-source *ip-address*	IP address of authorized manager
<subnet-mask>	Subnet mask of the authorized IP address
/ *prefix-length(1-32)*	Prefix length of the authorized IP address
interface-type 0/a-b, 0/c	Interface of the authorized administrator is allowed to connected to
vlan *a,b or a-b or a,b,c-d*	VLAN ID of the authorized administrator is allowed to connected to
cpu0	Out-of-band management interface.
service snmp	SNMP service
service telnet	Telnet service
service http	HTTP (Web) service
service https	HTTPS (SSL) service
service ssh	SSH service

Default Settings

By default no authorized-manager ip-source is assigned. All services, vlan, and interfaces are allowed for an authorized-manager but default expect for the out-of-band management interface.

Command Modes

Global Configuration Mode

User Guidelines

The no form removes the administrator from the list.

Example

```
switch(config)# authorized-manager ip-source 10.90.90.100
```

Command History

Version	History
1.00.001	This command was introduced.

show authorized-managers

Display the authorized-manager list.

Command

show authorized-managers [ip-source *<ip-address>***]**

Syntax Description

ip-source *ip-address*	IP address of authorized manager

Command Modes

Privileged EXEC mode

Example

```
switch#show authorized-managers

Ip Authorized Manager Table
---------------------------

Ip Address      : 10.90.90.100
Ip Mask        : 255.255.255.255
Services allowed : ALL
Ports allowed   : Fa0/1, Fa0/2, Fa0/3, Fa0/4
                  Fa0/5, Fa0/6, Fa0/7, Fa0/8
                  Fa0/9, Fa0/10, Fa0/11, Fa0/12
                  Fa0/13, Fa0/14, Fa0/15, Fa0/16
                  Fa0/17, Fa0/18, Fa0/19, Fa0/20
                  Fa0/21, Fa0/22, Fa0/23, Fa0/24
                  Gi0/1, Gi0/2, Gi0/3, Gi0/4
On cpu0        : Deny
Vlans allowed   : All Available Vlans
```

Command History

Version	History
1.00.001	This command was introduced.

Chapter 17
SNMP Command

SNMP Command List

snmp access

To configure the access settings of a SNMP group, and the no form removes the group.

Command

snmp access *<GroupName>* **{v1 | v2c | v3 {auth | noauth | authpriv}} [read <***ReadView* **| none>] [write <***WriteView* **| none>] [notify <***NotifyView* **| none>] [{volatile | nonvolatile}]**

no snmp access *<GroupName>* **{v1 | v2c | v3 {auth | noauth | authpriv}}**

Syntax Description

GroupName	Name of SNMP group
v1	SNMP version 1 is to be used
v2c	SNMP version 2v is to be used
v3	SNMP version 3 is to be used
auth	Authentication is required for the SNMP messages
noauth	Authentication is not required for the SNMP messages
authpriv	Both authentication and encryption are required for the SNMP messages
read *ReadView*	The SNMP group has read privilege and is allowed to access the specified MIB object groups
read none	The SNMP group has read privilege
write *WriteView*	The SNMP group has write privilege and is allowed to access the specified MIB object groups
write none	The SNMP group has write privilege
notify *NotifyView*	The SNMP group can receive SNMP Trap messages and is allowed to access the specified MIB object groups
notify none	The SNMP group can receive SNMP Trap messages
volatile	Store in volatile memory
nonvolatile	Store in nonvolatile memory

Default Settings

Group Name : iso
Read View : iso
Write View : iso
Notify View : iso
Storage Type : Non-volatile

Group Name : initial
Read View : restricted
Write View : restricted
Notify View : restricted
Storage Type : Non-volatile

Group Name : initial
Read View : iso
Write View : iso
Notify View : iso
Storage Type : Non-volatile

Group Name : ReadOnly
Read View : ReadWrite
Write View :
Notify View : ReadWrite
Storage Type : Non-volatile

Group Name : ReadWrite
Read View : ReadWrite
Write View : ReadWrite
Notify View : ReadWrite
Storage Type : Non-volatile

Command Modes Global Configuration Mode

User Guidelines Before configuring the access settings, the SNMP group has to be created first.

Example

```
switch(config)# snmp access oper v2c read operv2readview write
operv2writeview notify operv2notifyview nonvolatile
```

Command History

Version	History
1.00.001	This command was introduced

snmp community

To create a SNMP community, and the no form removes the community.

Command

snmp community *<CommunityName>* **security** *<SecurityName>* **[{volatile | nonvolatile}]**

no snmp community *<CommunityName>*

Syntax Description

CommunityName	SNMP community name
security *SecurityName*	Security name
volatile	Store in volatile memory
nonvolatile	Store in nonvolatile memory

Default Settings

Community Index : NETMAN
Community Name : NETMAN
Security Name : none
Storage Type : Non-volatile

Community Index : PUBLIC
Community Name : PUBLIC
Security Name : none
Storage Type : Non-volatile

Command Modes Global Configuration Mode

Example

```
switch(config)# snmp community oper security none nonvolatile
```

Command History

Version	History
1.00.001	This command was introduced

snmp engineid

To configure the SNMP engine identifier of the switch

Command

snmp engineid *<EngineIdentifier>*

no snmp engineid

Syntax Description

EngineIdentifier	A string of between 5 and 32 octets expressed in hexadecimal that is separated by dots

Default Settings

80.00.08.1c.04.46.53

Command Modes

Global Configuration Mode

User Guidelines

SNMP engine ID is unique for each switches

Example

```
switch(config)# snmp engineid 80.00.08.1c.04.46.ae
```

Command History

Version	History
1.00.001	This command was introduced

snmp group

To create a SNMP group and the no form deletes the group

Command

snmp group *<GroupName>* **user** *<UserName>* **security-model {v1 | v2c | v3 } [{volatile | nonvolatile}]**

no snmp group *<GroupName>* **user** *<UserName>* **security-model {v1 | v2c | v3 }**

Syntax Description

GroupName	SNMP group name
user *UserName*	Specify the user name
security-model v1	SNMP version 1 is to be used
security-model v2c	SNMP version 2v is to be used
security-model v3	SNMP version 3 is to be used
volatile	Store in volatile memory
nonvolatile	Store in nonvolatile memory

Default Settings

```
Security Model : v1
Security Name   : none
Group Name      : iso
Storage Type    : Non-volatile
------------------------------
Security Model : v1
Security Name   : ReadOnly
Group Name      : ReadOnly
Storage Type    : Non-volatile
------------------------------
Security Model : v1
Security Name   : ReadWrite
Group Name      : ReadWrite
Storage Type    : Non-volatile
------------------------------
Security Model : v2c
Security Name   : none
Group Name      : iso
Storage Type    : Non-volatile
------------------------------
Security Model : v2c
Security Name   : ReadOnly
Group Name      : ReadOnly
Storage Type    : Non-volatile
------------------------------
Security Model : v2c
Security Name   : ReadWrite
Group Name      : ReadWrite
Storage Type    : Non-volatile
------------------------------
Security Model : v3
Security Name   : initial
Group Name      : initial
Storage Type    : Non-volatile
------------------------------
Security Model : v3
Security Name   : templateMD5
Group Name      : initial
Storage Type    : Non-volatile
------------------------------
Security Model : v3
Security Name   : templateSHA
Group Name      : initial
Storage Type    : Non-volatile
```

Command Modes

Global Configuration Mode

Example

```
switch(config)# snmp group oper user operuser security-model
v2c nonvolatile
```

Command History

Version	History
1.00.001	This command was introduced

snmp trapinfo

To configure the SNMP Trap setting of a community user, and no form deletes the setting.

Command

snmp trapinfo community-user *<UserName>* **IPAddress {***<IPAddress>* **|** *<IP6Address>***} security-model {v1 | v2c | v3 {auth | noauth | authpriv}} [{volatile | nonvolatile}]**

no snmp trapinfo community-user *<UserName>* **security-model {v1 | v2c | v3}**

Syntax Description

community-user *UserName*	SNMP community-user name
IPAddress *IPAddress*	IPv4 address of SNMP Trap messages to be sent to
IPAddress *IP6Address*	IPv6 address of SNMP Trap messages to be sent to
security-model v1	SNMP version 1 is to be used
security-model v2c	SNMP version 2v is to be used
security-model v3 auth	SNMP version 3 is to be used, and authentication is used for the SNMP messages
security-model v3 noauth	SNMP version 3 is to be used, and no authentication is used for the SNMP messages
security-model v3 authpriv	SNMP version 3 is to be used, and authentication and encryption are used for the SNMP messages
volatile	Store in volatile memory
nonvolatile	Store in nonvolatile memory

Default Settings

None

Command Modes

Global Configuration Mode

Example

switch(config)# **snmp trapinfo community-user oper ipAddress 172.17.0.168 security-model v2c nonvolatile**

Command History

Version	History
1.00.001	This command was introduced

snmp user

To create a SNMP user and no form deletes the user.

Command

snmp user *<UserName>* **[auth {md5 | sha}** *<passwd>* **[priv DES** *<passwd>***]] [{volatile | nonvolatile}]**

no snmp user *<UserName>*

Syntax Description

UserName	SNMP user name
auth md5	Specify MD5 as authentication algorithm
auth sha	Specify Secure Hash as authentication algorithm

passwd	Authentication password
priv DES *passwd*	Encryption password
volatile	Store in volatile memory
nonvolatile	Store in nonvolatile memory

Default Settings

```
User                        : initial
Authentication Protocol : None
Privacy Protocol          : None
Storage Type               : Non-volatile
-----------------------------
User                        : ReadOnly
Authentication Protocol : None
Privacy Protocol          : None
Storage Type               : Non-volatile
-----------------------------
User                        : ReadWrite
Authentication Protocol : None
Privacy Protocol          : None
Storage Type               : Non-volatile
-----------------------------
User                        : templateMD5
Authentication Protocol : MD5
Privacy Protocol          : None
Storage Type               : Non-volatile
-----------------------------
User                        : templateSHA
Authentication Protocol : SHA
Privacy Protocol          : DES_CBC
Storage Type               : Non-volatile
```

Command Modes

Global Configuration Mode

Example

```
switch(config)# snmp user operator1
```

Command History

Version	History
1.00.001	This command was introduced

snmp view

To create a SNMP view which limits the range of MIB objects that a SNMP administrator can access to. The no form deletes the SNMP view.

Command

snmp view *<ViewName> <OIDTree>* **[mask** *<OIDMask>***] {included | excluded} [{volatile | nonvolatile}]**

no snmp view *<ViewName> <OIDTree>*

Syntax Description

ViewName	SNMP view name
OIDTree	The object ID of MIB tree
mask *OIDMask*	The mask of OID
included	Includes the object in the list that the SNMP administrator can access

excluded	Excludes the object from the list that the SNMP administrator can access
volatile	Store in volatile memory
nonvolatile	Store in nonvolatile memory

Default Settings

View Name : iso
Subtree OID : 1
Subtree Mask : 1
View Type : Included
Storage Type : Non-volatile

View Name : ReadWrite
Subtree OID : 1
Subtree Mask : 1
View Type : Included
Storage Type : Non-volatile

View Name : restricted
Subtree OID : 1
Subtree Mask : 1
View Type : Included
Storage Type : Non-volatile

Command Modes

Global Configuration Mode

Example

```
switch(config)# snmp view operv2readview 1.3.6.1 mask 1.1.1.1 included nonvolatile
```

Command History

Version	History
1.00.001	This command was introduced

snmp-server enable traps snmp authentication

To enable the authentication trap messages for SNMP v1 and v2c, and the no form disables it.

Command

```
snmp-server enable traps snmp authentication

no snmp-server enable traps snmp authentication
```

Default Settings

Disabled

Command Modes

Global Configuration Mode

Example

```
switch(config)# snmp-server enable traps snmp authentication
```

Command History

Version	History
1.00.001	This command was introduced

snmp-server enable traps

To enable specific SNMP trap message types, and no form disable them.

Command

snmp-server enable traps {firewall-limit | linkup | linkdown | sip-states |sip-cfg-change | coldstart | poe-power | dhcp-pool-limit | dsx1-line}

no snmp-server enable traps {firewall-limit | linkup | linkdown| sip-states | sip-cfg-change | coldstart | poe-power | dhcp-pool-limit | dsx1-line}

Syntax Description

firewall-limit	
linkup	Interfaces are linked up
linkdown	Interfaces are linked down
sip-states	The change of SIP protocol state
sip-cfg-change	The change of SIP configuration
coldstart	The switch is power cycled
poe-power	
dhcp-pool-limit	
dsx1-line	

Default Settings

Linkup and Linkdown messages are enabled

Command Modes

Global Configuration Mode

Example

```
switch(config)# snmp enable traps poe-power
```

Command History

Version	History
1.00.001	This command was introduced

snmp-server trap udp-port

To specify the UDP port for sending SNMP trap messages

Command

snmp-server trap udp-port *<port>*

no snmp-server trap udp-port

Syntax Description

<port>	UDP port number

Default Settings

162

Command Modes

Global Configuration Mode

Example

```
switch(config)# snmp-server trap udp-port 10162
```

Command History

Version	History
1.00.001	This command was introduced

snmp trap link-status

To enable sending link-status Trap message, and no form disables it

Command

```
snmp trap link-status
no snmp trap link-status
```

Default Settings

Disabled

Command Modes

Interface Configuration Mode

Example

```
switch(config-if)# snmp trap link-status
```

Command History

Version	History
1.00.001	This command was introduced

show snmp

To display the SNMP settings

Command

```
show snmp
```

Command Modes

Privileged EXEC Mode

Example

```
switch#show snmp

 0 SNMP Packets Input
    0 Bad SNMP Version errors
    0 Unknown community name
    0 Get request PDUs
    0 Get Next PDUs
    0 Set request PDUs

 0 SNMP Packets Output
    0 Too big errors
    0 No such name errors
    0 Bad value errors
    0 General errors
    0 Trap PDUs

 SNMP Manager-role output packets
    0 Drops

 SNMP Informs:
    0 Inform Requests generated
    0 Inform Responses received
    0 Inform messages Dropped
    0 Inform Requests awaiting Acknowledgement

 SNMP Trap Listen Port is 162
```

Command History

Version	History
1.00.001	This command was introduced

show snmp community

To display the SNMP community information

Command

```
show snmp community
```

Command Modes

Privileged EXEC Mode

Example

```
switch# show snmp community

Community Index : NETMAN
Community Name  : NETMAN
Security Name   : none
Context Name    :
Transport Tag   :
Storage Type    : Non-volatile
Row Status      : Active
------------------------------
Community Index : PUBLIC
Community Name  : PUBLIC
Security Name   : none
Context Name    :
Transport Tag   :
Storage Type    : Non-volatile
Row Status      : Active
------------------------------
Community Index : oper
Community Name  : oper
Security Name   : none
Context Name    :
Transport Tag   :
Storage Type    : Non-volatile
Row Status      : Active
------------------------------
```

Command History

Version	History
1.00.001	This command was introduced

show snmp engineID

To display the SNMP engine ID

Command

```
show snmp engineID
```

Command Modes

Privileged EXEC Mode

Example

```
switch# show snmp engineid
EngineId: 80.00.08.1c.04.46.53
```

Command History

Version	History
1.00.001	This command was introduced

show snmp group

To display the SNMP group information

Command

```
show snmp group
```

Command Modes Privileged EXEC Mode

Example

```
switch#  show snmp group

Security Model : v1
Security Name  : none
Group Name     : iso
Storage Type   : Non-volatile
Row Status     : Active
------------------------------
Security Model : v1
Security Name  : ReadOnly
Group Name     : ReadOnly
Storage Type   : Non-volatile
Row Status     : Active
------------------------------
Security Model : v1
Security Name  : ReadWrite
Group Name     : ReadWrite
Storage Type   : Non-volatile
Row Status     : Active
------------------------------
Security Model : v2c
Security Name  : none
Group Name     : iso
Storage Type   : Non-volatile
Row Status     : Active
------------------------------
Security Model : v2c
Security Name  : ReadOnly
Group Name     : ReadOnly
Storage Type   : Non-volatile
Row Status     : Active
------------------------------
Security Model : v2c
Security Name  : ReadWrite
Group Name     : ReadWrite
Storage Type   : Non-volatile
Row Status     : Active
------------------------------
Security Model : v3
Security Name  : initial
Group Name     : initial
Storage Type   : Non-volatile
Row Status     : Active
------------------------------
Security Model : v3
Security Name  : templateMD5
Group Name     : initial
Storage Type   : Non-volatile
Row Status     : Active
------------------------------
Security Model : v3
Security Name  : templateSHA
Group Name     : initial
Storage Type   : Non-volatile
Row Status     : Active
------------------------------
```

Command History	Version	History
	1.00.001	This command was introduced

show snmp group access

To display the access setting of SNMP group

Command

```
show snmp group access
```

Command Modes Privileged EXEC Mode

Example

```
switch# show snmp group access

Group Name   : iso
Read View    : iso
Write View   : iso
Notify View  : iso
Storage Type : Non-volatile
Row Status   : Active
------------------------------
Group Name   : iso
Read View    : iso
Write View   : iso
Notify View  : iso
Storage Type : Non-volatile
Row Status   : Active
------------------------------
Group Name   : initial
Read View    : restricted
Write View   : restricted
Notify View  : restricted
Storage Type : Non-volatile
Row Status   : Active
------------------------------
Group Name   : initial
Read View    : iso
Write View   : iso
Notify View  : iso
Storage Type : Non-volatile
Row Status   : Active
------------------------------
Group Name   : initial
Read View    : iso
Write View   : iso
Notify View  : iso
Storage Type : Non-volatile
Row Status   : Active
------------------------------
Group Name   : ReadOnly
Read View    : ReadWrite
Write View   :
Notify View  : ReadWrite
Storage Type : Non-volatile
Row Status   : Active
------------------------------
Group Name   : ReadOnly
Read View    : ReadWrite
Write View   :
Notify View  : ReadWrite
Storage Type : Non-volatile
Row Status   : Active
------------------------------
Group Name   : ReadWrite
Read View    : ReadWrite
Write View   : ReadWrite
Notify View  : ReadWrite
Storage Type : Non-volatile
Row Status   : Active
------------------------------
Group Name   : ReadWrite
```

```
Read View    : ReadWrite
Write View   : ReadWrite
Notify View  : ReadWrite
Storage Type : Non-volatile
Row Status   : Active
----------------------------
```

Command History

Version	History
1.00.001	This command was introduced

show snmp inform statistics

To display the recipient information of SNMP traps

Command

show snmp inform statistics

Command Modes

Privileged EXEC Mode

Example

```
switch# show snmp inform statistics

Target Address Name : operV2
IP Address          : 172.17.0.168
------------------------------
```

Command History

Version	History
1.00.001	This command was introduced

show snmp trapinfo

To display the SNMP trap information

Command

show snmp trapinfo

Command Modes

Privileged EXEC Mode

Example

```
switch# show snmp trapinfo

Host IP Address     : 172.17.0.168
Community/User Name : oper
Security Model      : v2c
Security Level      : No Authenitcation, No Privacy
------------------------------
```

Command History

Version	History
1.00.001	This command was introduced

show snmp user

To display the SNMP user information

Command

show snmp user

Command Modes

Privileged EXEC Mode

Example

```
switch# show snmp user

Engine ID             : 80.00.08.1c.04.46.53
User                 : initial
Authentication Protocol : None
Privacy Protocol       : None
Storage Type           : Non-volatile
Row Status             : Active
-----------------------------
Engine ID             : 80.00.08.1c.04.46.53
User                 : ReadOnly
Authentication Protocol : None
Privacy Protocol       : None
Storage Type           : Non-volatile
Row Status             : Active
-----------------------------
Engine ID             : 80.00.08.1c.04.46.53
User                 : ReadWrite
Authentication Protocol : None
Privacy Protocol       : None
Storage Type           : Non-volatile
Row Status             : Active
-----------------------------
Engine ID             : 80.00.08.1c.04.46.53
User                 : templateMD5
Authentication Protocol : MD5
Privacy Protocol       : None
Storage Type           : Non-volatile
Row Status             : Active
-----------------------------
Engine ID             : 80.00.08.1c.04.46.53
User                 : templateSHA
Authentication Protocol : SHA
Privacy Protocol       : DES_CBC
Storage Type           : Non-volatile
Row Status             : Active
-----------------------------
```

Command History

Version	History
1.00.001	This command was introduced

show snmp viewtree

To display SNMP view information

Command **show snmp viewtree**

Command Modes Privileged EXEC Mode

Example

```
switch# show snmp viewtree

View Name    : iso
Subtree OID  : 1
Subtree Mask : 1
View Type    : Included
Storage Type : Non-volatile
Row Status   : Active
------------------------------
View Name    : ReadWrite
Subtree OID  : 1
Subtree Mask : 1
View Type    : Included
Storage Type : Non-volatile
Row Status   : Active
------------------------------
View Name    : restricted
Subtree OID  : 1
Subtree Mask : 1
View Type    : Included
Storage Type : Non-volatile
Row Status   : Active
------------------------------
```

Command History

Version	History
1.00.001	This command was introduced

show snmp-server traps

To display the configured trap message information

Command **show snmp-server traps**

Command Modes Privileged EXEC Mode

Example

```
switch# show snmp-server traps
Currently enabled traps:
------------------------
linkup,linkdown,
```

Command History

Version	History
1.00.001	This command was introduced

Chapter 18
SSH Command

SSH Command List

ssh

To activate the SSH server function on the switch. The no format is to turn it off.

Command

```
ssh {enable | disable}
```

Syntax Description

enable	To turn on the SSH server function.
disable	To turn off the SSH server function.

Default Settings

Enabled

Command Modes

Global Configuration Mode

Example

```
switch(config)# ssh enable
```

Command History

Version	History
1.00.001	This command was introduced

ip ssh

To configure the SSH server settings. The no format will cancel the settingand go back to default value.

Command

```
ip ssh {version compatibility | cipher ([des-cbc] [3des-cbc])
|  auth ([hmac-md5] [hmac-sha1]) }

no ip ssh {version compatibility | cipher ([des-cbc] [3des-cbc])
| auth ([hmac-md5] [hmac-sha1]) }
```

Syntax Description

version compatibility	The supported version of SSH.
cipher ([des-cbc] [3des-cbc])	To configure SSH Cipher algorithm. User can choose from DES (Data Encryption Standard) or 3DES (Triple_Data Encryption Standard) encryption algorithm in CBC (Cipher Blocking Chain) mode.
auth ([hmac-md5] [hmac-sha1])	To configure authentication encryption algorithm. User can choose two different Hash-based Message Authentication Codes (HMAC): MD5 (Message-Digest algorithm 5) or SHA1 (Secure Hash Algorithm).

Default Settings

Version: 2
Cipher: 3DES-CBC
Authentication: HMAC-SHA1

Command Modes

Global Configuration Mode

User Guidelines

When set version compatibility, both SSH version-1 and SSH version-2 will be supported.

a

Example

```
switch(config)# ip ssh version compatibility
```

Command History

Version	History
1.00.001	This command was introduced

debug ssh

To enable the trace level messages of SSH. The no format will reset all settings.

Command

debug ssh {all | [shut] [mgmt] [data] [ctrl] [dump] [resource] [failall] [buffer] [server]}

no debug ssh {all | [shut] [mgmt] [data] [ctrl] [dump] [resource] [failall] [buffer] [server]}

Syntax Description

all	Enable or disable all categories of messages.
shut	Shutdown messages.
mgmt	Management messages.
data	Data Path messages.
ctrl	Control panel messages.
dump	Packet Dump messages.
resource	All resource messages except for buffer.
failall	Failure messages.
buffer	Buffer messages.
server	SSH server messages.

Default Settings

Disabled.

Command Modes

Privileged EXEC Mode

Example

```
switch# debug ssh all
```

Command History

Version	History
1.00.001	This command was introduced

show ip ssh

To display the SSH server information.

Command

```
show ip ssh
```

Command Modes

Privileged EXEC Mode

Example

```
switch# show ip ssh

Version         : 2
Cipher Algorithm : 3DES-CBC
Authentication   : HMAC-SHA1
Trace Level      : None
Server Status    : Enable
```

Command History

Version	History
1.00.001	This command was introduced

Chapter 19
SSL Command

SSL Command List

ip http secure

To activate SSL server on the switch and configure Cipher and key settings. The no form will deactivate SSL server and all settings.

Command

```
ip http secure { server | ciphersuite [rsa-null-md5]
[rsa-null-sha1]        [RSA-DES-SHA1]        [RSA-3DES-SHA1]
[dh-rsa-des-sha1] [dh-rsa-3des-sha1] [RSA-EXP1024-DES-SHA1] |
crypto key rsa [usage-keys (512|1024)] }

no ip http secure { server |  ciphersuite [rsa-null-md5]
[rsa-null-sha1]        [RSA-DES-SHA1]        [RSA-3DES-SHA1]
[dh-rsa-des-sha1] [dh-rsa-3des-sha1] [RSA-EXP1024-DES-SHA1]}
```

Syntax Description

server	SSL server
ciphersuite	SSL Cipher algorithm
rsa-null-md5	RSA-NULL-MD5 cipher algorithm
rsa-null-sha1	RSA-NULL-SHA1 cipher algorithm
RSA-DES-SHA1	RSA-DES-SHA1 cipher algorithm
RSA-3DES-SHA1	RSA-3DES-SHA1 cipher algorithm
dh-rsa-des-sha1	DH-RSA-DES-SHA1 cipher algorithm
dh-rsa-3des-sha1	DH-RSA-3DES-SHA1 cipher algorithm
RSA-EXP1024-DES-SHA1	RSA-EXP1024-DES-SHA1 cipher algorithm
crypto key rsa	To specify the RSA key length
usage-keys 512	The RSA key length is 512
usage-keys 1024	The RSA key length is 1024

Default Settings

SSL server is disabled.
Cipher Suite is RSA-DES-SHA1, RSA-3DES-SHA1, and RSA-EXP1024-DES-SHA1

Command Modes

Global Configuration Mode

Example

```
switch(config)# ip http secure ciphersuite rsa-null-md5
```

Command History

Version	History
1.00.001	This command was introduced

debug ssl

To enable the debug messages of SSL. The no format will reset all settings.

Command

debug ssl {all | [shut] [mgmt] [data] [ctrl] [dump] [resource] [failall] [buffer]}

no debug ssl {all | [shut] [mgmt] [data] [ctrl] [dump] [resource] [failall] [buffer]}

Syntax Description

all	Enable or disable all categories of messages.
shut	Shutdown messages.
mgmt	Management messages.
data	Data Path messages.
ctrl	Control panel messages.
dump	Packet Dump messages.
resource	All resource messages except for buffer.
failall	Failure messages.
buffer	Buffer messages.

Default Settings

Disabled

Command Modes

Privileged EXEC Mode

Example

```
switch# debug ssl all
```

Command History

Version	History
1.00.001	This command was introduced

show ssl server-cert

To display SSL server certification

Command

show ssl server-cert

Command Modes

Privileged EXEC Mode

User Guidelines

The server certification has to be created first.

Example

```
switch# show ssl server-cert

Certificate:
    Data:
        Version: 1 (0x0)
        Serial Number:
            87:97:71:61:7f:72:c6:ae
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=CA, L=Torrance, O=TRENDnet
        Validity
            Not Before: Aug 18 12:26:51 2009 GMT
            Not After : Aug 18 12:26:51 2011 GMT
        Subject: CN=TL2-E284
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                 00:b4:95:58:2a:04:2d:a4:6b:a2:6a:75:19:d7:c3:
                 7d:f6:5b:5e:93:78:11:a5:b1:66:b7:b6:9e:65:3f:
                 de:d3:a0:84:54:58:da:18:0a:fb:d5:c3:bf:ab:a8:
                 b9:e1:76:fa:15:d3:cb:b5:2e:6a:54:dc:a4:5d:39:
                 aa:48:ea:55:81:2f:c5:16:38:57:4f:73:4c:ba:c2:
                 d5:4d:61:2e:ab:a4:79:03:6c:03:b3:3b:00:71:91:
                 93:12:8a:3b:2e:9c:bb:7d:7d:b8:a4:ca:f8:53:88:
                 c3:a5:2c:ba:e1:61:09:76:b1:4d:f7:9d:de:14:ef:
                 5e:2e:ca:a9:2e:30:46:11:29
                Exponent: 65537 (0x10001)
    Signature Algorithm: sha1WithRSAEncryption
3e:dc:a0:a8:6e:c0:50:5e:98:be:82:01:35:50:3a:be:c7:42:
35:93:c7:f4:d7:f5:2e:eb:cd:ec:fb:fd:d4:8d:e9:26:51:7c:
06:c8:1c:8b:46:92:12:43:c1:9d:0a:86:52:98:5b:f4:5a:dd:
25:99:af:17:3c:ba:1a:c1:42:aa:a9:b3:63:f6:17:9d:eb:16:
c6:8b:aa:26:8f:79:56:bf:6a:cb:bc:67:55:af:88:20:f5:f0:
6d:1a:27:aa:50:83:64:e0:f1:ae:89:7a:5e:17:1b:f7:7b:1f:
da:7f:ec:1b:69:d8:a5:e6:c6:de:5d:5b:c7:35:37:c6:ce:5b:
9b:f3
```

Command History

Version	History
1.00.001	This command was introduced

show ip http secure server status

To display the SSL server status

Command

```
show ip http secure server status
```

Command Modes

Privileged EXEC Mode

Example

```
switch# show ip http secure server status

HTTP secure server status      : Disabled
HTTP secure server ciphersuite  : RSA-NULL-MD5:
```

Command History

Version	History
1.00.001	This command was introduced

Chapter 20
System Log Command

System Log Command List

copy logs

Backup the system log to a remote tftp server

Command

copy logs *tftp://ip-address/filename*

Syntax Description

tftp://ip-address/filename	The IP address the remote tftp server and the name of the system log file to be saved.

Command Modes

Global Configuration Mode

User Guidelines

The maximum lengths of filename are 32 characters.

Example

```
switch(config)# copy logs tftp://172.17.0.100/syslog1
```

Command History

Version	History
1.00.001	This command was introduced

logging

To configure the syslog server settings, and the no form resets all settings.

Command

logging { *<ip-address>* **| buffered** *<size (1-200)>* **| console |facility {local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7| } |trap [{** *<level (0-7)>* **| alerts | critical | debugging | emergencies | errors |informational | notification | warnings }] | on }**

no logging { *<ip-address>* **| buffered | console | facility | trap | on }**

Syntax Description

ip-address	IP address of the syslog server
buffered *size (1-200)*	The size of internal logging buffer
console	Enable logging to the console
Facility local0~7	Specifies the facility that is indicated in the message. Possible values: local0, local1, local2, local3, local4, local5, local 6, local7
trap	Enable trap messages
level (0-7)	Severity levels
alerts	Alert level: action must be taken immediately
critical	Critical level: Critical conditions
debugging	Debug level: Debug messages
emergencies	Emergency level: System is unusable
errors	Error level: Error conditions
informational	Informational level: Informational messages
notification	Notification level: Normal but significant condition
warnings	Warning level: Warning conditions
on	Enable the syslog

Default Settings

Logging: Enabled
Console: Disabled
Timestamp: Enabled
Trap: Informational
IP address: None
Facility: Local0
Buffered: 50

Command Modes

Global Configuration Mode

Example

```
switch(config)# logging console
```

Command History

Version	History
1.00.001	This command was introduced

mailserver

Specify the IP address of mail server to be used for sending the lemail alerts messages. The no form resets the setting.

Command

mailserver *<ip-address>*

no mailserver

Syntax Description

ip-address	The IP address of mail server

Default Settings

No mail server is configured.

Command Modes

Global Configuration Mode

Example

```
switch(config)# mailserver 172.17.0.201
```

Command History

Version	History
1.00.001	This command was introduced

clear logs

Clear the system log buffers

Command

```
clear logs
```

Command Modes

Global Configuration Mode

Example

```
switch(config)# clear logs
```

Command History

Version	History
1.00.001	This command was introduced

show logging

To display the logging status, setting, and contents of buffer.

Command

```
show logging
```

Command Modes

Privileged EXEC Mode

Example

```
switch# show logging

System Log Information
----------------------
Syslog logging   : enabled(Number of messages 0)
Console logging  : disabled(Number of messages 0)
TimeStamp option : enabled
Trap logging     : Informational
Log server IP    : 20.0.0.1
Facility         : Default (local0)
Buffered size    : 50 Entries

LogBuffer(3 Entries, 612 bytes)
<130> Jan  1 00:07:47 2009:SYSTEM-2:System started up
<134> Jan  1 01:39:15 2009:CLI-6:Login failed : Login incorrect
ATE1 V1
<134> Jan  1 01:39:19 2009:CLI-6:User root logged in
```

Command History

Version	History
1.00.001	This command was introduced

show email alerts

To display the setting of mailserver.

Command

show email alerts

Command Modes

Privileged EXEC Mode

Example

```
switch# show email alerts
Mail server IP    : 172.17.0.201
```

Command History

Version	History
1.00.001	This command was introduced

Chapter 21
SNTP Command

SNTP Command List

clock set

To set the system time.

Command

clock set <*hh:mm:ss day month year***>**

Syntax Description

hh:mm:ss day month year	Specify the system time.

Command Modes

Privileged EXEC Mode

User Guidelines

The format of day, month and year are:
- Day: 1~31
- Month: Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec
- Year: yyyy

Example

```
switch# clock set 08:00:00 1 Jan 2010
```

Command History

Version	History
1.00.001	This command was introduced

set sntp

To enable/disable the Simple Network Time Protocol (SNTP) function, synchronizing the system time to the SNTP server..

Command

set sntp {enable | disable}

Syntax Description

enable	Enables the SNTP.
disable	Disables the SNTP.

Default Settings Disable

Command Modes Global Configuration Mode

Example

```
switch(config)# set sntp enable
```

Command History

Version	History
1.00.001	This command was introduced

set sntp dst

To enable/disable the Daylight Saving Time (DST) function of SNTP.

Command

set sntp dst {enable | disable}

Syntax Description

enable	Enables the DST function.
disable	Disable the DST function.

Default Settings Disable

Command Modes Global Configuration Mode

Example

```
switch(config)# set sntp dst enable
```

Command History

Version	History
1.00.001	This command was introduced

sntp dst

To configure the period of DST function.

Command

sntp dst from {january | february | march | april | may | june | july | august | september | october | november | december} *<day (1-31)> <hour (0-23)> <minute (0-59)>* **to {january | february | march | april | may | june | july | august | september | october | november | december}** *<day (1-31)> <hour (0-23)> <minute (0-59)>*

Syntax Description

from	Time that DST startis from
january ~ december	Specify the month that DST starts.
day (1-31)	Specify the day that DST starts.
hour (0-23)	Specify the hour that DST starts.
minute (0-59)	Specify the minute that DST starts.
to	Time that DST ends from
january ~ december	Specify the month that DST ends.
day (1-31)	Specify the day that DST ends.
hour (0-23)	Specify the hour that DST endts.
minute (0-59)	Specify the minute that DST ends.

Command Modes

Global Configuration Mode

Example

```
switch(config)# sntp dst from april 1 0 0 to September 1 0 0
```

Command History

Version	History
1.00.001	This command was introduced

sntp poll-interval

To set the time interval that SNTP synchronizes the time on SNTP server.

Command

sntp poll-interval *<seconds (30-86400)>*

Syntax Description

seconds (30-86400)	Specify the time interval that SNTP synchronizes the time on SNTP server.

Default Settings

30 seconds

Command Modes

Global Configuration Mode

Example

```
switch(config)# sntp poll-interval 3600
```

Command History

Version	History
1.00.001	This command was introduced

sntp primary-ip

To set the primary SNTP server IP address.

Command **sntp primary-ip** *<ip-address>*

Syntax Description		
	ip-address	Specify the IP address of the primary SNTP server.

Command Modes Global Configuration Mode

Example

```
switch(config)# sntp primary-ip 172.17.5.254
```

Command History	Version	History
	1.00.001	This command was introduced

sntp secondary-ip

To set the secondary SNTP server IP address.

Command **sntp secondary-ip** *<ip-address>*

Syntax Description		
	ip-address	Specify the IP address of thesecondary SNTP server.

Command Modes Global Configuration Mode

Example

```
switch(config)# sntp secondary-ip 172.17.5.253
```

Command History	Version	History
	1.00.001	This command was introduced

sntp timezone

To determine the time zone used in order to adjust the system clock.

Command **sntp timezone offset [-]** *<hour (0-13)> <minute (0-59)>*

Syntax Description		
	offset	The adjustment for time zone relative to GMT.
	-	To subtract time to GMT.
	hour (0-13)	Specify the number of hours different from GMT.
	minute (0-59)	Specify the number of minutes different from GMT.

Command Modes Global Configuration Mode

Example

```
switch(config)# sntp timezone offset – 8 0
```

Command History

Version	History
1.00.001	This command was introduced

show clock

To display the system date and time.

Command

```
show clock
```

Command Modes

Privileged EXEC Mode

Example

```
switch# show clock

Wed Dec 23 18:04:11 2009
```

Command History

Version	History
1.00.001	This command was introduced

show sntp

To display current SNTP settings.

Command

```
show sntp
```

Command Modes

Privileged EXEC Mode

Example

```
switch# show sntp

SNTP Information
-----------------------------------------
SNTP status        : Disabled
Poll interval(Sec)  : 30 sec.
Primary server IP   : 0.0.0.0
Secondary server IP : 0.0.0.0
Current Time       : 01 Jan 2009 00:36:47
Time Zone offset : +00:00

SNTP DST status  : Disabled
DST from        : Jan 01 00:00
DST to          : Jan 01 00:00
```

Command History

Version	History
1.00.001	This command was introduced

Chapter 22
Configuration Command

Configuration Command List

write

To save the running configuration.

Command

write { *flash:filename* | *startup-config* | *tftp://ip-address/filename* }

Syntax Description

flash:filename	Write to a designated flash driver with designated file name.
startup-config	Write to start up configuration.
tftp://ip-address/filename	Write to a remote TFTP site with designated file name.

Command Modes

Privileged EXEC Mode

Example

```
switch# write start-config
```

Command History

Version	History
1.00.001	This command was introduced

copy startup-config

To backup the startup configuration to NV-RAM or a remote site.

Command

copy startup-config { *flash: filename* | *tftp://ip-address/filename* }

Syntax Description

flash:filename	Copy to a designated flash driver with designated file name.
tftp://ip-address/filename	Copy to a remote TFTP site with designated file name.

Command Modes

Privileged EXEC Mode

Example

```
switch# copy startup-config flash:backupstarup
```

Command History

Version	History
1.00.001	This command was introduced

copy

To replace the startup configuration by a another configuration file in remote TFTP site or NV-RAM.

Command

copy { *tftp://ip-address/filename* **startup-config |** *flash: filename* **startup-config }**

Syntax Description

tftp://ip-address /filename **startup-config**	Specify the URL and file name of the remote configuration file.
flash: filename **startup-config**	Specify the driver and file name of the local configuration file.

Command Modes

Privileged EXEC Mode

Example

```
switch# copy flash:backupstarup startup-config
```

Command History

Version	History
1.00.001	This command was introduced

erase

To reset the startup configuration, NV-RAM or the configuration file in flash to default value.

Command

erase { startup-config | nvram: | *flash:filename***}**

Syntax Description

startup-config	To reset startup configuration to default.
nvram:	To reset the NV-RAM to default.
flash:filename	To reset the configutation file in flash to default.

Command Modes

Privileged EXEC Mode

Example

```
switch# erase startup-config
```

Command History

Version	History
1.00.001	This command was introduced

Chapter 23
Firmware Upgrade Command

Firmware Upgrade Command List

- archive download-sw /overwrite

archive download-sw /overwrite

To download the image from a TFTP server.

Command

archive download-sw /overwrite *tftp://ip-address/filename*

Syntax Description		
	tftp://ip-address /filename	Specify the URL of the image file.

Command Modes

Privileged EXEC Mode

Example

```
switch# archive download-sw /overwrite
tftp://172.17.5.111/image.hex
```

Command History	Version	History
	1.00.001	This command was introduced

Chapter 24
Reboot Command

Reboot Command List

reload

Reboot the Switch

Command **reload**

Command Modes Privileged EXEC Mode

Example

```
switch# reload
```

Command History

Version	History
1.00.001	This command was introduced

Note If the Switch reboots without write the running configurations, the last configuration wrote in NV-RAM will be loaded.

Chapter 25
Port Manager Command

Port Manager Command List

monitor session

To enable and configure the port mirroring function.

Command

```
monitor session [session_number 1-1] { destination interface
<interface-type>  <interface-id>  |  source  interface
<interface-type> <interface-id> { rx | tx | both } }

no monitor session [session_number 1-1] { destination interface
<interface-type>  <interface-id>  |  source  interface
<interface-type> <interface-id> }
```

Syntax Description

session_number 1-1	Specify the ID of the mirror session.
destination interface *interface-type interface-id*	Specify the destination port of the mirror session. Interface-type including *Fa* (Fast Ethernet) or *Gi* (Gigabit Ethernet). Interface-id is slot/port number.
source interface *interface-type interface-id*	Specify the source port of the mirror session. Interface information including interface-type: *Fa* (Fast Ethernet) or *Gi* (Gigabit Ethernet), and slot/port number.
rx	Monitoring the traffic received from the source port.
tx	Monitoring the traffic transmitted from the source port.
both	Monitoring the traffic both received and transmitted from the source port.

Default Settings

Disable

Command Modes Global Configuration Mode

User Guidelines
1. Using no form to disable the port mirroring function.
2. Destination port and source port have to be counfigured separately.
3. A port-channel can be mirrored, however, a port-channel port cannot.

Example
```
switch(config)# monitor session 1 destination interface fa 0/1
switch(config)# monitor session 1 source interface fa 0/2 both
```

Command History

Version	History
1.00.001	This command was introduced

negotiation

To enable auto-negotiation function to ports.

Command

negotiation

no negotiation

Command Modes Interface Configuration Mode

User Guidelines The configured port speed, duplex mode, and flow control only take effect when auto-negotiation disabled.

Example
```
switch(config-if)# no megotiation
```

Command History

Version	History
1.00.001	This command was introduced

speed

To set the port speed.

Command

speed { 10 | 100 | 1000 }

Syntax Description

10	Port runs at 10Mbps.
100	Port runs at 100Mbps.
1000	Port runs at 1000Mbps.

Default Settings The N-way result with link partner.

Command Modes Interface Configuration Mode

User Guidelines

The configured port speed and duplex settings only takes effect when auto-negotiation disabled.

Example

```
switch(config-if)# speed 100
```

Command History

Version	History
1.00.001	This command was introduced

duplex

To set the port duplex mode.

Command

```
duplex { full | half }
```

Syntax Description

full	Port runs at full duplex mode.
half	Port runs at half duplex mode.

Default Settings

Full

Command Modes

Interface Configuration Mode

Example

```
switch(config-if)# duplex half
```

Command History

Version	History
1.00.001	This command was introduced

flowcontrol

To enable/disable 802.3x flow control on ports.

Command

```
flowcontrol { on | off }
```

Syntax Description

on	Enable flow control.
off	Disable flow control.

Default Settings

Off

Command Modes

Interface Configuration Mode

Example

```
switch(config-if)# flowcontrol on
```

Command History

Version	History
1.00.001	This command was introduced

mdi

To set MDI or MDIX mode for ports.

Command

mdi { auto | mdi | mdix }

Syntax Description

auto	Port performs the auto MDI/MDIX function.
mdi	Port fixed at MDI mode.
mdix	Port fixed at MDIX mode.

Default Settings

Auto

Command Modes

Interface Configuration Mode

Example

```
switch(config-if)# mdi mdi
```

Command History

Version	History
1.00.001	This command was introduced

show flow-control

To display the flow control settings and statistics of interfaces.

Command

show flow-control [interface *<interface-type> <interface-id>***]**

Syntax Description

interface *interface-type interface-id*	Specify which interface to show flow-control settings. Interface-type including *Fa* (Fast Ethernet) or *Gi* (Gigabit Ethernet). Interface-id is slot/port number.

Command Modes

Privileged EXEC Mode

Example

```
switch# show flow-control int fa 0/2

Port Tx FlowControl Rx FlowControl  Tx Pause RxPause
---- -------------- --------------- -------- --------
Fa0/2 off            off             0        0
```

Command History

Version	History
1.00.001	This command was introduced

show mdi-mdix

To display the MDI/MDIX setting on ports.

Command

show mdi-mdix [interface *<interface-type> <interface-id>***]**

Syntax Description

interface *interface-type interface-id*	Specify which interface to show MDI/MDIX setting Interface-type including *Fa* (Fast Ethernet) or *Gi* (Gigabit Ethernet). Interface-id is slot/port number.

Command Modes

Privileged EXEC Mode

User Guidelines

System will disply MDI/MDIX setting for all ports when executing the command without port parameter.

Example

```
switch# show mdi-mdix

Fa0/1   AUTO/MDI/MDIX is auto
Fa0/2   AUTO/MDI/MDIX is auto
Fa0/3   AUTO/MDI/MDIX is auto
Fa0/4   AUTO/MDI/MDIX is auto
Fa0/5   AUTO/MDI/MDIX is auto
Fa0/6   AUTO/MDI/MDIX is auto
Fa0/7   AUTO/MDI/MDIX is auto
Fa0/8   AUTO/MDI/MDIX is auto
Fa0/9   AUTO/MDI/MDIX is auto
Fa0/10  AUTO/MDI/MDIX is auto
Fa0/11  AUTO/MDI/MDIX is auto
Fa0/12  AUTO/MDI/MDIX is auto
Fa0/13  AUTO/MDI/MDIX is auto
Fa0/14  AUTO/MDI/MDIX is auto
Fa0/15  AUTO/MDI/MDIX is auto
Fa0/16  AUTO/MDI/MDIX is auto
Fa0/17  AUTO/MDI/MDIX is auto
Fa0/18  AUTO/MDI/MDIX is auto
Fa0/19  AUTO/MDI/MDIX is auto
Fa0/20  AUTO/MDI/MDIX is auto
Fa0/21  AUTO/MDI/MDIX is auto
Fa0/22  AUTO/MDI/MDIX is auto
Fa0/23  AUTO/MDI/MDIX is auto
Fa0/24  AUTO/MDI/MDIX is auto
Gi0/1   AUTO/MDI/MDIX is auto
Gi0/2   AUTO/MDI/MDIX is auto
Gi0/3   AUTO/MDI/MDIX is auto
Gi0/4   AUTO/MDI/MDIX is auto
```

Command History

Version	History
1.00.001	This command was introduced

show port-monitoring

To display the port monitoring settings.

Command **show port-monitoring**

Command Modes Privileged EXEC Mode

Example

```
switch# show port-monitoring

Port Monitoring  is enabled
Monitor Port : Fa0/9

Port       Ingress-Monitoring    Egress-Monitoring
----       ------------------    -----------------
Fa0/1      Enabled               Enabled
Fa0/2      Disabled              Disabled
Fa0/3      Disabled              Disabled
Fa0/4      Disabled              Disabled
Fa0/5      Disabled              Disabled
```

Command History

Version	History
1.00.001	This command was introduced

Chapter 26
VLAN Command

VLAN Command List

vlan

To create a VLAN or enter a VLAN interface configured.

Command

vlan *<vlan-id(1-4094)>*

no vlan *<vlan-id(1-4094)>*

Syntax Description

vlan-id(1-4094)	Specify the VLAN ID to create or enter.

Command Modes

Global Configuration Mode

User Guidelines

Using no form to delete a VLAN.

Example

```
switch(config)# vlan 100
switch(config-vlan)#
```

Command History

Version	History
1.00.001	This command was introduced

switchport acceptable-frame-type

To configure the acceptable frame type of a port.

Command

switchport acceptable-frame-type {all | tagged | untaggedAndPrioritytagged}

no switchport acceptable-frame-type

Syntax Description

all	Accepts all kinds of frames.
tagged	Accepts only tagged frames
untaggedAndPrioritytagged	Accepts only untagged frames and frames with priority tag.

Default Settings

all

Command Modes

Interface Configuration Mode

Example

```
switch(config-if)# switchport acceptable-frame-type tagged
```

Command History

Version	History
1.00.001	This command was introduced

switchport ingress-filter

To filter all ingress packets which do not carry the same VLAN tag with the VLAN membership of the port.

Command

switchport ingress-filter

no switchport ingress-filter

Default Settings

Disable

Command Modes

Interface Configuration Mode

User Guidelines

Using no form to disable the ingress filtering of the port

Example

```
switch(config-if)# switchport ingress-filter
```

Command History

Version	History
1.00.001	This command was introduced

switchport pvid

To set the port VLAN ID of the port, all ingress untagged or priority tagged packet from this port will be assign to this VLAN.

Command

switchport pvid *<vlan-id(1-4094)>*

no switchport pvid

Syntax Description	*vlan-id(1-4094)*	Specify the PVID of the port.

Default Settings

1

Command Modes

Interface Configuration Mode

Example

```
switch(config-if)# switchport pvid 100
```

Command History	Version	History
	1.00.001	This command was introduced

ports

To apply the VLAN membership to ports or port-channels.

Command

ports ([*<interface-type> <0/a-b,0/c,...>***] [***<interface-type> <0/a-b,0/c,...>***] [port-channel** *<a,b,c-d>***]) [untagged (***<interface-type> <0/a-b,0/c,...>** **[***<interface-type> <0/a-b,0/c,...>***] [port-channel** *<a,b,c-d>***] [all])] [forbidden** *<interface-type> <0/a-b,0/c,...>* **[***<interface-type> <0/a-b,0/c,...>***] [port-channel** *<a,b,c-d>***]] [name** *<vlan-name>***]**

Syntax Description		
	interface-type 0/a-b,0/c,...	Specify the ports to apply the VLAN membership. Interface-type including *Fa* (Fast Ethernet) or *Gi* (Gigabit Ethernet). Interface-id is slot/port number.
	port-channel *a,b,c-d*	Specify the port-channels to apply the VLAN membership.
	untagged	Apply untagged membership to interfaces.
	all	Apply untagged membership to all interfaces.
	forbidden	Apply forbidden membership to interfaces.
	name *vlan-name*	Specify the name of this VLAN.

Default Settings

The default port membership is tagged.

Command Modes

Config-vlan Mode

User Guidelines

The untagged port must be the subset of member port.

Example

```
switch(config-vlan)# ports fa 0/1-5 untagged fa 0/5 forbidden
fa 0/7 name trendnet
```

Command History	Version	History
	1.00.001	This command was introduced

debug vlan

To enable the debug mode for VLAN.

Command

debug vlan { global | [{fwd | priority | redundancy} [initshut] [mgmt] [data] [ctpl] [dump] [os] [failall] [buffer] [all]]}

no debug vlan { global | [{fwd | priority | redundancy} [initshut] [mgmt] [data] [ctpl] [dump] [os] [failall] [buffer] [all]]}

Syntax Description

global	Displays the global debug messages for multiple instances.
fwd	Displays the forwarding debug messages.
priority	Displays the VLAN priority debug messages.
redundancy	Displays the redundancy related debug messages.
initshut	Displays the initial and shutdown debug messages.
mgmt	Displays the management related debug messages.
data	Displays the data path debug messages.
ctpl	Displays the control plan debug messages.
dump	Displays the packet dump debug messages.
os	Displays the debug messages for all resources except buffer.
failall	Displays the all failure messages.
buffer	Displays the buffer debug messages.
all	Displays all debug messages.

Default Settings

Disable

Command Modes

Privileged EXEC Mode

User Guidelines

Using no form the disable debug mode.

Example

```
switch# debug vlan all
```

Command History

Version	History
1.00.001	This command was introduced

show vlan

To display the VLAN member port information and VLAN number.

Command

show vlan [brief | id *<vlan-range>* **| summary]**

Syntax Description

brief	Display the brief of VLAN information.
id *<vlan-range>*	Limited a range of VLAN to display the information. The vlan-range format is a-b, b should be larger than a.
summary	Display the number of VLAN.

Command Modes

Privileged EXEC Mode

User Guidelines

System will display all the VLAN brief information when executing the command without any parameter.

Example

Single Instance:

```
switch# show vlan brief

Vlan database
-------------
Vlan ID           : 1
Member Ports       : Fa0/1, Fa0/2, Fa0/3, Fa0/4, Fa0/5, Fa0/6
                    Fa0/7, Fa0/8, Fa0/9, Fa0/10, Fa0/11, Fa0/12
                    Fa0/13, Fa0/14, Fa0/15, Fa0/16, Fa0/17,
                    Fa0/18, Fa0/19, Fa0/20, Fa0/21, Fa0/22,
                    Fa0/23, Fa0/24
                    Gi0/1, Gi0/2, Gi0/3, Gi0/4
Untagged Ports     : Fa0/1, Fa0/2, Fa0/3, Fa0/4, Fa0/5, Fa0/6
                    Fa0/7, Fa0/8, Fa0/9, Fa0/10, Fa0/11, Fa0/12
                    Fa0/13, Fa0/14, Fa0/15, Fa0/16, Fa0/17,
                    Fa0/18, Fa0/19, Fa0/20, Fa0/21, Fa0/22,
                    Fa0/23, Fa0/24
                    Gi0/1, Gi0/2, Gi0/3, Gi0/4
Forbidden Ports    : None
Name               :
Status             : Permanent
------------------------------------------------------

switch# show vlan summary

Number of vlans : 1
```

Multiple Instance:

```
switch# show vlan

Switch - default

Vlan database
-------------
Vlan ID : 1
Member Ports : Gi0/1
Untagged Ports : Gi0/1
Forbidden Ports : None
Name :
Status : Permanent
------------------------------------------------------

Switch - cust1

Vlan database
-------------
Vlan ID : 1
Member Ports : Fa0/1, Fa0/2, Fa0/3, Fa0/4, Fa0/5
Untagged Ports : Fa0/1, Fa0/2, Fa0/3, Fa0/4, Fa0/5
Forbidden Ports : None
Name :
Status : Permanent
------------------------------------------------------
Vlan ID : 2
Member Ports : Gi0/1
Untagged Ports : None
Forbidden Ports : None
```

```
Name :
Status : Dynamic Gvrp
------------------------------------------------
```

Command History

Version	History
1.00.001	This command was introduced

show vlan device info

To display the VLAN settings and detailed information of the device.

Command

```
show vlan device info
```

Command Modes

Privileged EXEC Mode

Example

Single Instance:

```
switch# show vlan device info

Vlan device configurations
--------------------------
Vlan Status                    : Enabled
Vlan Oper status               : Enabled
Gvrp status                    : Disabled
Gvrp Oper status               : Disabled
Bridge Mode                    : Customer Bridge
Traffic Classes                : Enabled
Vlan Operational Learning Mode   : IVL
Version number                 : 1
Max Vlan id                    : 4095
Max supported vlans            : 256
```

Multiple Instance:

```
switch# show vlan device info

Switch default

Vlan device configurations
--------------------------
Vlan Status : Enabled
Vlan Oper status : Enabled
Gvrp status : Enabled
Gmrp status : Disabled
Gvrp Oper status : Enabled
Gmrp Oper status : Disabled
Mac-Vlan Status : Disabled
Protocol-Vlan Status : Enabled
Bridge Mode : Provider Edge
Bridge
Traffic Classes : Enabled
Vlan Operational Learning Mode : IVL
Version number : 1
Max Vlan id : 4094
Max supported vlans : 1024
```

Command History

Version	History
1.00.001	This command was introduced

show vlan port config

To display the VLAN configurations of ports.

Command

show vlan port config [{port *<interface-type> <interface-id>***}]**

Syntax Description

port *interface-type interface-id*	Specify which port to show VLAN configurations. Interface-type including *Fa* (Fast Ethernet) or *Gi* (Gigabit Ethernet). Interface-id is slot/port number.

Command Modes Privileged EXEC Mode

User Guidelines System will display VLAN configurations for all port when executing the command without a port parameter.

Example

Single Instance:

```
switch# show vlan port config port fa 0/1

Vlan Port configuration table
------------------------------
Port Fa0/1
 Port Vlan ID                    : 1
 Port Acceptable Frame Type        : Admit All
 Port Ingress Filtering           : Enabled
 Port Mode                       : Hybrid
 Port Gvrp Status                 : Enabled
 Port Gvrp Failed Registrations     : 0
 Gvrp last pdu origin             : 00:00:00:00:00:00
 Port Restricted Vlan Registration   : Disabled
 Default Priority                : 0
 ------------------------------------------------------
```

Multiple Instance:

```
switch# show vlan port config

Switch - default

Vlan Port configuration table
------------------------------
Port Fa0/1
Port Vlan ID : 1
Port Acceptable Frame Type : Admit All
Port Ingress Filtering : Disabled
Port Mode : Hybrid
Port Gvrp Status : Enabled
Port Gmrp Status : Enabled
Port Gvrp Failed Registrations : 0
Gvrp last pdu origin : 00:00:00:00:00:00
Port Restricted Vlan Registration : Disabled
Port Restricted Group Registration : Disabled
Mac Based Support : Disabled
Port-and-Protocol Based Support : Enabled
Default Priority : 0
------------------------------------------------------

Switch - cust1

Vlan Port configuration table
------------------------------
Port Fa0/2
Port Vlan ID : 20
Port Acceptable Frame Type : Admit All
Port Ingress Filtering : Disabled
Port Mode : Hybrid
Port Gvrp Status : Enabled
Port Gmrp Status : Enabled
Port Gvrp Failed Registrations : 0
Gvrp last pdu origin : 00:00:00:00:00:00
Port Restricted Vlan Registration : Disabled
Port Restricted Group Registration : Disabled
Mac Based Support : Disabled
Port-and-Protocol Based Support : Enabled
```

```
Default Priority : 0
-------------------------------------------------------

Port Fa0/3
Port Vlan ID : 1
Port Acceptable Frame Type : Admit All
Port Ingress Filtering : Disabled
Port Mode : Hybrid
Port Gvrp Status : Enabled
Port Gmrp Status : Enabled
Port Gvrp Failed Registrations : 0
Gvrp last pdu origin : 00:25:64:93:1c:35
Port Restricted Vlan Registration : Disabled
Port Restricted Group Registration : Disabled
Mac Based Support : Disabled
Port-and-Protocol Based Support : Enabled
Default Priority : 0
-------------------------------------------------------
```

Command History

Version	History
1.00.001	This command was introduced

Chapter 27
Dynamic VLAN Command

Dynamic VLAN Command List

set gvrp

To global enable/disable GVRP function.

Command

```
set gvrp { enable | disable }
```

Syntax Description

enable	Enables GVRP globally.
disable	Disable GVRP globally.

Default Settings

Enable

Command Modes

Global Configuration Mode

Example

```
switch(config)# set gvrp disable
```

Command History

Version	History
1.00.001	This command was introduced

set port gvrp

To enable/disable gvrp on specific ports.

Command

set port gvrp *<interface-type> <interface-id>* **{ enable | disable }**

Syntax Description

interface-type interface-id	Specify which port to enable GVRP function. Interface-type including *Fa* (Fast Ethernet) or *Gi* (Gigabit Ethernet). Interface-id is slot/port number.
enable	Enables GVRP on the port.
disable	Disables GVRP on the port.

Default Settings

Enable

Command Modes

Global Configuration Mode

User Guidelines

If port GVRP is disabled, but global GVRP is enabled, any GVRP packet received by this port will be discarded and no GVRP registrations will be propagated from other ports

Example

```
switch(config)# set port gvrp fa 0/1 disable
```

Command History

Version	History
1.00.001	This command was introduced

set garp timer

To set the GARP timers on an interface.

Command

set garp timer {join *<time in milli seconds(10-1073741810)>* **| leave** *<time in milli seconds(30-2147483630)>* **| leaveall***<time in milli seconds(40-2147483640)>***}**

Syntax Description

join *<time in milli seconds(10-1073741810)>*	Specify the join time of GARP.
leave *<time in milli seconds(30-2147483630)>*	Specify the leave time of GARP.
leaveall*<time in milli seconds(40-2147483640)>*	Specify the leaveall time of GARP.

Default Settings

Join - 20
Leave - 60
Leaveall - 100

Command Modes

Interface Configuration Mode

User Guidelines

1. Leave timer must be greater than 2 times join time.
2. Leaveall time must be greater than Leave time

Example

```
switch(config-if)# set garp timer join 50
```

Command History

Version	History
1.00.001	This command was introduced

vlan restricted

To enable/disable the restricted VLAN on an interface.

Command

vlan restricted {enable | disable}

Syntax Description

enable	Enalbes VLAN restriction.
disable	Disables VLAN restriction.

Default Settings

Disable

Command Modes

Interface Configuration Mode

User Guidelines

When a port enables VLAN restriction, only static configured VLAN can be learnt from this interface.

Example

```
switch(config-if)# vlan restricted enable
```

Command History

Version	History
1.00.001	This command was introduced

shutdown garp

To shutdown GARP function.

Command

shutdown garp

no shutdown garp

Default Settings

Enable

Command Modes

Global Configuration Mode

User Guidelines

1. GARP cannot be activated if VLAN is shutdown.
2. GARP cannot be shutdown if GVRP or GMRP is activated.

Example

```
switch(config)# shutdown garp
```

Command History

Version	History
1.00.001	This command was introduced

debug garp

To enable the debug mode of GARP function.

Command

debug garp { global | [{protocol | gvrp | redundancy} [initshut] [mgmt] [data] [ctpl] [dump] [os] [failall] [buffer] [all]]}

no debug garp { global | [{protocol | garp | redundancy} [initshut] [mgmt] [data] [ctpl] [dump] [os] [failall] [buffer] [all]]

Syntax Description

global	Displays the global GARP debug messages for multiple instances.
protocol	Displays the protocol related debug messages.
Gvrp	Displays the GVRP related debug messages.
Redundancy	Displays the redundancy related debug messages.
Initshut	Displays the initial and shutdown debug messages.
Mgmt	Displays the management related debug messages.
Data	Displays the data path debug messages.
Ctpl	Displays the control plane debug messages.
dump	Displays the packet dump debug messages.
Os	Displays the debug messages for all resources except buffer.
Failall	Displays the all failure messages.
Buffer	Displays the buffer debug messages.
all	Displays all debug messages.

Default Settings

Disable

Command Modes

Privileged EXEC Mode

Example

```
switch#
```

Command History

Version	History
1.00.001	This command was introduced

show garp timer

To display the port timer settings.

Command

show garp timer [{ port *<interface-type> <interface-id>***}]**

Syntax Description

port	Specify which port to show GVRP timer setting.
interface-type *interface-id*	Interface-type including *Fa* (Fast Ethernet) or *Gi* (Gigabit Ethernet). Interface-id is slot/port number.

Command Modes

Privileged EXEC Mode

User Guidelines

System will display timer settings for all port when executing the command without a port parameter.

Example

```
switch# show garp timer port fa 0/1

Garp Port Timer Info (in milli seconds)
---------------------------------------

Port     Join-time      Leave-time      Leave-all-time
-----    ---------      ----------      --------------
Fa0/1    200            600             10000
```

Command History

Version	History
1.00.001	This command was introduced

Chapter 28
RSTP Command

RSTP Command List

spanning-tree

To enable spanning tree function.

Command

spanning-tree

no spanning-tree

Command Modes

Global Configuration Mode

User Guidelines

Using no form to disable STP.

Example

```
switch(config)# spanning-tree
```

Command History

Version	History
1.00.001	This command was introduced

spanning-tree compatibility

To set the spanning tree compatibility version.

Command

spanning-tree compatibility {stp|rst|mst}

no spanning-tree compatibility

Syntax Description

stp	Compatible wirh STP.
rst	Compatible with RSTP.
mst	Compatible with MSTP.

Default Settings

rst

Command Modes

Global Configuration Mode

User Guidelines

Using no form to reset the STP compatibility to default.

Example

```
switch(config)#  spanning-tree compatibility stp
```

Command History

Version	History
1.00.001	This command was introduced

spanning-tree mode

To choose the spanning tree opreation mode.

Command

spanning-tree mode {mst|rst}

Syntax Description

mst	Operates with MSTP mode.
rst	Operates with RSTP mode

Default Settings

rst

Command Modes

Global Configuration Mode

User Guidelines

If the configured mode is not the same with current running mode, spanning tree will be shutdown and restart.

Example

```
switch(config)# spanning-tree mode mst

switch(config)# spanning-tree mode rst
Spanning Tree protocol enabled is MST. Now MST is being shutdown
and RST is being enabled
```

Command History

Version	History
1.00.001	This command was introduced

spanning-tree pathcost dynamic

To enable the dynamic pathcost according to the port speed..

Command

spanning-tree pathcost dynamic

no spanning-tree pathcost dynamic

Default Settings

Disable

Command Modes

Global Configuration Mode

User Guidelines

1. If the cost has been configured on a CIST or a RSTP interface, then this command won't take effect on those interfaces.
2. If the cost has been configured on a port of MST instance, then this command won't take effect on that instance. However, the pathcost of all the other instances on the same port will still be calculated dynamically.
3. Using no form to disable the dynamic pathcost function.

Example

```
switch(config)# spanning-tree pathcost dynamic
```

Command History

Version	History
1.00.001	This command was introduced

spanning-tree transmit hold-count

To set a hold counter to limit maximum transmission rate of the Switch.

Command

spanning-tree transmit hold-count *<value (1-10)>*

no spanning-tree transmit hold-count

Syntax Description

value (1-10)	Specify the value of hold counter.

Default Settings

3

Command Modes

Global Configuration Mode

User Guidelines

Using no form to reset the hold count to default.

Example

```
switch(config)# spanning-tree transmit hold-count 10
```

Command History

Version	History
1.00.001	This command was introduced

spanning-tree timers

To set the timer of spanning tree.

Command

spanning-tree {forward-time *<seconds(4-30)>* **| hello-time** *<seconds(1-2)>* **| max-age** *<seconds(6-40)>***}**

no spanning-tree { forward-time | hello-time | max-age }

Syntax Description

forward-time *seconds(4-30)*	The time period that a port changes the STP state from blocking to forwarding.
hello-time *seconds(1-2)*	Time interval for a root bridge broadcasts the hello packets to other switches.
max-age *seconds(6-40)*	The maximum age for STP information learned from the network on any port before it is discarded

Default Settings

Forward-time - 15 seconds
Hello-time - 2 seconds
Max-age - 20 seconds

Command Modes

Global Configuration Mode

User Guidelines

1. The relationship between these timer must follow this formula:
2 x (Forward-time - 1) >= Max-age
Max-Age >= 2 x (Hello-time +1)
2. Using no form to reset the timer to default.

Example

```
switch(config)# spanning-tree forward-time 10
```

Command History

Version	History
1.00.001	This command was introduced

spanning-tree auto-edge

To enable the auto-detection of a port.

Command

spanning-tree auto-edge

no spanning-tree auto-edge

Default Settings

Enable

Command Modes

Interface Configuration Mode

User Guidelines

Using no form to disable the auto-edge function.

Example

```
switch(config-if)# spanning-tree auto-edge
```

Command History	Version	History
	1.00.001	This command was introduced

spanning-tree restricted-role

To enable the root guard function to prevent the port becoming a root port.

Command

spanning-tree restricted-role

no spanning-tree restricted-role

Default Settings

Disable

Command Modes

Interface Configuration Mode

User Guidelines

Using no form to disable the root guard function.

Example

```
switch(config-if)# spanning-tree restricted-role
```

Command History	Version	History
	1.00.001	This command was introduced

spanning-tree restricted-tcn

To enable the topology change guard function to prevent the topology change caused by this port.

Command

spanning-tree restricted-tcn

no spanning-tree restricted-tcn

Default Settings

Disable

Command Modes

Interface Configuration Mode

User Guidelines

Using no form to disable the topology change guard function.

Example

```
switch(config-if)# spanning-tree restricted-tcn
```

Command History	Version	History
	1.00.001	This command was introduced

spanning-tree interface attributes

To set detailed spanning attrebutes to ports.

Command

spanning-tree {cost *<value(0-200000000)>* **| disable | link-type {point-to-point | shared} | portfast | port-priority** *<value(0-240)>***}**

no spanning-tree {cost | disable | link-type | portfast | port-priority}

Syntax Description

cost *value(0-200000000)*	Specify the pathcost of this port.
disable	Disbles spanning tree on this port.
link-type point-to-point	Specify the port link type is point to point.
link-type shared	Specify the port connects to a LAN which has another bridge.
portfast	Specify the port connects to host
port-priority *value(0-240)*	Speficy the port STP priority.

Default Settings

Cost	-	2000000
Portfast	-	Not in portfast
Link-type	-	Shared
Port-priority	-	128

Command Modes

Interface Configuration Mode

User Guidelines

1. A portfast port will change to forwarding quickly during STP convergence, so that it can speed up the STP convergence.
2. Using no form to reset the port attributes to default.

Example

```
switch(config-if)# spanning-tree cost 100
```

Command History

Version	History
1.00.001	This command was introduced

shutdown spanning-tree

To shutdown the spanning tree function.

Command

shutdown spanning-tree

Command Modes

Global Configuration Mode

User Guidelines

MSTP and RSTP are exclusive to each other, so that spanning tree function must be shutdown when changing the STP operation mode.

Example

```
switch(config)# shutdown spanning-tree
```

Command History

Version	History
1.00.001	This command was introduced

clear spanning-tree counters

To clear the spanning tree counters.

Command

```
clear spanning-tree counters
```

Command Modes

Global Configuration Mode

Example

```
switch(config)# clear spanning-tree counters
```

Command History

Version	History
1.00.001	This command was introduced

debug spanning-tree

To enable the debug mode for spanning tree function.

Command

```
debug spanning-tree { global | { all | errors | init-shut |
management | memory | bpdu | events | timer | state-machine
{ port-info | port-recieve | port-role-selection |
role-transition | state-transition | protocol-migration |
topology-change | port-transmit | bridge-detection } |
redundancy | sem-variables}}

no debug spanning-tree {global | {all | errors | init-shut |
management | memory | bpdu |events | timer | state-machine
{port-info | port-recieve | port-role-selection |
role-transition | state-transition | protocol-migration |
topology-change | port-transmit | bridge-detection } redundancy
| sem-variables}}
```

Syntax Description

global	Displays the MSTP global debug messages.
all	Displays all RSTP/MSTP debug messages.
errors	Displays the error code debug messages.
init-shut	Displays the initial and shutdown debug messages.
management	Displays the management related debug messages.
memory	Displays the memory related debug messages.
bpdu	Displays the BPDU related debug messages.
events	Displays the events related debug messages.
timer	Displays the timer related debug messages.
state-machine	Displays the state-machine related debug messages.
port-info	Displays the port information messages.
port-recieve	Displays the port received messages.
port-role-selection	Displays the port role selection messages.
role-transition	Displays the role transition messages.
state-transition	Displays the state transition messages.
protocol-migration	Displays the protocol migration messages.
topology-change	Displays the topology change messages.
port-transmit	Displays the port transmission messages.
bridge-detection	Displays the bridge detection messages.
redundancy	Displays the redundancy related messages.
sem-variables	Displays the state-mechine vaiaables debug messages.

Default Settings

Disable

Command Modes

Privileged EXEC Mode

User Guidelines

Using no form to disable the debug mode.

Example

```
switch# debug spanning-tree all
```

Command History

Version	History
1.00.001	This command was introduced

show spanning-tree

To display the spanning port states, statistics, settings and detailed information.

Command

```
show spanning-tree [{ summary | blockedports | pathcost method }]
```

Syntax Description

summary	Display the summary of port states.
blockedports	Display current block port number.
pathcost method	Display the pathcost method setting.

Command Modes

Privileged EXEC Mode

Example

Single Instance:

```
switch# show spanning-tree
Root Id        Priority   32768
               Address    00:18:8b:bf:75:30
               Cost 0
               Port 0 [0]
               This bridge is the root
Max age 20 Sec, forward delay 15 Sec

Spanning tree Protocol Enabled
Bridge Id      Priority 32768
               Address 00:18:8b:bf:75:30
               Hello Time 2 sec, Max Age 20 sec, Forward Delay
15 sec
               Dynamic Path Cost is Enabled
Name    Role        State       Cost    Prio   Type
----    ----        -----       ----    ----   ------
Fa0/1   Designated  Forwarding  200000   128    SharedLan
Fa0/2   Designated  Forwarding  200000   128    SharedLan
Fa0/3   Designated  Forwarding  200000   128    SharedLan
Fa0/4   Disabled    Discarding  200000   128    SharedLan

switch# show spanning-tree summary

Spanning Tree port pathcost method is Long

Spanning tree enabled protocol is RSTP

RSTP Port Roles and States
Port-Index  Port-Role    Port-State   Port-Status
----------  ---------    ----------   -----------
1           Disabled     Discarding   Enabled
2           Disabled     Discarding   Enabled
3           Disabled     Discarding   Enabled
4           Root          Forwarding   Enabled

switch# show spanning-tree blockedports

Blocked Interfaces List:

The Number of Blocked Ports in the system is :1

switch# show spanning-tree pathcost method

Spanning Tree port pathcost method is Long
```

Multiple Instance:

```
switch# show spanning-tree
Root Id        Priority   32768
               Address    00:18:8b:bf:75:30
               Cost 0
               Port 0 [0]
               This bridge is the root
Max age 20 Sec, forward delay 15 Sec

MST00
Spanning tree Protocol Enabled
```

```
S-VLAN Component: MST00 is executing the mstp compatible
Multiple Spanning Tree Protocol
Bridge Id      Priority 32768
               Address 00:18:8b:bf:75:30
               Hello Time 2 sec, Max Age 20 sec, Forward Delay
15 sec
               Dynamic Path Cost is Enabled
Name    Role        State       Cost    Prio   Type
----    ----        -----       ----    ----   ------
Fa0/1   Designated  Forwarding  200000   128    SharedLan
Fa0/2   Designated  Forwarding  200000   128    SharedLan
Fa0/3   Designated  Forwarding  200000   128    SharedLan
Fa0/4   Disabled    Discarding  200000   128    SharedLan

switch# show spanning-tree summary

Switch - default

Spanning Tree port pathcost method is Long
Spanning tree enabled protocol is MSTP

MST00 Port Roles and States
Port-Index Port-Role Port-State Port-Status
---------- --------- ---------- -----------
49         Disabled  Forwarding Disabled

Switch - cust1

Spanning Tree port pathcost method is Long
Spanning tree enabled protocol is MSTP

MST00 Port Roles and States
Port-Index Port-Role   Port-State Port-Status
---------- ---------   ---------- -----------
1          Designated  Forwarding Enabled
2          Root        Forwarding Enabled
3          Designated  Forwarding Enabled
4          Disabled    Discarding Enabled

Switch - cust2

Spanning Tree port pathcost method is Long
Spanning tree enabled protocol is MSTP
MST00 Port Roles and States
Port-Index Port-Role   Port-State Port-Status
---------- ---------   ---------- -----------
5          Designated  Forwarding Enabled
6          Root        Forwarding Enabled
7          Alternate   Discarding Enabled
8          Disabled    Discarding Enabled
```

Command History

Version	History
1.00.001	This command was introduced

show spanning-tree active

To display the spanning tree information on active ports.

Command

```
show spanning-tree active [detail]
```

Syntax Description

detail	Display the details of spanning tree bridge.

Command Modes

Privileged EXEC Mode

Example

Single Instance:

```
switch# show spanning-tree active
Root Id   Priority 8192
          Address 00:74:24:00:01:00
          Cost 2000000
          Port Fa0/1
Hello Time 2 Sec, Max Age 20 Sec, Forward Delay 15 Sec

Spanning Tree Enabled Protocol RSTP
Bridge    Id Priority 32768
          Address 00:18:8b:bf:75:30
          Hello Time 2 sec, Max Age 20 sec, Forward Delay 15 sec
Name   Role   State        Cost     Prio  Type
----   ----   -----        ----     ----  ------
Fa0/1  Root   Forwarding   2000000  128   SharedLan

switch# show spanning-tree active detail

Spanning tree Protocol has been disabled
Bridge Identifier has priority 32768, Address 00:74:24:00:01:00
Configured Hello time 2 sec, Max Age 20 sec, Forward Delay 15
sec
Dynamic Path Cost Enabled
Number of Topology Changes 0
Time since topology Change 0 seconds ago
Transmit Hold-Count 6
 Max Age 20 Sec, Forward Delay 15 Sec
Hello Time 2 Sec
```

Multiple Instance:

```
switch# show spanning-tree active switch default

Switch default

Root Id    Priority 32768
           Address 00:51:02:03:04:05
           Cost 0
           Port 0 [0]
This bridge is the root
Max age 20 Sec, forward delay 15 Sec

MST00

MST00 is executing the mstp compatible Multiple Spanning Tree
Protocol
Bridge Id   Priority 32768
            Address 00:51:02:03:04:05
            Max age is 20 sec, forward delay is 15 sec
Name   Role   State        Cost     Prio  Type
----   ----   -----        ----     ----  ------
Fa0/1  Root   Forwarding   2000000  128   SharedLan
```

Command History

Version	History
1.00.001	This command was introduced

show spanning-tree bridge

To display the spanning tree bridge settings.

Command

show spanning-tree bridge [{ address | forward-time | hello-time | id |max-age | protocol | priority | detail }]

Syntax Description

address	Display the MAC address of spanning tree bridge.
forward-time	Display the current setting of spanning tree forward time.
hello-time	Display the current setting of spanning tree hello time.
id	Display the spanning tree bridge ID.
max-age	Display the current setting of spanning tree max-age.
protocol	Display the current setting of spanning tree protocol.
priority	Display the current setting of spanning tree bridge priority.
detail	Display the spanning tree bridge details.

Command Modes

Privileged EXEC Mode

Example

Single Instance:

```
switch# show spanning-tree bridge

Bridge ID              HelloTime MaxAge FwdDly Protocol
---------              --------- ------ ------ --------
80:00:00:74:24:00:01:00    20       2000   15     rstp

switch# show spanning-tree bridge address

Bridge Address is 00:74:24:00:01:00

switch# show spanning-tree bridge forward-time

Bridge Forward delay is  15 sec

switch# show spanning-tree bridge hello-time

Bridge Hello Time is 2 sec

switch# show spanning-tree bridge id

Bridge ID is 80:00:00:74:24:00:01:00

switch# show spanning-tree bridge max-age

Bridge Max Age is 20 sec

switch# show spanning-tree bridge protocol

Bridge Protocol Running is RSTP

switch# show spanning-tree bridge priority

Bridge Priority is 32768

switch# show spanning-tree bridge detail

Bridge Id   Priority 32768,
            Address 00:74:24:00:01:00
            Hello Time 2 sec, Max Age 20 sec, Forward Delay
            15 sec
```

Multiple Instance:

```
switch# show spanning-tree bridge

Switch - default
MST Instance Bridge ID              MaxAge FwdDly Protocol
------------ ---------              ------ ------ --------
MST00        80:00:00:74:24:00:01:00 20     15     mstp

Switch - cust1
MST Instance Bridge ID              MaxAge FwdDly Protocol
------------ ---------              ------ ------ --------
MST00        80:00:00:74:24:00:01:02 20     15     mstp

switch# show spanning-tree bridge address
Switch - default
```

```
MST00 00:74:24:00:01:00

Switch - cust1
MST00 00:74:24:00:01:02
```

Command History

Version	History
1.00.001	This command was introduced

show spanning-tree interface

To display the spanning tree states, statistics, settings information on a port.

Command

show spanning-tree interface *<interface-type> <interface-id>* **[{ cost | priority | portfast | rootcost | restricted-role | restricted-tcn | state | stats | detail }]**

Syntax Description

interface-type interface-id	Specify the information of which interface to display. Interface-type including *Fa* (Fast Ethernet), *Gi* (Gigabit Ethernet) or port-channel. Interface-id is slot/port number or port channel ID.
cost	Display the port cost.
priority	Display the port priority.
portfast	Display the portfast state.
rootcost	Display the rootcost.
restricted-role	Display the setting of restricted-role function.
restricted-tcn	Display the setting of restricted-tcn function.
state	Display the spanning tree state
stats	Display the spanning tree statistics
detail	Display the detailed information of port and root bridge.

Command Modes

Privileged EXEC Mode

User Guidelines

Example

Single Instance:

```
switch# show spanning-tree interface fa 0/1

Role   State       Cost     Prio  Type
----   -----       ----     ----  ----
Root   Forwarding  2000000  128   SharedLan

switch# show spanning-tree interface fa 0/1 cost

Port cost is 2000000

switch# show spanning-tree interface fa 0/1 priority

Port Priority is 128

switch# show spanning-tree interface fa 0/1 portfast

PortFast is enabled

switch# show spanning-tree interface fa 0/1 rootcost

Root Cost is 2000000

switch# show spanning-tree interface fa 0/1 restricted-role

Restricted Role is Enabled

swtich# show spanning-tree interface fa 0/1 restricted-tcn

Restricted TCN is Enabled

switch# show spanning-tree interface fa 0/1 state

Forwarding

switch# show spanning-tree interface fa 0/1 stats

Statistics for Port Fa0/1
Number of Transitions to forwarding State : 2
Number of RSTP BPDU Count received : 3384
Number of Config BPDU Count received : 18
Number of TCN BPDU Count received : 1
Number of RSTP BPDU Count Transmitted : 1470
Number of Config BPDU Count Transmitted : 22
Number of TCN BPDU Count Transmitted : 0
Number of Invalid BPDU Count Transmitted : 0
Port Protocol Migration Count : 1

switch# show spanning-tree interface fa 0/1 detail

Port 1 [Fa0/1] is Root , Forwarding
Port PathCost 2000000, Port Priority 128, Port Identifier 128.1
Designated Root has priority 8192, address 00:18:8b:bf:75:30
Designated Bridge has priority 8192, address 00:18:8b:bf:75:30
Designated Port Id is 128.1, Designated PathCost 0
No of Transitions to forwarding State :1
PortFast is disabled
Link Type is Shared
```

```
BPDUs : sent 1479 , recieved 3458

Multiple Instance:

switch# show spanning-tree interface fa 0/1

Switch - default
Role   State       Cost     Prio  Type
----   -----       ----     ----  ----
Root   Forwarding  2000000  128   SharedLan

switch# show spanning-tree interface fa 0/1 cost

Port cost is 2000000
Switch - default

switch# show spanning-tree interface fa 0/1 priority

Switch – default
Port Priority is 128

switch# show spanning-tree interface fa 0/1 portfast

Switch – default
PortFast is enabled

switch# show spanning-tree interface fa 0/1 rootcost

Switch – default
Root Cost is 2000000

switch# show spanning-tree interface fast 0/1 restricted-role

Switch – default
Restricted Role is Enabled

switch# show spanning-tree interface fast 0/1 restricted-tcn

Switch – default
Restricted TCN is Enabled
switch# show spanning-tree interface fa 0/1 state

Switch – default
Forwarding

switch# show spanning-tree interface fa 0/1 stats

Switch – default
Statistics for Port Fa0/1
Number of Transitions to forwarding State : 2
Number of RSTP BPDU Count received : 3384
Number of Config BPDU Count received : 18
Number of TCN BPDU Count received : 1
Number of RSTP BPDU Count Transmitted : 1470
Number of Config BPDU Count Transmitted : 22
Number of TCN BPDU Count Transmitted : 0
Number of Invalid BPDU Count Transmitted : 0
Port Protocol Migration Count : 1
```

```
switch# show spanning-tree interface fa 0/1 detail

Switch – default
Port 1 [Fa0/1] is Root , Forwarding
Port PathCost 2000000, Port Priority 128, Port Identifier 128.1
Designated Root has priority 8192, address 00:18:8b:bf:75:30
Designated Bridge has priority 8192, address 00:18:8b:bf:75:30
Designated Port Id is 128.1, Designated PathCost 0
No of Transitions to forwarding State :1
PortFast is disabled
Link Type is Shared
BPDUs : sent 1470 , recieved 3458
```

Command History

Version	History
1.00.001	This command was introduced

show spanning-tree root

To display the information of the spanning root bridge.

Command

show spanning-tree root [{ address | cost | forward-time | hello-time | id | max-age | port | priority | detail }]

Syntax Description

address	Display the MAC address of root bridge.
forward-time	Display the root cost value.
hello-time	Display the hello time setting.
id	Display the root bridge ID.
max-age	Disply the max age of root bridge.
port	Display the root port.
priority	Display the root priority.
detail	Display the detailed information of bridge.

Command Modes

Privileged EXEC Mode

Example

```
switch# show spanning-tree root

Root ID                 RootCost MaxAge FwdDly RootPort
-------                 -------------- ------ --------
80:00:08:00:1f:3f:73:26  0        20    15    0

switch# show spanning-tree root address

Root Bridge Address is 08:00:1f:3f:73:26

switch# show spanning-tree root cost

Root Cost is 2000000

switch# show spanning-tree root forward-time

Forward delay is 15 sec

switch# show spanning-tree root hello-time

Hello Time is 2 sec

switch# show spanning-tree root id

Root Bridge Id is 80:00:08:00:1f:3f:73:26

switch# show spanning-tree root max-age

Root MaxAge is 20

switch# show spanning-tree root port

Root Port is 1

switch# show spanning-tree root priority

Root Priority is 32768

switch# show spanning-tree root detail

We are the root of the Spanning Tree
Root Id Priority 32768
        Address 08:00:1f:3f:73:26
        Cost 0
        Port 0
Hello Time 2 Sec, Max Age 20 Sec, Forward Delay 15 Sec
```

Command History

Version	History
1.00.001	This command was introduced

Chapter 29
MSTP Command

MSTP Command List

spanning-tree priority

To set the bridge priority of spanning tree.

Command

spanning-tree [mst *<instance-id>*] **priority** *<value(0-61440)>*

no spanning-tree [mst *<instance-id(1-64)>*] **priority**

Syntax Description

mst *instance-id*	Specify the priority of which MST instance to configure.
priority *value(0-61440)*	Specify the bridge priority of spanning tree.

Default Settings

32768

Command Modes

Global Configuration Mode

User Guidelines

MST instance configuration is only available when MSTP is running.

Example

```
switch(config)# spanning-tree mst 10 priority 1
```

Command History

Version	History
1.00.001	This command was introduced

spanning-tree mst configuration

To enter MSTP Configuration Mode

Command **spanning-tree mst configuration**

Command Modes Global Configuration Mode

User Guidelines Spanning tree mode must be MST before entering the MSTP Configuration Mode.

Example
```
switch(config)# spanning-tree mst configuration
switch(config-mst)#
```

Command History

Version	History
1.00.001	This command was introduced

spanning-tree mst max-hops

To set the maximum hops permitted in MST

Command

spanning-tree mst max-hops *<value(6-40)>*

no spanning-tree mst max-hops

Syntax Description

value(6-40)	Specify the maximum hop number.

Default Settings 20

Command Modes Global Configuration Mode

User Guidelines Using no form to reset the maximum hop number to default.

Example
```
switch(config)# spanning-tree mst max-hops 6
```

Command History

Version	History
1.00.001	This command was introduced

spanning-tree mst max-instance

To set the maximum MST instance of the Switch.

Command

spanning-tree mst max-instance *<short(1-64)>*

no spanning-tree mst max-instance

Syntax Description

short(1-64)	Specify the max instance number of the Switch.

Default Settings 64

Command Modes Global Configuration Mode

User Guidelines Using no form to reset the max instance number to default.

Example

```
switch(config)# spanning-tree mst max-instance 16
```

Command History

Version	History
1.00.001	This command was introduced

instance

To assign VLAN range to a MST instance.

Command

instance *<instance-id(1-64)>* **vlan** *<vlan-range>*

no instance *<instance-id(1-64)>* **[vlan** *<vlan-range>***]**

Syntax Description

instance-id(1-64)	Specify which instance to configure.
vlan *vlan-range*	Specify which VLAN to map.

Default Settings Instance 0 – VLAN 1~4094

Command Modes MSTP Configuration Mode

User Guidelines Use no form to reset the VLAN mapping to default.

Example

```
switch(config-mst)# instance 1 vlan 1-100
```

Command History

Version	History
1.00.001	This command was introduced

name

To set the name for the MST reigon.

Command

name *<string(optional max Length)>*

no name

Syntax Description

string(optional max Length)	Specify the name of MST reigon.

Default Settings 00: 00: 00: 00: 00: 00

Command Modes MSTP Configuration Mode

User Guidelines Using no form the reset the name to default.

Example

```
switch(config-mst)# name trendnet
```

Command History

Version	History
1.00.001	This command was introduced

revision

To set the revision number for the MST reigon.

Command

revision *<value(0-65535)>*

no revision

Syntax Description

value(0-65535)	Specify the number of revision.

Default Settings 0

Command Modes MSTP Configuration Mode

User Guidelines Using no form to reset the revision number to default.

Example

```
switch(config-mst)# revision 1
```

Command History

Version	History
1.00.001	This command was introduced

spanning-tree mst hello-time

To set the MST hello time to a port.

Command

spanning-tree mst hello-time *<value(1-2)>*

no spanning-tree mst hello-time

Syntax Description

value(1-2)	Specify the hello time value of the port.

Default Settings 2 seconds

Command Modes Interface Configuration Mode

User Guidelines Use no form to reset the hello time value to default.

Example

```
switch(config-if)# spanning-tree mst hello-time 1
```

Command History

Version	History
1.00.001	This command was introduced

show spanning-tree mst

To display the information of MST instances.

Command

show spanning-tree mst [*<instance-id(1-64)>***] [detail]**

Syntax Description

instance-id(1-64)	Specify information of which MST instance to show.
detail	Display more details of MST instance information.

Command Modes Privileged EXEC Mode

User Guidelines System will display MST information for all instances when executing the command without instance-id parameter.

Example

```
switch# show spanning-tree mst 1

## MST01
Vlans mapped: 2
Bridge Address 00:50:ba:fd:51:49 Priority 32768
Root Address 00:50:ba:fd:51:49 Priority 32768
Root this switch for MST01
Interface Role Sts Cost Prio.Nbr Type
--------- ---- --- ---- -------- ----
Fa0/1 Master Forwarding 2000000 128.1 SharedLan

switch# show spanning-tree mst 1 detail

## MST01
Vlans mapped: 2
Bridge Address 00:50:ba:fd:51:49 Priority 32768
Root Address 00:50:ba:fd:51:49 Priority 32768
Root this switch for MST01
Fa0/1 of MST01 is Master , Forwarding
Port info port id 128.1 priority 128 cost 2000000
Designated root address 00:50:ba:fd:51:49 priority 32768 cost
0
Designated bridge address 00:50:ba:fd:51:49 priority 32768 port
id 128.1
```

Command History

Version	History
1.00.001	This command was introduced

show spanning-tree mst interface

To display the MSTP status, statistics and current setting on interfaces.

Command

show spanning-tree mst [*<instance-id(1-64)>***] interface** *<interface-type> <interface-id>* **[{ stats | hello-time | detail }]**

Syntax Description

instance-id(1-64)

interface *interface-type interface-id*	Specify which interface to show the multiple spanning tree information. Interface-type including *Fa* (Fast Ethernet), *Gi* (Gigabit Ethernet) or port-channel. Interface-id is slot/port number or port-channel ID.
stats	Display the BPDU statistic on this interface.
hello-time	Display the hello-time setting on the interface.
detail	Display details multiple spanning tree on the interface.

Command Modes

Privileged EXEC Mode

Example

```
switch# show spanning-tree mst 1 interface fa 0/1

Instance  Role    Sts         Cost    Prio.Nbr
--------  ----    ---         ----    --------
1         Master  Forwarding  2000000 128.1

switch# show spanning-tree mst 1 interface fa 0/1 stats

MST01 Bpdus sent 2, Received 0

switch# show spanning-tree mst 1 interface fa 0/1 hello-time

MST01 2

switch# show spanning-tree mst 1 interface fa 0/1 detail

Fa0/1 of MST01 is Master , Forwarding
Port info port id 128.1 priority 128 cost 2000000
Designated root address 00:50:ba:fd:51:49 priority 32768 cost
0
Designated bridge address 00:50:ba:fd:51:49 priority 32768 port
id 128.1
```

Command History

Version	History
1.00.001	This command was introduced

show spanning-tree mst configuration

To display current multiple spanning tree settings.

Command

show spanning-tree mst configuration

Command Modes

Privileged EXEC Mode

Example

Single Instance:

```
switch# show spanning-tree mst configuration

Name [trendnet]
Revision 2
Instance Vlans mapped
-------- ---------------------------------------------
0        1,3-1024,1025-2048,2049-3072,3073-4094
1        2
---------------------------------------------------------
```

Multiple Instance:

```
switch# show spanning-tree mst configuration

Switch - default
Name [trendnet1]
Revision 0
Instance Vlans mapped
-------- ---------------------------------------------
0        1-1024,1025-2048,2049-3072,3073-4094
---------------------------------------------------------
Switch - cust1
Name [trendnet2]
Revision 0
Instance Vlans mapped
-------- ---------------------------------------------
0        1-1024,1025-2048,2049-3072,3073-4094
---------------------------------------------------------
```

Command History

Version	History
1.00.001	This command was introduced

Chapter 30
Link Aggregation Command

Link Aggregation Command List

set port-channel

To enable or disable port channel function of the Switch.

Command

```
set port-channel { enable | disable }
```

Syntax Description

enable	Enables the port channel.
disable	Disables the port channel.

Default Settings

Disable

Command Modes

Global Configuration Mode

Example

```
switch(config)# set port-channel enable
```

Command History

Version	History
1.00.001	This command was introduced

lacp system-priority

To set the LACP priority of the Switch.

Command

```
lacp system-priority <0-65535>
no lacp system-priority
```

Syntax Description	*0-65535*	Specify the value of LACP system priority.

Default Settings 32768

Command Modes Global Configuration Mode

User Guidelines The system priority decides the standby or active links in a aggregation when the number of member port exceeds the maximum number of the etherchannel that Switch supported.

Example

```
switch(config)# lacp system-priority 1
```

Command History	Version	History
	1.00.001	This command was introduced

port-channel load-balance

To choose the load balance algorithm of the port-channel.

Command

port-channel load-balance {src-mac | dest-mac | src-dest-mac| src-ip | dest-ip | src-dest-ip} [*<port-channel-index(1-65535)>* **]**

no port-channel load-balance [*<port-channel-index(1-65535)>* **]**

Syntax Description	**src-mac**	Hashing according to the source MAC address of the packets.
	dest-mac	Hashing according to the destication MAC address of the packets.
	src-dest-mac	Hashing according to the source and destication MAC address of the packets.
	src-ip	Hashing according to the source IP address of the packets.
	dest-ip	Hashing according to the destication IP address of the packets.
	src-dest-ip	Hashing according to the source and destication IP address of the packets.
	port-channel-index(1-65535)	Specify which port channel to set the load balance algorithm.

Default Settings src-dest-mac

Command Modes Global Configuration Mode

User Guidelines Using no form to reset the load balance algorithm to default.

Example

```
switch(config)# port-channel load-balance src-dest-ip 1
```

Command History

Version	History
1.00.001	This command was introduced

channel-group

To join a port to a channel group.

Command

channel-group *<channel-group-number(1-65535)>* **mode {active | passive | on}**

no channel-group

Syntax Description

channel-group-number(1-65535)	Specify which channel group to configure.
mode active	Activates the LACP negotiation.
mode passive	LACP negotiation starts only when LACP packet is received.
mode on	Disables the LACP negotiation, using manual aggregation.

Command Modes

Interface Configuration Mode

User Guidelines

1. Port-channel group must be crested before assign port to a channel group.
2. The MTU of the port and channel group must be the same.

Example

```
switch(config-if)# channel-group 1 mode active
```

Command History

Version	History
1.00.001	This command was introduced

lacp port-priority

To set the LACP port priority of a port.

Command

lacp port-priority *<0-65535>*

no lacp port-priority

Syntax Description

0-65535	Specify the port priority of the port.

Default Settings

128

Command Modes

Interface Configuration Mode

User Guidelines

The port priority decides the standby or active links in a aggregation when the number of member port exceeds the maximum number of the etherchannel that Switch supported.

Example

```
switch(config-if)# lacp port-priority 1
```

Command History

Version	History
1.00.001	This command was introduced

lacp timeout

To choose the LACP timeout period when no packet receive from peer..

Command

lacp timeout {long | short }

no lacp timeout

Syntax Description

long	Specify a long time out value. LACP PDU will be sent every 30 seconds and LACP timeout value is 90 seconds
short	Specify a short time out value. LACP PDU will be sent every 1 seconds and LACP timeout value is 3 seconds

Default Settings

Long

Command Modes

Interface Configuration Mode

Example

```
switch(config-if)# lacp timeout short
```

Command History

Version	History
1.00.001	This command was introduced

lacp wait-time

The period that ports get aggregated after receiving LACP PDU.

Command

lacp wait-time *<0-10>*

no lacp wait-time

Syntax Description

0-10	Specify the wait time in seconds.

Default Settings

2 seconds

Command Modes

Interface Configuration Mode

Example

```
switch(config-if)# lacp wait-time 0
```

Command History

Version	History
1.00.001	This command was introduced

shutdown port-channel

To shutdown the port channel group.

Command

shutdown port-channel

no shutdown port-channel

Default Settings

Active

Command Modes

Global Configuration Mode

User Guidelines

Using no form to reactivate the port channel group.

Example

```
switch(config)# shutdown port-channel
```

Command History

Version	History
1.00.001	This command was introduced

show etherchannel

To display the information of port channel groups.

Command

show etherchannel [*<channel-group-number>* **{ detail | load-balance | port | port-channel | summary | protocol}]**

Syntax Description

channel-group-number	Specify the information of which port channel group to display.
detail	Displays the detailed information of the etherchannel.
load-balance	Displays the load-balance or frame-distribution scheme among ports in the port channel of the etherchannel.
port	Displays the port information of the etherchannel.
port-channel	Displays the port-channel of the etherchannel.
summary	Displays summary of the etherchannel.
protocol	Displays protocol used in the etherchannel.

Command Modes

Privileged EXEC Mode

User Guidelines

System will display the global information and the summary of all port channel groups when executing this command without any keyword.

Example

```
switch# show etherchannel

Port-channel Module Admin Status is enabled
Port-channel Module Oper Status is enabled
Port-channel System Identifier is  00:74:24:00:01:00

Maximum ports per Port Channel is 8 with maximum 8 active ports

              Channel Group Listing
              ---------------------
Group : 1
----------
Protocol : LACP

switch# show etherchannel 1 detail
Port-channel Module Admin Status is enabled
Port-channel Module Oper Status is enabled
Port-channel System Identifier is  00:74:24:00:01:00

Maximum ports per Port Channel is 8 with maximum 8 active ports
LACP System Priority: 32768

              Channel Group Listing
              ---------------------
Group: 1
----------
Protocol :LACP

              Ports in the Group
              ------------------

Port : Gi0/1
-------------

Port State = Down, Not in Bundle
Channel Group : 1
Mode : Active
Pseudo port-channel = Po1
LACP port-priority  = 128
LACP Wait-time  = 2 secs
LACP Port Identifier = 25
LACP Activity : Active
LACP Timeout : Long

Aggregation State : Aggregation, Defaulted

              LACP Port   Admin  Oper   Port    Port
Port     State   Priority    Key    Key    Number  State
-------------------------------------------------------------
Gi0/1    Down    128         1      1      0x19    0xa2

Port-channel : Po1
-------------------

Number of Ports = 1
HotStandBy port = null
Port state = Port-channel Ag-Not-Inuse
Protocol = LACP
MAC selection = Dynamic
```

```
Default Port = None

switch# show etherchannel 1 load-balance

              Channel Group Listing
              ---------------------
Group : 1
----------
Source & Destination MAC Address

switch# show etherchannel 1 port

              Channel Group Listing
              ---------------------
Group: 1
----------
Protocol :LACP

              Ports in the Group
              ------------------

Port : Gi0/1
-------------

Port State = Down, Not in Bundle
Channel Group : 1
Mode : Active
Pseudo port-channel = Po1
LACP port-priority  = 128
LACP Wait-time  = 2 secs
LACP Port Identifier = 25
LACP Activity : Active
LACP Timeout : Long

Aggregation State : Aggregation, Defaulted

              LACP Port   Admin  Oper   Port    Port
Port    State   Priority    Key    Key    Number  State
-----------------------------------------------------------
Gi0/1   Down    128         1      1      0x19    0xa2

switch# show etherchannel 1 port-channel

Port-channel Module Admin Status is enabled
Port-channel Module Oper Status is enabled
Port-channel System Identifier is  00:74:24:00:01:00

Maximum ports per Port Channel is 8 with maximum 8 active ports

              Channel Group Listing
              ---------------------
Group : 1
----------

             Port-channels in the group:
             ---------------------------

Port-channel : Po1
-------------------
```

```
Number of Ports = 1
HotStandBy port = null
Port state = Port-channel Ag-Not-Inuse
Protocol = LACP
MAC selection = Dynamic
Default Port = None

switch# show etherchannel 1 summary

Port-channel Module Admin Status is enabled
Port-channel Module Oper Status is enabled
Port-channel System Identifier is  00:74:24:00:01:00

Maximum ports per Port Channel is 8 with maximum 8 active ports

Flags:
D - down        P - in port-channel
I - stand-alone  S - suspended
H - Hot-standby (LACP only)

Number of channel-groups in use: 1
Number of aggregators: 1

Group  Port-channel   Protocol   Ports
------------------------------------------------------------
1     Po1(D)         LACP      Gi0/1(D)

switch# show etherchannel 1 protocol

               Channel Group Listing
               ---------------------
Group : 1
----------
Protocol : LACP
```

Command History

Version	History
1.00.001	This command was introduced

show lacp

To display the LACP port channel counters or neighbors information.

Command

show lacp [*<port-channel(1-65535)>***] { counters | neighbor [detail] }**

Syntax Description

port-channel (1-65535)	Specify the information of which port channel to display.
counters	Displays the traffic statistics.
neighbor	Displays the neighbot information.
detail	Displays the detailed neighbot information.

Command Modes Privileged EXEC Mode

Example

```
switch# show lacp 1 counters

          LACPDUs       LACPDUs
Port     Sent   Recv        Pkts Err
---------------------------------------------
Channel group: 1
------------------
Gi0/1     788   704          0       0
Gi0/2     636   596          0       0

switch# show lacp 1 neighbor

Flags:
A - Device is in Active mode
P - Device is in Passive mode

Channel group 1 neighbors

Port Gi0/1
----------
Partner System ID : 08:01:02:03:04:05
Flags : P
LACP Partner Port Priority : 128
LACP Partner Oper Key : 2
LACP Partner Port State : 0x3c
Port State Flags Decode
-------------------------
Activity : Passive
LACP Timeout : Long
Aggregation State : Aggregation, Sync, Collecting, Distributing

Port Gi0/2
----------
Partner System ID : 06:01:02:03:04:05
Flags : P
LACP Partner Port Priority : 128
LACP Partner Oper Key : 2
LACP Partner Port State : 0x3c
Port State Flags Decode
-------------------------
Activity : Passive
LACP Timeout : Long
Aggregation State : Aggregation, Sync, Collecting, Distributing
```

Command History

Version	History
1.00.001	This command was introduced

show interfaces etherchannel

To display the etherchannel information of a port.

Command

show interfaces [*<interface-type>* *<interface-id>* **] etherchannel**

Syntax Description

interface-type	Specify the information of which port to show.
interface-id	Interface-type including *Fa* (Fast Ethernet) or *Gi* (Gigabit Ethernet). Interface-id is slot/port number.

Command Modes

Privileged EXEC Mode

User Guidelines

System will display the etherchannel information for all ports and also the etherchannel global information when executing this command without a interface parameter.

Example

```
switch# show interface gi 0/1 etherchannel

Port : Gi0/1
-------------

Port State = Down, Not in Bundle
Channel Group :  1
Mode : Active
Pseudo port-channel = Po1
LACP port-priority  = 128
LACP Wait-time  = 2 secs
LACP Admin Port = 25
LACP Activity : Active
LACP Timeout : Long

Aggregation State : Aggregation, Defaulted

              LACP Port   Admin  Oper   Port    Port
Port    State   Priority    Key    Key    Number  State
-----------------------------------------------------------
Gi0/1   Down    128         1      1      0x19    0xa2

switch# show interface etherchannel

Port : Gi0/1
-------------

Port State = Down, Not in Bundle
Channel Group : 1
Mode : Active
Pseudo port-channel = Po1
LACP port-priority  = 128
LACP Wait-time  = 2 secs
LACP Port Identifier = 25
LACP Activity : Active
LACP Timeout : Long

Aggregation State : Aggregation, Defaulted

              LACP Port   Admin  Oper   Port    Port
Port    State   Priority    Key    Key    Number  State
-----------------------------------------------------------
Gi0/1   Down    128         1      1      0x19    0xa2

Port-channel : Po1
-------------------

Number of Ports = 1
HotStandBy port = null
Port state = Port-channel Ag-Not-Inuse
Protocol = LACP
MAC selection = Dynamic
Default Port = None
```

Command History

Version	History
1.00.001	This command was introduced

Chapter 31
802.1X Command

802.1X Command List

dot1x re-authenticate

To initial a re-authentication request immediately on 802.1X enable ports.

Command

dot1x re-authenticate [interface *<interface-type>* *<interface-id>***]**

Syntax Description

interface *interface-type interface-id*	Specify the interface to send re-authentication request. Interface-type including *Fa* (Fast Ethernet) or *Gi* (Gigabit Ethernet). Interface-id is slot/port number.

Command Modes

Privileged EXEC Mode

User Guidelines

System will initial the re-authentication to all 802.1X enable ports when executing this command without a port parameter.

Example

```
switch# dot1x re-authenticate int fa 0/1
```

Command History

Version	History
1.00.001	This command was introduced

dot1x system-auth-control

To enable 802.1X authentication on the Switch.

Command

dot1x system-auth-control

no dot1x system-auth-control

Default Settings

Disable

Command Modes

Global Configuration Mode

User Guidelines

Using no form to disable the 802.1X authentication.

Example

```
switch(config)# dot1x system-auth-control
```

Command History

Version	History
1.00.001	This command was introduced

aaa authentication dot1x default

To choose local or RADIUS database for 802.1X authentication.

Command

aaa authentication dot1x default { group radius | local}

Syntax Description

group radius	Using the database on RADIUS server.
local	Using the local database.

Default Settings

Local

Command Modes

Global Configuration Mode

Example

```
switch(config)# aaa authentication dot1x default group radius
```

Command History

Version	History
1.00.001	This command was introduced

dot1x local-database

To create user information in local database.

Command

dot1x local-database *<username>* **password** *<password>* **permission {allow | deny} [***<auth-timeout (value(0-7200))>***] [interface** *<interface-type> <interface-list>***]**

no dot1x local-database *<username>*

Syntax Description

username	Specify the user name of a local database entry.
password *password*	Specify the password of a local database entry.
permission allow	Specify the user is allowed to access ports configured.
permission deny	Specify the user is not allowed to access ports configured.
auth-timeout (value(0-7200))	Time interval between authentication attmpts.
interface *interface-type interface-list*	Port list the 802.1X authentication can be applied.

Default Settings

Permission – allow
Auth-timeout – 0
Interface – All ports

Command Modes

Global Configuration Mode

User Guidelines

1. When the timeout vlaue is 0, the authenticator will use the re-authentication period of the authenticator port
2. When create a user account without permission, auth-timeout and interface values, system will assign default value to this account.

Example

```
switch(config)# dot1x local-database trendnet password trendnet123 permission deny
```

Command History

Version	History
1.00.001	This command was introduced

radius-server host

To configure the details of RADIUS server.

Command

radius-server host *<ip-address>* **[timeout** *<1-120>***] [retransmit** *<1-254>***] key** *<secret-key-string>*

no radius-server host *<ip address>*

Syntax Description

ip-address	Specify the IP address of RADIUS server.
timeout *1-120*	Specify the time period that a client waits for the response from the RADIUS server before re-sending the request.
retransmit *1-254*	The maximum number that a client re-sends the request when there is no response from RADIUS server.
key *secret-key-string*	The encryption key for the communication of RADIUS server.

Default Settings

timeout – 3 seconds
retransmit – 3 times

Command Modes

Global Configuration Mode

User Guidelines

When configure a RADIUS server without timeout and retransmit parameter, system will apply the default values.

Example

```
switch(config)# radius-server host 172.17.5.111 key trendnet
```

Command History

Version	History
1.00.001	This command was introduced

dot1x control-direction

To choose the authentication control direction on ports.

Command

```
dot1x control-direction {in | both}

no dot1x control-direction
```

Syntax Description

in	Specify the the authentication control is only for ingress packets.
both	Specify the the authentication control is for both ingress and egress packets.

Default Settings

both

Command Modes

Interface Configuration Mode

User Guidelines

Using no form the reset the control direction to default.

Example

```
switch(config-if)# dot1x control-direction in
```

Command History

Version	History
1.00.001	This command was introduced

dot1x default

To configure 802.1X with default values on the port.

Command

dot1x default

Default Settings

Per-interface 802.1X protocol enable state	-	Enabled (force-authorized)
Periodic reauthentication	-	Disabled
Number of seconds between reauthentication attempts	-	3600 seconds
Quiet period	-	60 seconds
Retransmission time	-	30 seconds
Maximum retransmission number	-	2 times
Client timeout period	-	30 seconds
TX period	-	30 seconds
Defaults authentication server timeout period	-	30 seconds

Command Modes

Interface Configuration Mode

Example

```
switch(config-if)# dot1x default
```

Command History

Version	History
1.00.001	This command was introduced

dot1x max-req

To set the maximum 802.1X Extensible Authentication Protocol (EAP) retries of the client before restarting authentication process.

Command

dot1x max-req *<count(1-10)>*

no dot1x max-req

Syntax Description

count(1-10)	Specify the maximum number of retry.

Default Settings

2 retries

Command Modes

Interface Configuration Mode

User Guidelines

Using no form to reset the number of retry to default.

Example

```
switch(config-if)# dot1x max-req 10
```

Command History

Version	History
1.00.001	This command was introduced

dot1x max-start

To set the maximum EAPOL retries of the authenticator.

Command

dot1x max-start *<count(1-65535)>*

no dot1x max-start

Syntax Description

count(1-65535)	Specify the number of retry.

Default Settings

3 retries

Command Modes

Interface Configuration Mode

User Guidelines

Using no form to reset the number of retry to default.

Example

```
switch(config-if)# dot1x max-start 10
```

Command History

Version	History
1.00.001	This command was introduced

dot1x port-control

To set the authenticator control on ports.

Command

dot1x port-control {auto | force-authorized | force-unauthorized}

no dot1x port-control

Syntax Description

auto	Enable the 802.1X authentication on this port, and the port authorized or unauthorized will based on the 802.1X authentication result.
force-authorized	All traffic is transparent to the port.
force-unauthorized	All traffic is blocked to the port.

Default Settings Force-authorized

Command Modes Interface Configuration Mode

Example

```
switch(config-if)# dot1x port-control auto
```

Command History

Version	History
1.00.001	This command was introduced

dot1x reauthenitcation

To enable the periodic re-authentication on ports.

Command

dot1x reauthenitcation

no dot1x reauthenitcation

Default Settings Disable

Command Modes Interface Configuration Mode

User Guidelines UJsing no form to disable the 802.1X re-authentication.

Example

```
switch(config-if)# dot1x reauthenitcation
```

Command History

Version	History
1.00.001	This command was introduced

dot1x timeout

To configure the 802.1X timers.

Command

dot1x timeout {quiet-period *<value (0-65535)>* **| {reauth-period | server-timeout | supp-timeout | tx-period }***<value (1-65535)>***}**

no dot1x timeout {quiet-period | reauth-period | server-timeout | supp-timeout | tx-period }

Syntax Description

quiet-period *value (0-65535)*	The period that Switch will not do anything after a failed authentication.
reauth-period *value (1-65535)*	The period between re-authentication attempts.
server-timeout *value (1-65535)*	The period that Switch waits for the re-transmission to the RADIUS server.
supp-timeout *value (1-65535)*	The period that Switch waits for the re-transmission to the client.
tx-period *value (1-65535)*	The period that Switch waits for a response to an EAP-request/identity frame from the client before retransmitting the request.

Default Settings

quiet-period - 60 seconds
reauth-period - 3600 seconds
server-timeout - 30 seconds
supp-timeout - 30 seconds
tx-period - 30 seconds

Command Modes

Interface Configuration Mode

User Guidelines

Using no form to reset the timers to default.

Example

```
switch(config-if)# dot1x timeout quiet-period 120
```

Command History

Version	History
1.00.001	This command was introduced

shutdown dot1x

To shutdown the 802.1X authentication.

Command

shutdown dot1x

no shutdown dot1x

Default Settings

Enable

Command Modes

Global Configuration Mode

User Guidelines

Using no form to reactivate the 802.1X authentication.

Example

```
switch(config)# shutdown dot1x
```

Command History

Version	History
1.00.001	This command was introduced

debug dot1x

To enable the debug mode of 802.1X authentication.

Command

debug dot1x {all | errors | events | packets | state-machine | redundancy}

no debug dot1x {all | errors | events | packets | state-machine | redundancy}

Syntax Description

all	Displays all 802.1X debug messages.
errors	Displays error code debug messages
events	Displays event debug messages
packets	Displays packet debug messages
state-machine	Displays state-machine related debug messages
redundancy	Displays redundancy related debug messages.

Default Settings

Disable

Command Modes

Privileged EXEC Mode

User Guidelines

Using no form to disable the debug mode.

Example

```
switch# debug dot1x all
```

Command History

Version	History
1.00.001	This command was introduced

debug radius

To enable debug mode for RADIUS.

Command

debug radius {all | errors | events | packets | responses | timers}

no debug radius

Syntax Description

all	Displays all RADIUS debug messages.
errors	Displays the error code debug messages.
events	Displays the event related debug messages.
packets	Displays the packet related debug messages.
responses	Displays the server response related debug messages.
timers	Displays the timer related debug messages.

Default Settings

Disable

Command Modes

Privileged EXEC Mode

User Guidelines

Using no form to disable the debug mode.

Example

```
switch# debug radius all
```

Command History

Version	History
1.00.001	This command was introduced

show dot1x

To display the status, settings and information of 802.1X function.

Command

show dot1x [{ interface *<interface-type> <interface-id>* **| statistics interface** *<interface-type> <interface-id>* **| local-database | all }]**

Syntax Description

interface *interface-type interface-id*	Specify which interface to show 802.1X status and settings. Interface-type including *Fa* (Fast Ethernet) or *Gi* (Gigabit Ethernet). Interface-id is slot/port number.
statistics	Display 802.1X statistics of a specific interface.
interface *interface-type interface-id*	Specify which interface to show 802.1X statistics. Interface-type including *Fa* (Fast Ethernet) or *Gi* (Gigabit Ethernet). Interface-id is slot/port number.
local-database	Display 802.1X local user database information
all	Display 802.1X status and settings for all interfaces.

Command Modes

Privileged EXEC Mode

User Guidelines

System will display global 802.1X global status when executing the command without any parameter.

Example

```
switch# show dot1x

 Sysauthcontrol                   = Disabled
 Module Oper Status                = Disabled
 Dot1x Protocol Version            = 2
 Dot1x Authentication Method       = Local
 Nas ID                          = fsNas1

switch# show dot1x interface fa 0/1

Dot1x Info for Fa0/1
---------------------

AuthMode            = PORT-BASED
PortStatus          = AUTHORIZED
AuthSM State        = INITIALIZE
BendSM State        = INITIALIZE
AuthPortStatus      = AUTHORIZED
AdminControlDirection = BOTH
OperControlDirection  = BOTH
MaxReq              = 2
Port Control        = Force Authorized
QuietPeriod         = 60 Seconds
Re-authentication    = Disabled
ReAuthPeriod        = 3600 Seconds
ServerTimeout       = 30 Seconds
SuppTimeout         = 30 Seconds
Tx Period           = 30 Seconds

switch# show dot1x statistics interface fa 0/1

PortStatistics Parameters for Dot1x
-----------------------------------

TxReqId       = 0
TxReq         = 0
TxTotal       = 0

RxStart       = 0
RxLogoff      = 0
RxRespId      = 0
RxResp        = 0

RxInvalid     = 0
RxLenErr      = 0
RxTotal       = 0

RxVersion     = 0
LastRxSrcMac   = 00:00:00:00:00:00

switch# show dot1x local-database
Pnac Authentication Users Database
----------------------------------
User name : trendnet
Protocol : 4
Timeout : 0 seconds
Ports : Fa0/1, Fa0/2, Fa0/3, Fa 0/4, Fa 0/5, Fa 0/6, Fa 0/7,
Fa 0/8, Fa 0/9, Fa 0/10, Fa 0/11, Fa 0/12, Fa 0/13, Fa 0/14,
Fa 0/15, Fa 0/16, Fa 0/17, Fa 0/18, Fa 0/19, Fa 0/20, Fa 0/21,
```

```
Fa 0/22, Fa 0/23, Fa 0/24
Permission : Allow
--------------------------------
```

Command History

Version	History
1.00.001	This command was introduced

show radius server

To display current status and settings of RADIUS servers

Command

show radius server

Command Modes

Privileged EXEC Mode

Example

```
switch# show radius server

Radius Server Host Information
------------------------------
Index : 1
Server address : 172.17.5.135
Shared secret : password
Radius Server Status : Enabled
Response Time : 20
Maximum Retransmission : 10
------------------------------------------
```

Command History

Version	History
1.00.001	This command was introduced

show radius statistics

To display the RADIUS traffic statistics of the Switch.

Command

show radius statistics

Command Modes

Privileged EXEC Mode

Example

```
switch# show radius statistics

Radius Server Statistics
------------------------
Index : 1
Radius Server Address : 172.17.5.135
UDP port number : 1812
Round trip time : 0
No of request packets : 7
No of retransmitted packets : 72
No of access-accept packets : 0
No of access-reject packets : 0
No of access-challenge packets : 0
No of malformed access responses : 0
No of bad authenticators : 0
No of pending requests : 94
No of time outs : 81
No of unknown types : 0
-----------------------------------------
```

Command History

Version	History
1.00.001	This command was introduced

Chapter 32
IGMP Snooping Command

IGMP Command List

ip igmp snooping

To enable IGMP snooping globally or on a specific VLAN.

Command

```
ip igmp snooping

no ip igmp snooping
```

Default Settings

Disable

Command Modes

Global Configuration Mode
Config-vlan Mode

User Guidelines

Using no form to disable IGMP snooping.

Example

```
switch(config)# ip igmp snooping

switch(config-vlan)# ip igmp snooping
```

Command History

Version	History
1.00.001	This command was introduced

ip igmp snooping clear counters

To clear the IGMP snooping. counters

Command

ip igmp snooping clear counters [Vlan *<vlanid (1-4094)>***]**

Syntax Description		
	Vlan *vlanid (1-4094)*	Specify the counters of which VLAN to clear.

Command Modes

Global Configuration Mode

User Guidelines

System will clear all IGMP counters when executing this command without a VLAN parameter.

Example

```
switch(config)# ip igmp snooping clear counters vlan 1
```

Command History	Version	History
	1.00.001	This command was introduced

ip igmp snooping group-query-interval

To set up the time interval to send the group specific query.

Command

ip igmp snooping group-query-interval *<(1-5) seconds>*

no ip igmp snooping group-query-interval

Syntax Description		
	(1-5) seconds	Specify the time interval to send IGMP query.

Default Settings

2 seconds

Command Modes

Global Configuration Mode

User Guidelines

Using no form to reset the time interval to default.

Example

```
switch(config)# ip igmp snooping group-query-interval 5
```

Command History	Version	History
	1.00.001	This command was introduced

ip igmp snooping mrouter

To configure static IGMP multicast router ports on a specific VLAN.

Command

ip igmp snooping mrouter *<interface-type> <0/a-b, 0/c, ...>*

no ip igmp snooping mrouter *<interface-type> <0/a-b, 0/c, ...>*

Syntax Description

interface-type 0/a-b, 0/c, ...	Specify the type and ID of the static multicast router port. Interface-type including *Fa* (Fast Ethernet) or *Gi* (Gigabit Ethernet). Interface-id is slot/port number.

Command Modes

Config-vlan Mode

User Guidelines

Using no form to delete a static IGMP multicast router port.

Example

```
switch(config-vlan)# ip igmp snooping mrouter int fa 0/1
```

Command History

Version	History
1.00.001	This command was introduced

ip igmp snooping mrouter-time-out

To set the time-out period that an IGMP multicast router port hasn't received IGMP router control packet, it will be deleted.

Command

ip igmp snooping mrouter-time-out *<(60 - 600) seconds>*

no ip igmp snooping mrouter-time-out

Syntax Description

(60-600) seconds	Specify the time out period of IGMP multicast router ports.

Default Settings

125 seconds

Command Modes

Global Configuration Mode

User Guidelines

Using no form to reset the time out period to default.

Example

```
switch(config)# ip igmp snooping mrouter-time-out 60
```

Command History

Version	History
1.00.001	This command was introduced

ip igmp snooping port-purge-interval

To set the purge interval that an IGMP member port hasn't' received IGMP report packet, it will be deleted.

Command

ip igmp snooping port-purge-interval *<(130 - 1225) seconds>*

no ip igmp snooping port-purge-interval

Syntax Description

(130-1225) seconds	Specify the port purge interval.

Default Settings

260 seconds

Command Modes

Global Configuration Mode

User Guidelines

Using no form to reset the port purge interval to default.

Example

```
switch(config)# ip igmp snooping port-purge-interval 150
```

Command History

Version	History
1.00.001	This command was introduced

ip igmp snooping querier-query-interval

To set up the time interval to send the IGMP general query.

Command

ip igmp snooping querier-query-interval *<(60 - 600) seconds>*

no ip igmp snooping querier-query-interval

Syntax Description

(60-600) seconds	Specify the time interval of general query.

Default Settings

125 seconds

Command Modes

Global Configuration Mode

User Guidelines

Using no form to reset the query interval to default.

Example

```
switch(config)# ip igmp snooping querier-query-interval 150
```

Command History

Version	History
1.00.001	This command was introduced

ip igmp snooping report-forward

To configure which kind of ports that IGMP snooping reports should be forwarded.

Command

ip igmp snooping report-forward {all-ports | router-ports}

no ip igmp snooping report-forward

Syntax Description

all-ports	To forward IGMP reports to all ports.
router-ports	To forward IGMP reports to router ports.

Default Settings

Router ports

Command Modes

Global Configuration Mode

User Guidelines

Using no form to reset the forwarding port to default.

Example

```
switch(config)# ip igmp snooping report-forward all-ports
```

Command History

Version	History
1.00.001	This command was introduced

ip igmp snooping report-suppression-interval

To set the time interval that IGMPv2 report of the same group will not be forwarded to the router ports

Command

ip igmp snooping report-suppression-interval *<(1 - 25) seconds>*

no ip igmp snooping report-suppression-interval

Syntax Description

(1-25) seconds	Specify the report suppression time interval.

Default Settings

5 seconds

Command Modes

Global Configuration Mode

User Guidelines

Using no form to reset the time interval to default.

Example

```
switch(config)# ip igmp snooping report-suppression-interval
10
```

Command History

Version	History
1.00.001	This command was introduced

ip igmp snooping retry-count

To set the maximum retries for group specific queries which sent to a port

received a IGMPv2 leave message.

Command

ip igmp snooping retry-count *<1 - 5>*

no ip igmp snooping retry-count

Syntax Description

1 - 5	Specify the maximum retries for group specific queries.

Default Settings

2

Command Modes

Global Configuration Mode

User Guidelines

Using no form to reset the retry counter to default.

Example

```
switch(config)# ip igmp snooping retry-count 5
```

Command History

Version	History
1.00.001	This command was introduced

ip igmp snooping send-query

To configure if the Switch sends IGMP queries.

Command

ip igmp snooping send-query { enable | disable }

Syntax Description

enable	Switch sends IGMP queries.
disable	Switch does not send IGMP queries.

Default Settings

Enable

Command Modes

Global Configuration Mode

Example

```
switch(config)# ip igmp snooping send-query disable
```

Command History

Version	History
1.00.001	This command was introduced

ip igmp snooping fast-leave

Enable or disable the IGMP snooping fast leave function on a VLAN.

Command

ip igmp snooping fast-leave

no ip igmp snooping fast-leave

Default Settings Disable

Command Modes Config-vlan Mode

Example

```
switch(config-vlan)# ip igmp snooping fast-leave
```

Command History

Version	History
1.00.001	This command was introduced

ip igmp snooping querier

To configure the switch as the IGMP querier in a VLAN.

Command

ip igmp snooping querier

no ip igmp snooping querier

Default Settings Non-querier

Command Modes Config-vlan Mode

User Guidelines Using no form to reset the switch to non-querier.

Example

```
switch(config-vlan)# ip igmp snooping querier
```

Command History

Version	History
1.00.001	This command was introduced

shutdown snooping

To shutdown the snooping of the Switch.

Command

shutdown snooping

no shutdown snooping

Default Settings No shutdown

Command Modes Global Configuration Mode

User Guidelines

Using no form the restart the snooping.

Example

```
switch(config)# shutdown snooping
```

Command History

Version	History
1.00.001	This command was introduced

debug ip igmp snooping

To enable the debug mode of IGMP snooping.

Command

```
debug ip igmp snooping {[init] [resources] [tmr] [src] [grp]
[qry] [vlan] [pkt] [fwd] [mgmt] [redundancy] | all }

no debug ip igmp snooping {[init] [resources] [tmr] [src] [grp]
[qry] [vlan] [pkt] [fwd] [mgmt] [redundancy] | all }
```

Syntax Description

init	Displays the initial and shudown debug message.
resources	Displays the system resources management debug messages.
tmr	Displays the timer debug messages.
src	Displays the source debug messages.
grp	Displays the group debug messages.
qry	Displays the query related debug messages.
vlan	Displays the vlan debug messages.
pkt	Displays the packet dump debug messages.
fwd	Displays the L2 FDB related debug messages.
mgmt	Displays the management related debug messages.
redundancy	Displays the redundancy related debug messages.
all	Displays all debug messages.

Default Settings

Disable

Command Modes

Privileged EXEC Mode

User Guidelines

Usin no form to disable the debug mode.

Example

```
switch# debug ip igmp snooping all
```

Command History

Version	History
1.00.001	This command was introduced

show ip igmp snooping

To display current settings of IGMP snooping function.

Command

show ip igmp snooping [Vlan *<vlan id>***]**

Syntax Description

Vlan *vlan id*	

Command Modes

Privileged EXEC Mode

Example

```
switch# show ip igmp snooping

Snooping VLAN Configuration for the VLAN 1
  IGMP Snooping enabled
  IGMP configured version is V2
  IGMP Operating version is V2
  Fast leave is disabled
  Snooping switch is configured as Non-Querier
  Snooping switch is acting as Non-Querier
  Query interval is 125 seconds
```

Command History

Version	History
1.00.001	This command was introduced

show ip igmp snooping forwarding-database

To display the addresses information in IGMP forwarding database.

Command

show ip igmp snooping forwarding-database [Vlan *<vlan id>***]**

Syntax Description

Vlan *vlan id*	

Command Modes

Privileged EXEC Mode

User Guidelines

System will display multicast addresses in FDB when executing the command without a given VLAN parameter.

Example

```
switch# show ip igmp snooping forwarding-database vlan 1

 Vlan  MAC-Address         Ports
 ----  -----------------    -----
    1  01:00:5e:7f:ff:64    Fa0/9
```

Command History

Version	History
1.00.001	This command was introduced

show ip igmp snooping globals

To display the current global settings of IGMP snooping function.

Command

show ip igmp snooping globals

Command Modes

Privileged EXEC Mode

Example

```
switch# sh ip igmp snooping globals

Snooping Configuration
----------------------------
IGMP Snooping globally enabled
IGMP Snooping is operationally enabled
Transmit Query on Topology Change  globally disabled
Multicast forwarding mode is MAC based
Proxy reporting globally disabled
Router port purge interval is 125 seconds
Port purge interval is 260 seconds
Report forward interval is 5 seconds
Group specific query interval is 1 seconds
Querier query interval is 125 seconds
Reports are forwarded on router ports
Group specific query retry count is 2
```

Command History

Version	History
1.00.001	This command was introduced

show ip igmp snooping groups

To display the IGMP snooping group information

Command

show ip igmp snooping groups [Vlan *<vlan id>* **[Group** *<Address>***]]**

Syntax Description

Vlan *vlan id*	
Group *Address*	

Command Modes

Privileged EXEC Mode

User Guidelines

System will display all the IGMP group information snooped by the Switch when executing the command without given VLAN and group address parameters.

Example

```
switch# sh ip igmp snooping groups vlan 1 Group 239.255.255.250

Snooping Group information
----------------------------
Index: 1
Index: 2
Index: 3
VLAN ID:1  Group Address: 239.255.255.250
Filter Mode: EXCLUDE
Exclude sources: None
Receiver Ports:
  Fa0/9
```

Command History

Version	History
1.00.001	This command was introduced

show ip igmp snooping mrouter

To display the IGMP multicast router learned or configured on the Switch.

Command

show ip igmp snooping mrouter [Vlan *<vlan index>***]**

Syntax Description

Vlan *vlan index*		Specify the information in which VLAN to display.

Command Modes

Privileged EXEC Mode

User Guidelines

System will display the IGMP multicast router information for all VLANs when executing the command without a given VLAN parameter.

Example

Single Instance:

```
switch# show ip igmp snooping mrouter

Vlan Ports
----- ------
1 Gi0/1(dynamic), Gi0/2(static)
2 Gi0/3(static), Gi0/4(dynamic)
```

Multiple Instance:

```
switch# show ip igmp snooping mrouter

Switch cust1

Vlan Ports
----- ------
1 Gi0/1(static)
2 Gi0/2(static)

Switch cust2

Vlan Ports
----- ------
1 Gi0/3(static)
2 Gi0/3(static)
```

Command History

Version	History
1.00.001	This command was introduced

show ip igmp snooping statistics

To display the IGMP snooping statistics.

Command

show ip igmp snooping statistics [Vlan *<vlan id>***]**

Syntax Description

Vlan *vlan id*	Specify the statistic in which VLAN to display.

Command Modes

Privileged EXEC Mode

User Guidelines

System will display IGMP Snooping statistics for all VLANs when executing the command without a given VLAN parameter.

Example

```
switch# show ip igmp snooping statistics vlan 1

Snooping Statistics for VLAN 1
  General queries received : 0
  Group specific queries received : 0
 Group and source specific queries received : 0
  ASM reports received : 477
  SSM reports received : 0
  IS_INCLUDE messages received : 0
  IS_EXCLUDE messages received : 0
  TO_INCLUDE messages received : 0
  TO_EXCLUDE messages received : 0
  ALLOW messages received : 0
  Block messages received : 0
  Leave messages received : 25
  General queries transmitted : 0
  Group specific queries transmitted : 0
  ASM reports transmitted : 0
  SSM reports transmitted : 0
  Leaves transmitted : 2
  Packets dropped : 0
```

Command History

Version	History
1.00.001	This command was introduced

Chapter 33
Static MAC Entries Command

Static MAC Entries Command List

mac-address-table aging-time

To set the aging time of L2 Forwarding Database (FDB).

Command

mac-address-table aging-time *<10-1000000 seconds>*

no mac-address-table aging-time

Syntax Description

10-1000000 seconds	Specify the aging time if L2 FDB.

Default Settings

300

Command Modes

Global Configuration Mode

Example

```
switch(config)# mac-address-table aging-time 100
```

Command History

Version	History
1.00.001	This command was introduced

mac-address-table static multicast

To create a static multicast entry in L2 FBD.

Command

mac-address-table static multicast *<aa:aa:aa:aa:aa:aa>* **vlan** *<vlan-id(1-4094)>* **[recv-port** *<interface-type>* *<interface-id>***] interface ([***<interface-type>* *<0/a-b,0/c,...>***] [***<interface-type>* *<0/a-b,0/c,...>***] [port-channel** *<a,b,c-d>***]]) [forbidden-ports ([***<interface-type>* *<0/a-b,0/c,...>***] [***<interface-type>* *<0/a-b,0/c,...>***] [port-channel** *<a,b,c-d>***]]) [status { permanent | deleteOnReset | deleteOnTimeout }]**

no mac-address-table static multicast *<aa:aa:aa:aa:aa:aa>* **vlan** *<vlan-id(1-4094)>* **[recv-port** *<interface-type>* *<interface-id>***]**

Syntax Description

aa:aa:aa:aa:aa:aa	MAC address of the static multicast.
vlan *vlan-id(1-4094)*	VLAN of the static multicast.
recv-port *interface-type interface-id*	The received port of the static multicast. Interface-type including *Fa* (Fast Ethernet) or *Gi* (Gigabit Ethernet). Interface-id is slot/port number.
interface	The member interfaces of the static multicast.
interface-type 0/a-b,0/c,...	Specify the member port type and ID. Interface-type including *Fa* (Fast Ethernet) or *Gi* (Gigabit Ethernet). Interface-id is slot/port number.
port-channel *a,b,c-d*	Specify the member port channel ID.
forbidden-ports	The forbidden interface of this static multicast.
interface-type 0/a-b,0/c,...	Specify the forbidden port type and ID. Interface-type including *Fa* (Fast Ethernet) or *Gi* (Gigabit Ethernet). Interface-id is slot/port number.
port-channel *a,b,c-d*	Specify the forbidden port channel ID.
status	Specify the status of this static multicast.
permanent	The static multicast will keep alive.
deleteOnReset	The static multicast will be deleted after switch reset.
deleteOnTimeout	The static multicast will be deleted when aging time out.

Default Settings

Default Status – Permanent

Command Modes

Global Configuration Mode

User Guidelines

1. Using no form to delete a configured entry.
2. Multiple member port is allowed.

Example

```
switch(config)# mac-address-table static multicast
01:00:5e:11:22:33 vlan 1 interface fa 0/1 fa 0/2 status
permanent
```

Command History

Version	History
1.00.001	This command was introduced

mac-address-table static unicast

To create a static unicast entry in L2 FBD.

Command

mac-address-table static unicast *<aa:aa:aa:aa:aa:aa>* **vlan** *<vlan-id(1-4094)>* **[recv-port** *<interface-type>* *<interface-id>***] interface ([***<interface-type>* *<0/a-b,0/c,...>***] [***<interface-type>* *<0/a-b,0/c,...>***] [port-channel** *<a,b,c-d>***]) [status { permanent | deleteOnReset | deleteOnTimeout }]**

no mac-address-table static unicast *<aa:aa:aa:aa:aa:aa>* **vlan** *<vlan-id(1-4094)>* **[recv-port** *<interface-type>* *<interface-id>***]**

Syntax Description

aa:aa:aa:aa:aa:aa	MAC address of the static unicast.
vlan *vlan-id(1-4094)*	VLAN of the static unicast.
recv-port *interface-type interface-id*	The reveived port of the static unicast. Interface-type including *Fa* (Fast Ethernet) or *Gi* (Gigabit Ethernet). Interface-id is slot/port number.
interface	The interface to forward the static unicast.
interface-type 0/a,0/b,...	Specify the port type and ID to forward. Interface-type including *Fa* (Fast Ethernet) or *Gi* (Gigabit Ethernet). Interface-id is slot/port number.
port-channel *a,b,...*	Specify the port channel ID to forward.
status	Specify the status of this static unicast.
permanent	The static multicast will keep alive.
deleteOnReset	The static multicast will be deleted after switch reset.
deleteOnTimeout	The static multicast will be deleted when aging time out.

Default Settings

Status – Permanent

Command Modes

Global Configuration Mode

User Guidelines

Using no form to delete a configured entry.

Example

```
switch(config)# mac-address-table static unicast aa:bb:cc:dd:ee:ff vlan 1 int fa 0/1 status deleteonreset
```

Command History

Version	History
1.00.001	This command was introduced

show mac-address-table

To display the MAC address data learned or configured in MAC address table.

Command

show mac-address-table [vlan *<vlan-range>***] [address** *<aa:aa:aa:aa:aa:aa>***] [{interface** *<interface-type> <interface-id>***}]**

Syntax Description

vlan *vlan-range*	To display MAC addresses belong to a specific VLAN range.
address *aa:aa:aa:aa:aa:aa*	Specify a specific MAC address to display.
interface *interface-type interface-id*	To display MAC addresses under a specific port. Interface-type including *Fa* (Fast Ethernet), *Gi* (Gigabit Ethernet) or port-channel. Interface-id is slot/port number or port channel ID.

Command Modes

Privileged EXEC Mode

User Guidelines

System will display all MAC addresses when executing the command without given VLAN, address and interface parameters.

Example

```
switch# show mac-address-table int fa 0/9

Vlan    Mac Address        Type     Ports
----    -----------        ----     -----
1       00:00:48:bf:f3:01   Learnt   Fa0/9
1       00:03:64:00:01:23   Learnt   Fa0/9
1       00:0d:60:cc:2f:fe   Learnt   Fa0/9
1       00:0d:60:fb:52:c6   Learnt   Fa0/9
1       00:0e:7b:a0:12:97   Learnt   Fa0/9
1       00:0f:3d:2a:f0:1f   Learnt   Fa0/9
1       00:0f:3d:a8:88:9b   Learnt   Fa0/9
1       00:0f:ea:f0:0e:1e   Learnt   Fa0/9
1       00:0f:ea:f0:22:4f   Learnt   Fa0/9
1       00:10:c6:d0:ff:4f   Learnt   Fa0/9
1       00:11:25:43:38:83   Learnt   Fa0/9
1       00:11:25:87:1d:30   Learnt   Fa0/9
1       00:11:2f:2a:4f:ee   Learnt   Fa0/9
1       00:11:2f:8a:73:59   Learnt   Fa0/9
1       00:11:95:10:b3:7b   Learnt   Fa0/9
1       00:12:28:00:08:00   Learnt   Fa0/9
1       00:13:46:da:92:e9   Learnt   Fa0/9
1       00:13:46:f1:1a:92   Learnt   Fa0/9
1       00:14:85:13:cc:c6   Learnt   Fa0/9

Total Mac Addresses displayed: 19
```

Command History

Version	History
1.00.001	This command was introduced

show mac-address-table aging-time

To display the current setting of MAC table aging time.

Command **show mac-address-table aging-time**

Command Modes Privileged EXEC Mode

Example

```
switch# show mac-address-table aging-time

Mac Address Aging Time: 300
```

Command History

Version	History
1.00.001	This command was introduced

show mac-address-table count

To display the statistics for each kind of MAC address in MAC address table.

Command **show mac-address-table count [vlan** *<vlan-id(1-4094)>***]**

Syntax Description

vlan *vlan-id(1-4094)*	Specify information of which VLAN to display.

Command Modes Privileged EXEC Mode

User Guidelines System will display all statistics when executing the command without a given VLAN parameter.

Example

```
switch# show mac-address-table count vlan 1

Mac Entries for Vlan 1:
-------------------------
Dynamic Unicast Address Count    : 2
Dynamic Multicast Address Count  : 1
Static Unicast Address Count     : 2
Static Multicast Address Count   : 2
---------------------------------------
```

Command History

Version	History
1.00.001	This command was introduced

show mac-address-table dynamic multicast

To display the multicast MAC address dynamic learned in MAC address table.

Command **show mac-address-table dynamic multicast [vlan** *<vlan-range>***] [address** *<aa:aa:aa:aa:aa:aa>***] [{interface** *<interface-type> <interface-id>***}]**

Syntax Description

vlan *vlan-range*	To display MAC addresses belong to a specific VLAN range.
address *aa:aa:aa:aa:aa:aa*	Specify a specific MAC address to display.
interface *interface-type interface-id*	To display MAC addresses under a specific port. Interface-type including *Fa* (Fast Ethernet), *Gi* (Gigabit Ethernet) or port-channel. Interface-id is slot/port number or port channel ID.

Command Modes

Privileged EXEC Mode

User Guidelines

System will display all multicast MAC addresses dynamic learned when executing the command without given VLAN, address and interface parameters.

Example

```
switch# show mac-address-table dynamic multicast vlan 1

Vlan    Mac Address        Type     Ports
----    -----------        ----     -----
1       01:00:5e:7f:ff:fa   Learnt   Fa0/3, Fa0/11

Total Mac Addresses displayed: 1
```

Command History

Version	History
1.00.001	This command was introduced

show mac-address-table dynamic unicast

To display the unicast MAC address dynamic learned in MAC address table.

Command

show mac-address-table dynamic unicast [vlan *<vlan-range>***] [address** *<aa:aa:aa:aa:aa:aa>***] [{interface** *<interface-type> <interface-id>***}]**

Syntax Description

vlan *vlan-range*	To display MAC addresses belong to a specific VLAN range.
address *aa:aa:aa:aa:aa:aa*	Specify a specific MAC address to display.
interface *interface-type interface-id*	To display MAC addresses under a specific port. Interface-type including *Fa* (Fast Ethernet), *Gi* (Gigabit Ethernet) or port-channel. Interface-id is slot/port number or port channel ID.

Command Modes

Privileged EXEC Mode

User Guidelines

System will display all unicast MAC addresses dynamic learned when executing the command without given VLAN, address and interface parameters.

Example

```
switch# show mac-address-table dynamic unicast vlan 1

Vlan    Mac Address        Type     Ports
----    -----------        ----     -----
1       00:18:8b:bf:75:30   Learnt   Fa0/3
1       00:19:cb:d2:f2:75   Learnt   Fa0/11
1       00:22:15:0c:85:6c   Learnt   Fa0/11

Total Mac Addresses displayed: 3
```

Command History

Version	History
1.00.001	This command was introduced

show mac-address-table static multicast

To display the static multicast MAC address in MAC address table.

Command

show mac-address-table static multicast [vlan *<vlan-range>***] [address** *<aa:aa:aa:aa:aa:aa>***] [{interface** *<interface-type> <interface-id>***}]**

Syntax Description

vlan *vlan-range*	To display MAC addresses belong to a specific VLAN range.
address *aa:aa:aa:aa:aa:aa*	Specify a specific MAC address to display.
interface *interface-type interface-id*	To display MAC addresses under a specific port. Interface-type including *Fa* (Fast Ethernet), *Gi* (Gigabit Ethernet) or port-channel. Interface-id is slot/port number or port channel ID.

Command Modes

Privileged EXEC Mode

User Guidelines

System will display all static multicast MAC addresses when executing the command without given VLAN, address and interface parameters.

Example

```
switch# show mac-address-table static multicast vlan 1

Static Multicast Table
----------------------
Vlan          : 1
Mac Address    : 11:22:33:44:55:66
Member Ports   : Fa0/5
Status        : Permanent
-----------------------------------------------
Vlan          : 1
Mac Address    : 11:33:55:77:99:bb
Member Ports   : Fa0/7
Status        : Permanent
-----------------------------------------------

Total Mac Addresses displayed: 2
```

Command History

Version	History
1.00.001	This command was introduced

show mac-address-table static unicast

To display the static unicast MAC address in MAC address table.

Command

show mac-address-table static unicast [vlan *<vlan-range>***] [address** *<aa:aa:aa:aa:aa:aa>***] [{interface** *<interface-type> <interface-id>***}]**

Syntax Description

vlan *vlan-range*	To display MAC addresses belong to a specific VLAN range.
address *aa:aa:aa:aa:aa:aa*	Specify a specific MAC address to display.
interface *interface-type interface-id*	To display MAC addresses under a specific port. Interface-type including *Fa* (Fast Ethernet), *Gi* (Gigabit Ethernet) or port-channel. Interface-id is slot/port number or port channel ID.

Command Modes

Privileged EXEC Mode

User Guidelines

System will display all static unicast MAC addresses when executing the command without given VLAN, address and interface parameters.

Example

```
switch# show mac-address-table static unicast vlan 1

Vlan  Mac Address       RecvPort Status        Ports
----  -----------       -------- ------        -----
1     00:11:22:33:44:55          Permanent     Fa0/2
1     00:22:33:44:55:66          Permanent     Fa0/1

Total Mac Addresses displayed: 2
```

Command History

Version	History
1.00.001	This command was introduced

Chapter 34
Port Security Command

Port Security Command List

max learning address

To limits the number of MAC address learned from a port.

Command

max learning address *<address number(0-64)>*

no max learning address

Syntax Description		
	address number(0-64)	Specify the number of MAC can be learned of the port.

Default Settings

Disable

Command Modes

Interface Configuration Mode

User Guidelines

Using no form to disable the MAC learning limitation.

Example

```
switch(config-if)# max learning address 64
```

Command History	Version	History
	1.00.001	This command was introduced

show max-learning-address

To display the current port security setting on each port.

Command

show max-learning-address

Command Modes

Privileged EXEC Mode

Example

```
switch# show max-learning-address

Port       Port Security Status  Max Learning Address
----       -------------------   -----------------
Fa0/1      Enabled               64
Fa0/2      Disabled              0
Fa0/3      Enabled               16
Fa0/4      Disabled              0
Fa0/5      Enabled               32
Fa0/6      Disabled              0
Fa0/7      Enabled               8
Fa0/8      Disabled              0
Fa0/9      Disabled              0
Fa0/10     Disabled              0
Fa0/11     Disabled              0
Fa0/12     Disabled              0
Fa0/13     Disabled              0
Fa0/14     Disabled              0
Fa0/15     Disabled              0
Fa0/16     Disabled              0
Fa0/17     Disabled              0
Fa0/18     Disabled              0
Fa0/19     Disabled              0
Fa0/20     Disabled              0
Fa0/21     Disabled              0
Fa0/22     Disabled              0
Fa0/23     Disabled              0
Fa0/24     Disabled              0
Gi0/1      Disabled              0
Gi0/2      Disabled              0
Gi0/3      Disabled              0
Gi0/4      Disabled              0
```

Command History

Version	History
1.00.001	This command was introduced

Chapter 35
ACL Command

ACL Command List

mac access-list extended

To create and enter a MAC access control list.

Command

mac access-list extended *<access-list-number (1-65535)>*

no mac access-list extended *<short (1-65535)>*

Syntax Description

access-list-number (1-65535)	Specify the ID of access control list.
short (1-65535)	Specify the ID of access control list.

Command Modes

Global Configuration Mode

User Guidelines

1. Using no form to delete the access control list.
2. The ID cannot be duplicated for all access control list.

Example

```
switch(config)# mac access-list extended 1
switch(config-ext-macl)#
```

Command History

Version	History
1.00.001	This command was introduced

ip access-list

To create and enter an IP access control list.

Command

ip access-list { standard *<access-list-number (1-1000)>* **| extended** *<access-list-number (1001-65535)>* **}**

no ip access-list { standard *<access-list-number (1-1000)>* **| extended** *<access-list-number (1001-65535)>* **}**

Syntax Description

standard *access-list-number (1-1000)*	Specify the ID to a standard IP access control list.
extended *access-list-number (1001-65535)*	Specify the ID to a extended IP access control list.

Command Modes

Global Configuration Mode

User Guidelines

1. Using no form to delete the access control list.
2. The ID cannot be duplicated for all access control list.

Example

```
switch(config)# ip access-list standard 200
switch(config-std-nacl)#
```

Command History

Version	History
1.00.001	This command was introduced

deny (MAC Access List Configuration)

To configure a rule that packets matched will be filtered.

Command

deny { any | host *<mac-address>***}{ any | host** *<mac-address>* **} [aarp | amber | dec-spanning | decnet-iv | diagnostic | dsm | etype-6000 | etype-8042 | lat | lavc-sca | mop-console | mop-dump | msdos | mumps | netbios | vines-echo | vines-ip | xns-id |** *<protocol (0-65535)>***] [Vlan** *<vlan-id (1-4094)>***]**

Syntax Description

any	Matching packets with any source MAC address.
host *mac-address*	Matching packets with a specific source MAC address.
any	Matching packets with any destination MAC address.
host *mac-address*	Matching packets with a specific destination MAC address.
aarp	Matching packets with ether type aarp, 0x80F3(33011).
amber	Matching packets with ether type amber, 0x6008(24584).
dec-spanning	Matching packets with ether type dec-spanning, 0x8138 (33080).
decnet-iv	Matching packets with ether type decnet_iv, 0x6003 (24579).
diagnostic	Matching packets with ether type diagnostic, 0x6005(24581).
dsm	Matching packets with ether type dsm, 0x8309(32825).
etype-6000	Matching packets with ether type etype-6000, 0x6000(24576).
etype-8042	Matching packets with ether type etype-8042, 0x8042(32834).
lat	Matching packets with ether type lat, 0x6004(24580).
lavc-sca	Matching packets with ether type lavc-sca, 0x6007(24583).
mop-console	Matching packets with ether type mop-consol, 0x6002(24578).
mop-dump	Matching packets with ether type mop_dump, 0x6001(24577).
msdos	Matching packets with ether type msdos, 0x8041(32833).
mumps	Matching packets with ether type mumps, 0x6009(24585).
netbios	Matching packets with ether type netbios, 0x8040(32832).
vines-echo	Matching packets with ether type vines-echo, 0x0BAF(2991).
vines-ip	Matching packets with ether type vines-ip, 0x0BAD(2989).
xns-id	Matching packets with ether type xns-id, 0x0807(2055).
protocol (0-65535)	Matching packets with a specific ether type value.
Vlan *vlan-id (1-4094)*	Matching packets with a specific VLAN ID.

Command Modes

MAC Access List Configuration Mode

Example

```
switch(config-ext-macl)# deny any host 11-22-33-44-55-66 netbios
```

Command History

Version	History
1.00.001	This command was introduced

permit (MAC Access List Configuration)

To configure a rule that packets matched will be processed.

Command

permit { any | host *<mac-address>*}{ **any | host** *<mac-address>* **} [aarp | amber | dec-spanning | decnet-iv | diagnostic | dsm | etype-6000 | etype-8042 | lat | lavc-sca | mop-console | mop-dump | msdos | mumps | netbios | vines-echo | vines-ip | xns-id |** *<protocol (0-65535)>*] **[Vlan** *<vlan-id (1-4094)>*]

Syntax Description

any	Matching packets with any source MAC address.
host *mac-address*	Matching packets with a specific source MAC address.
any	Matching packets with any destination MAC address.
host *mac-address*	Matching packets with a specific destination MAC address.
aarp	Matching packets with ether type aarp, 0x80F3(33011).
amber	Matching packets with ether type amber, 0x6008(24584).
dec-spanning	Matching packets with ether type dec-spanning, 0x8138 (33080).
decnet-iv	Matching packets with ether type decnet_iv, 0x6003 (24579).
diagnostic	Matching packets with ether type diagnostic, 0x6005(24581).
dsm	Matching packets with ether type dsm, 0x8309(32825).
etype-6000	Matching packets with ether type etype-6000, 0x6000(24576).
etype-8042	Matching packets with ether type etype-8042, 0x8042(32834).
lat	Matching packets with ether type lat, 0x6004(24580).
lavc-sca	Matching packets with ether type lavc-sca, 0x6007(24583).
mop-console	Matching packets with ether type mop-consol, 0x6002(24578).
mop-dump	Matching packets with ether type mop_dump, 0x6001(24577).
msdos	Matching packets with ether type msdos, 0x8041(32833).
mumps	Matching packets with ether type mumps, 0x6009(24585).
netbios	Matching packets with ether type netbios, 0x8040(32832).
vines-echo	Matching packets with ether type vines-echo, 0x0BAF(2991).
vines-ip	Matching packets with ether type vines-ip, 0x0BAD(2989).
xns-id	Matching packets with ether type xns-id, 0x0807(2055).
protocol (0-65535)	Matching packets with a specific ether type value.
Vlan *vlan-id (1-4094)*	Matching packets with a specific VLAN ID.

Command Modes MAC Access List Configuration Mode

Example

```
switch(config-ext-macl)# permit host 11-22-33-44-55-66 any
msdos
```

Command History

Version	History
1.00.001	This command was introduced

deny (Standard IP Access List Configuration)

To configure a rule that packets matched will be filtered.

Command

deny { any | host *<src-ip-address>* **|** *<src-ip-address> <mask>* **}**
[{ any | host *<dest-ip-address>* **|** *<dest-ip-address> <mask>* **}]**

Syntax Description

any	Matching packet with any source IP address.
host *src-ip-address*	Matching packet with a specific source IP address.
src-ip-address mask	Matching packet with a range of source IP address. For example 172.17.5.1 with mask 255.255.255.0 means 172.15.5.0~255.
any	Matching packet with any destination IP address.
host *dest-ip-address*	Matching packet with a specific destination IP address.
dest-ip-address mask	Matching packet with a range of destination IP address. For example 172.17.5.1 with mask 255.255.255.0 means 172.15.5.0~255.

Command Modes Standard IP Access List Configuration Mode

Example

```
switch(config-std-nacl)# deny any 172.17.5.100 255.255.255.0
```

Command History

Version	History
1.00.001	This command was introduced

permit (Standard IP Access List Configuration)

To configure a rule that packets matched will be processed.

Command

permit { any | host *<src-ip-address>* **|** *<src-ip-address> <mask>* **}**
[{ any | host *<dest-ip-address>* **|** *<dest-ip-address> <mask>* **}]**

Syntax Description

any	Matching packet with any source IP address.
host *src-ip-address*	Matching packet with a specific source IP address.
src-ip-address mask	Matching packet with a range of source IP address. For example 172.17.5.1 with mask 255.255.255.0 means 172.15.5.0~255.
any	Matching packet with any destination IP address.
host *dest-ip-address*	Matching packet with a specific destination IP address.
dest-ip-address mask	Matching packet with a range of destination IP address. For example 172.17.5.1 with mask 255.255.255.0 means 172.15.5.0~255.

Command Modes

Standard IP Access List Configuration Mode

Example

```
switch(config-std-nacl)# permit host 172.17.6.1 172.17.5.100
255.255.255.0
```

Command History

Version	History
1.00.001	This command was introduced

deny (Extended IP Access List Configuration)

To configure a rule that packets matched will be filtered.

Command

deny { ip | ospf | pim | *<protocol-type (1-255)>***} { any | host** *<src-ip-address>* **|** *<src-ip-address> <mask>* **} { any | host** *<dest-ip-address>* **|** *<dest-ip-address> <mask>* **} [{tos** *<value (0-7)>* **| dscp** *<value (0-63)>***}]**

deny {tcp | udp} {any | host *<src-ip-address>* **|** *<src-ip-address> <src-ip-mask>***} {anyport |** *<src-port (1-65535)> <x8000>* **|** *xC000* **|** *xE000* **|** *xF000* **|** *xF800* **|** *xFC00* **|** *xFE00* **|** *xFF00* **|** *xFF80* **|** *xFFC0* **|** *xFFE0* **|** *xFFF0* **|** *xFFF8* **|** *xFFFC* **|** *xFFFE* **|** *xFFFF***} {any | host** *<dest-ip-address>* **|** *<dest-ip-address> <dest-ip-mask>***} {anyport |** *<dest-port (1-65535)> <x8000* **|** *xC000* **|** *xE000* **|** *xF000* **|** *xF800* **|** *xFC00* **|** *xFE00* **|** *xFF00* **|** *xFF80* **|** *xFFC0* **|** *xFFE0* **|** *xFFF0* **|** *xFFF8* **|** *xFFFC* **|** *xFFFE* **|** *xFFFF***} [{tos** *<value (0-7)>* **| dscp** *<value (0-63)>***}] [{ ack | ack-not }][{ rst | rst-not }]**

Syntax Description

ip	Matching all IP packets.
ospf	Matching all OSPF packets.
pim	Matching all PIM packets.
protocol-type (1-255)	Matching packets with specific protocol type.
any	Matching packet with any source IP address.
host *src-ip-address*	Matching packet with a specific source IP address.
src-ip-address mask	Matching packet with a range of source IP address. For example 172.17.5.1 with mask 255.255.255.0 means 172.15.5.0~255.
any	Matching packet with any destination IP address.
host *dest-ip-address*	Matching packet with a specific destination IP address.
dest-ip-address mask	Matching packet with a range of destination IP address. For example 172.17.5.1 with mask 255.255.255.0 means 172.15.5.0~255.
tos *value (0-7)*	Matching packets with specific ToS value.
dscp *value (0-63)*	Matching packets with specific DSCP type.
tcp	Matching all TCP packets.
udp	Matching all UDP packets.
anyport	Matching packets with any L4 source port.
src-port (1-65535) x8000 ~ xFFFF	Matching packets with a specific L4 source port.
dest-port (1-65535) x8000 ~ xFFFF	Matching packets with a specific L4 destination port.
ack	Macthing packets with a TCP acknowledge flag
ack-not	Macthing packets with a TCP acknowledge-not flag
rst	Macthing packets with a TCP reset flag
rst-not	Macthing packets with a TCP reset not flag

Command Modes

Extended IP Access List Configuration Mode

Example

```
switch(config-ext-nacl)# deny ip any any tos 7
```

Command History

Version	History
1.00.001	This command was introduced

permit (Extended IP Access List Configuration)

To configure a rule that packets matched will be processed.

Command

permit { ip | ospf | pim | *<protocol-type (1-255)>* **} { any | host** *<src-ip-address>* **|** *<src-ip-address> <mask>* **} { any | host** *<dest-ip-address>* **|** *<dest-ip-address> <mask>* **} [{tos** *<value (0-7)>* **| dscp** *<value (0-63)>* **}]**

permit {tcp | udp} {any | host *<src-ip-address>* **|** *<src-ip-address> <src-ip-mask>* **} {anyport |** *<src-port (1-65535)> <x8000* **|** *xC000* **|** *xE000* **|** *xF000* **|** *xF800* **|** *xFC00* **|** *xFE00* **|** *xFF00* **|** *xFF80* **|** *xFFC0* **|** *xFFE0* **|** *xFFF0* **|** *xFFF8* **|** *xFFFC* **|** *xFFFE* **|** *xFFFF>* **} {any | host** *<dest-ip-address>* **|** *<dest-ip-address> <dest-ip-mask>* **} {anyport |** *<dest-port (1-65535)> <x8000* **|** *xC000* **|** *xE000* **|** *xF000* **|** *xF800* **|** *xFC00* **|** *xFE00* **|** *xFF00* **|** *xFF80* **|** *xFFC0* **|** *xFFE0* **|** *xFFF0* **|** *xFFF8* **|** *xFFFC* **|** *xFFFE* **|** *xFFFF>* **} [{tos** *<value (0-7)>* **| dscp** *<value (0-63)>* **}] [{ ack | ack-not }][{ rst | rst-not }]**

Syntax Description

ip	Matching all IP packets.
ospf	Matching all OSPF packets.
pim	Matching all PIM packets.
protocol-type (1-255)	Matching packets with specific protocol type.
any	Matching packet with any source IP address.
host *src-ip-address*	Matching packet with a specific source IP address.
src-ip-address mask	Matching packet with a range of source IP address. For example 172.17.5.1 with mask 255.255.255.0 means 172.15.5.0~255.
any	Matching packet with any destination IP address.
host *dest-ip-address*	Matching packet with a specific destination IP address.
dest-ip-address mask	Matching packet with a range of destination IP address. For example 172.17.5.1 with mask 255.255.255.0 means 172.15.5.0~255.
tos *value (0-7)*	Matching packets with specific ToS value.
dscp *value (0-63)*	Matching packets with specific DSCP type.
tcp	Matching all TCP packets.
udp	Matching all UDP packets.
anyport	Matching packets with any L4 source port.
src-port (1-65535) x8000 ~ xFFFF	Matching packets with a specific L4 source port.
dest-port (1-65535) x8000 ~ xFFFF	Matching packets with a specific L4 destination port.
ack	Macthing packets with a TCP acknowledge flag
ack-not	Macthing packets with a TCP acknowledge-not flag
rst	Macthing packets with a TCP reset flag
rst-not	Macthing packets with a TCP reset not flag

Command Modes

Extended IP Access List Configuration Mode

Example

```
switch(config-ext-nacl)# deny ip any any tos 7
```

Command History

Version	History
1.00.001	This command was introduced

deny icmp (Extended IP Access List Configuration)

To configure a rule that packets matched will be filtered.

Command

deny icmp {any |host *<src-ip-address>*|*<src-ip-address> <mask>***} {any | host** *<dest-ip-address>* **|** *<dest-ip-address> <mask>* **} {message-type** *<(0-255)>***} {message-code** *<(0-255)>***}**

Syntax Description

any	Matching packet with any source IP address.
host *src-ip-address*	Matching packet with a specific source IP address.
src-ip-address mask	Matching packet with a range of source IP address. For example 172.17.5.1 with mask 255.255.255.0 means 172.15.5.0~255.
any	Matching packet with any destination IP address.
host *dest-ip-address*	Matching packet with a specific destination IP address.
dest-ip-address mask	Matching packet with a range of destination IP address. For example 172.17.5.1 with mask 255.255.255.0 means 172.15.5.0~255.
message-type *(0-255)*	Matching ICMP packets with specific message type.
message-code *(0-255)*	Matching ICMP packets with specific message code.

Command Modes

Extended IP Access List Configuration Mode

Example

```
switch(config-ext-nacl)# deny icmp any any message-type 10
message-code 10
```

Command History

Version	History
1.00.001	This command was introduced

permit icmp (Extended IP Access List Configuration)

To configure a rule that packets matched will be processed.

Command

permit icmp {any |host *<src-ip-address>*|*<src-ip-address> <mask>***} {any | host** *<dest-ip-address>* **|** *<dest-ip-address> <mask>* **} {message-type** *<(0-255)>***} {message-code** *<(0-255)>***}**

Syntax Description

any	Matching packet with any source IP address.
host *src-ip-address*	Matching packet with a specific source IP address.
src-ip-address mask	Matching packet with a range of source IP address. For example 172.17.5.1 with mask 255.255.255.0 means 172.15.5.0~255.
any	Matching packet with any destination IP address.
host *dest-ip-address*	Matching packet with a specific destination IP address.
dest-ip-address mask	Matching packet with a range of destination IP address. For example 172.17.5.1 with mask 255.255.255.0 means 172.15.5.0~255.
message-type *(0-255)*	Matching ICMP packets with specific message type.
message-code *(0-255)*	Matching ICMP packets with specific message code.

Command Modes

Extended IP Access List Configuration Mode

Example

```
switch(config-ext-nacl)# permit icmp any any message-type 10 message-code 10
```

Command History

Version	History
1.00.001	This command was introduced

mac access-group

To apply a MAC access control list to the port.

Command

mac access-group *<access-list-number (1-65535)>*

no mac access-group [*<access-list-number (1-65535)>***]**

Syntax Description

access-list-number (1-65535)	Specify which access control list to associate.

Command Modes

Interface Configuration Mode

User Guidelines

Using no form to dissociate ACL from the port.

Example

```
switch(config-if)# mac access-group 1
```

Command History

Version	History
1.00.001	This command was introduced

ip access-group

To apply an IP access control list from the port.

Command

ip access-group *<access-list-number (1-65535)>*

no ip access-group [*<access-list-number (1-65535)>***]**

Syntax Description

access-list-number (1-65535)	

Command Modes

Interface Configuration Mode

User Guidelines

Using no form to dissociate ACL from the port.

Example

```
switch(config-if)# ip access-group 1001
```

Command History

Version	History
1.00.001	This command was introduced

show access-lists

To display the details of configured access lists.

Command

show access-lists [[{ip | mac}] *<access-list-number (1-65535)>* **]**

Syntax Description

ip	To disply IP access control list.
mac	To display MAC access control list.
access-list-number (1-65535)	Specify the ID of access control list.

Command Modes

Privileged EXEC Mode

User Guidelines

System will display all access list information without a given IP or MAC access list number.

Example

```
switch# show access-lists mac 1

Extended MAC Access List 1
------------------------------
 EtherType                    : 0
 Vlan Id                      : 0
 Destination MAC Address        : 00:00:00:00:00:00
 Source MAC Address             : 00:00:00:00:00:00
 In Port List                  : NIL
 Filter Action                  : Permit
 Status                       : InActive
```

Command History

Version	History
1.00.001	This command was introduced

Chapter 36
Classmap Command

Classmap Command List

class-map

To create or enter a class map.

Command

class-map *<class-map-number(1-65535)>*

no class-map *<class-map-number(1-65535)>*

Syntax Description

class-map-number (1-65535)	Specify the class map ID.

Command Modes

Global Configuration Mode

User Guidelines

Using no form to delete a class map.

Example

```
switch(config)# class-map 1
```

Command History

Version	History
1.00.001	This command was introduced

match access-group

To associate a access control rule.

Command

match access-group { mac-access-list | ip-access-list } *<acl-index-num (1-65535) >*

Syntax Description

mac-access-list	Specify the rule of MAC access list to associate.
ip-access-list	Specify the rule of standard or extended IP access list to associate.
acl-index-num (1-65535)	Specify the access control list ID.

Command Modes

Class-map Configuration Mode

User Guidelines

The access control list rule must be created before associating.

Example

```
switch(config-cmap)# match access-group mac-access-list 1
```

Command History

Version	History
1.00.001	This command was introduced

show class-map

To display the settings of class maps.

Command

show class-map [*<class-map-num(1-65535)>***]**

Syntax Description

class-map-num (1-65535)	Specify which class map to display.

Command Modes

Privileged EXEC Mode

User Guidelines

System will show all the class map information when executing the command without a given class map number.

Example

```
switch# show class-map

DiffServ Configurations:
------------------------

Class map 1
--------------
Filter ID                : 1
Filter Type              : MAC-FILTER


DiffServ Configurations:
------------------------

Class map 2
--------------
Filter ID                : 1
Filter Type              : MAC-FILTER
```

Command History

Version	History
1.00.001	This command was introduced

Chapter 37
Policymap Command

Policymap Command List

policy-map

To create or enter a policy map.

Command

policy-map *<policy-map-number(1-65535)>*

no policy-map *<policy-map-number(1-65535)>*

Syntax Description		
policy-map-number (1-65535)	Specify the policy map ID.	

Command Modes

Global Configuration Mode

User Guidelines

Using no form to delete a policy map.

Example

```
switch(config)# policy-map 1
```

Command History	Version	History
	1.00.001	This command was introduced

class

To associate a class map in policy map and enter the Policy-map Class Configuration Mode.

Command

class *<class-map-number(1-65535)>*

no class *<class-map-number(1-65535)>*

Syntax Description		
class-map-number (1-65535)	Specify the class map IP to associate.	

Command Modes

Policy-map Configuration Mode

User Guidelines

Class map must be created before associating.

Example

```
switch(config-pmap)# class 1

Existing Policy-map configurations have been deleted. Please
apply the policy-map to make it active.
switch(config-pmap-c)#
```

Command History

Version	History
1.00.001	This command was introduced

set

To set the new 802.1p priority or DSCP type of packets match the associated ACL rule.

Command

set {cos *<new-cos(0-7)>* **| ip dscp** *<new-dscp(0-63)>* **}**

no set {cos *<new-cos(0-7)>* **| ip dscp** *<new-dscp(0-63)>* **}**

Syntax Description

cos *new-cos(0-7)*	Specify the new 802.1p priority of the packet.
ip dscp *new-dscp (0-63)*	Specify the new DSCP type of the packet.

Command Modes

Policy-map Class Configuration Mode

Example

```
switch(config-pmap-c)# set cos 1
```

Command History

Version	History
1.00.001	This command was introduced

police

To set up the actions of packets match the associated ACL rule.

Command

police *<rate-Kbps>* **exceed-action {drop | policed-dscp-transmit** *<new-dscp(0-63)>***}**

Syntax Description

rate-Kbps	Set the traffic rate threshold in Kbps for the class map.
exceed-action drop	Drop packets if traffic rate exceeds the threshold.
exceed-action policed-dscp-transmit *new-dscp(0-63)*	Modifying the DSCP type value for packets if traffic rate exceeds the threshold.

Command Modes

Policy-map Class Configuration Mode

Example

```
switch(config-pmap-c)# police 64 exceed-action drop
```

Command History

Version	History
1.00.001	This command was introduced

show policy-map

To display the settings of a policy map.

Command

show policy-map [*<policy-map-num(1-65535)>* **[class** *<class-map-num(1-65535)>***]**

Syntax Description

policy-map-num (1-65535)	
class *class-map-num (1-65535)*	

Command Modes

Privileged EXEC Mode

User Guidelines

Example

```
switch# show policy-map

DiffServ Configurations:
------------------------
Quality of Service has been enabled

Policy Map 1 is active

Class Map: 1
-------------

In Profile Entry
----------------
In profile action          : policed-dscp 2

Out Profile Entry
-----------------
Metering on
Out profile action         : none
```

Command History

Version	History
1.00.001	This command was introduced

Chapter 38
Rate Limiting Command

Rate Limiting Command List

rate-limit egress

To enable and setup the egress packet rate limiting on a port.

Command

rate-limit egress [*<rate-value(64~1000000)>***]**

no rate-limit egress

Syntax Description

rate-value (64~1000000)	Specify the traffic Kbit per second is allowed to be transmitted for an egress port..

Default Settings

Disable

Command Modes

Interface Configuration Mode

User Guidelines

The no form is to disable the rate limiting on a port.

Example

```
switch(config-if)# rate-limit egress 64
```

Command History

Version	History
1.00.001	This command was introduced

rate-limit ingress

To enable and setup the ingress packet rate limiting on a port.

Command

rate-limit ingress [*<rate-value (64~1000000)>***]**

no rate-limit ingress

Syntax Description

rate-value (64~1000000)	Specify the traffic Kbit per second is allowed to be received for an ingress port.

Default Settings

Disable

Command Modes Interface Configuration Mode

User Guidelines The no form is to disable the rate limiting on a port.

Example

```
switch(config-if)# rate-limit ingress 64
```

Command History

Version	History
1.00.001	This command was introduced

show rate-limit

To display the current rate-limit setting of interfaces

Command

show rate-limit [interface *<interface-type> <interface-id>***]**

Syntax Description

interface *interface-type interface-id*	Specifying which interface to show rate limiting information. Interface-type including *Fa* (Fast Ethernet) or *Gi* (Gigabit Ethernet). Interface-id is slot/port number.

Command Modes Privileged EXEC Mode

User Guidelines System will show the information for all ports when executing the command without a given interface parameter.

Example

```
switch# show rate-limit int fa 0/1

Fa0/1
Ingress Rate Limit Control    : Disabled
Egress Rate Limit Control     : Enabled
Egress Rate Limit Control     : 64
```

Command History

Version	History
1.00.001	This command was introduced

Chapter 39
Storm Control Command

Storm Control Command List

storm-control pkt-type

To enable and configure the details of the storm control function.

Command

storm-control pkt-type { broadcast-only | multicast-broadcast | dlf-multicast-broadcast } rate-level *<rate-level (64-1024000)>*

no storm-control

Syntax Description

broadcast-only	Only controls the broadcast packets.
multicast-broadcast	Controls both broadcast and multicast packets.
dlf-multicast-broadcast	Controls broadcast, multicast and Destination Lookup Failed (DLF) unicast packets.
rate-level *rate-level(64-1024000)*	Specify the packet number all types above is allowed to be forwarded per second.

Default Settings

Disable

Command Modes

Global Configuration Mode

User Guidelines

The no form disables the storm control.

Example

```
switch(config)# storm-control broadcast level 500
```

Command History

Version	History
1.00.001	This command was introduced

Chapter 40
QoS Command

QoS Command List

set dscp

To configure the priority and switch queue mapping

Command

```
set dscp { enable | disable }
```

Syntax Description

enable	Enables DSCP and queue mapping.
disable	Disables DSCP and queue mapping.

Default Settings

Disable

Command Modes

Global Configuration Mode

User Guidelines

When DSCP is disabled, Switch map queue with 802.1p priority.

Example

```
switch(config)# set dscp enable
```

Command History

Version	History
1.00.001	This command was introduced

vlan map-priority

To set the 802.1p priority and queue mapping.

Command

vlan map-priority *<priority value(0-7)>* **traffic-class** *<Traffic class value(0-3)>*

Syntax Description

priority value(0-7)	Specify which priority to map.
traffic-class *Traffic class value(0-3)*	Specify which switch queue to map.

Default Settings

Priority	Default traffic class
0	0
1	0
2	1
3	1
4	2
5	2
6	3
7	3

Command Modes

Global Configuration Mode

Example

```
switch(config)# vlan map-priority 0 traffic-class 1
```

Command History

Version	History
1.00.001	This command was introduced

dscp map-type

To set the dscp type and queue mapping.

Command

dscp map-type *<integer(0-63)>* **traffic-class** *<integer(0-3)>*

Syntax Description

integer(0-63)	Specify which DSCP type to map.
traffic-class *integer(0-3)*	Specify which switch queue to map.

Command Modes

Global Configuration Mode

User Guidelines

DSCP must be enabled before configuring this command.

Example

```
switch(config)# dscp map-type 63 traffic-class 0
```

Command History

Version	History
1.00.001	This command was introduced

cosq scheduling algorithm

To choose the scheduling algorithm for switch queues.

Command **cosq scheduling algorithm { strict | wrr }**

Syntax Description

strict	The traffic in highest queue always process first.
wrr	Using weighted round-robin algorithm to handle packets in priority queues.

Default Settings Strict

Command Modes Global Configuration Mode

Example

```
switch(config)# cosq scheduling algorithm wrr
```

Command History

Version	History
1.00.001	This command was introduced

switchport priority default

To setup the 802.1p priority for untagged packets.

Command **switchport priority default** *<priority value(0-7)>*

no switchport priority default

Syntax Description

priority value(0-7)	Specify which priority to set.

Default Settings 0

Command Modes Interface Configuration Mode

User Guidelines The no form resets the priority to default value.

Example

```
switch(config-if)#
```

Command History

Version	History
1.00.001	This command was introduced

show vlan traffic-classes

To display the current setting of 802.1p priority and traffic class mapping.

Command **show vlan traffic-classes**

Command Modes Privileged EXEC Mode

Example

```
switch# show vlan traffic-classes

Traffic Class table
---------------------
Priority    Traffic Class
---------   -------------
0            0
1            0
2            1
3            1
4            2
5            2
6            3
7            3
```

Command History

Version	History
1.00.001	This command was introduced

show vlan port config

To display the VLAN settings of ports

Command

show vlan port config [{port *<interface-type>* *<interface-id>***}]**

Syntax Description

port *interface-type interface-id*	Specified which interface to display vlan configurations. Interface-type including *Fa* (Fast Ethernet) or *Gi* (Gigabit Ethernet). Interface-id is slot/port number.

Command Modes Privileged EXEC Mode

User Guidelines System will display the information of all ports when executing the command without a given port parameter.

Example

```
switch#  show vlan port  config port fa 0/1

Vlan Port configuration table
------------------------------
Port Fa0/1
 Port Vlan ID                    : 1
 Port Acceptable Frame Type        : Admit All
 Port Ingress Filtering           : Enabled
 Port Mode                       : Hybrid
 Port Gvrp Status                 : Enabled
 Port Gvrp Failed Registrations     : 0
 Gvrp last pdu origin             : 00:00:00:00:00:00
 Port Restricted Vlan Registration   : Disabled
 Default Priority                : 0
 ----------------------------------------------------
```

Command History	Version	History
	1.00.001	This command was introduced

show dscp

To display the current dscp setting.

Command

```
show dscp
```

Command Modes

Privileged EXEC Mode

Example

```
switch# show dscp

DSCP is disabled
```

Command History	Version	History
	1.00.001	This command was introduced

show cosq algorithm

To display the current setting of CoS scheduling algorithm.

Command

```
show cosq algorithm
```

Command Modes

Privileged EXEC Mode

Example

```
switch# show cosq algorithm

 CoSq Algorithm is StrictPriority
```

Command History	Version	History
	1.00.001	This command was introduced

Chapter 41
RMON Command

RMON Command List

set rmon

To enable or disable RMON function.

Command

```
set rmon { enable | disable }
```

Syntax Description

enable	Enable RMON.
disable	Disable RMON.

Default Settings

Disable

Command Modes

Global Configuration Mode

Example

```
switch(config)# set rmon enable
```

Command History

Version	History
1.00.001	This command was introduced

rmon alarm

To set a RMON alarm on a MIB object.

Command

```
rmon alarm <number (1-65535)> <mib-object-id (255)>
<sample-interval-time (1-2147482647)> {absolute | delta }
rising-threshold <value (0-2147483647)> <rising-event-number
(1-65535)> falling-threshold <value (0-2147483647)>
<falling-event-number (1-65535)> [owner <ownername (127)>]

no rmon alarm <number (1-65535)>
```

Syntax Description

number (1-65535)	Specify the alarm number.
mib-object-id (255)	The MIB OID to set alarm.
sample-interval-time (1-2147482647)	The time interval in seconds that alarm monitors the MIB variable.
absolute	To test the MIB variable directly.
delta	To test the change between samples of a MIB variable.
rising-threshold *value (0-2147483647)*	The threshold value to trigger alarm when the number of sample exceeds.
rising-event-number (1-65535)	The number of event to trigger when rising threshold is exceeded.
falling-threshold *value (0-2147483647)*	The threshold value to reset alarm when the number of sample exceeds.
falling-event-number (1-65535)	The number of event to trigger when falling threshold is exceeded.
owner *ownername (127)*	Specify the owner of the alarm.

Command Modes

Global Configuration Mode

User Guidelines

1. RMON function must be enabled and RMON event must be configured before configuring alarms.
2. Using no form to delete a RMON alarm on a MIB object.

Example

```
switch(config)# rmon alarm 1 1.3.6.1.2.1.17.7.1.3.1.1.3.141.0.0.0.0.0.22.0 10 delta rising-threshold 15 1 falling-threshold 10 1
```

Command History

Version	History
1.00.001	This command was introduced

rmon event

To add an event to RMON event table.

Command

rmon event *<number (1-65535)>* **[description** *<event-description (127)>***]** **[log]** **[owner** *<ownername (127)>***]** **[trap** *<community (127)>***]**

no rmon event *<number (1-65535)>*

Syntax Description

number (1-65535)	Specify the event number.
description *event-description (127)*	Setting the description of the event.
log	Generating syslog when event is triggered.
owner *ownername (127)*	Specify the owner of the event.
trap *community (127)*	Generating a trap message when event is triggered.

Command Modes Global Configuration Mode

User Guidelines
1. RMON function must be enabled and RMON event must be configured before configuring alarms.
2. Using no form to delete events from RMON event table.

Example
```
switch(config)# rmon event 1 description broadcast-too-high log owner trendnet trap redalert
```

Command History

Version	History
1.00.001	This command was introduced

rmon collection history

To enable and setup the RMON collection history on a port.

Command

rmon collection history *<index (1-65535)>* **[buckets** *<bucket-number (1-50)>***] [interval** *<seconds (1-3600)>***] [owner** <ownername (127)>**]**

no rmon collection history *<index (1-65535)>*

Syntax Description

index (1-65535)	Specify the index of history table.
buckets *bucket-number (1-50)*	The maximum number of RMON history collection.
interval *seconds (1-3600)*	The time interval for the history collection.
owner *ownername (127)*	Specify the owner of the history group.

Command Modes Interface Configuration Mode

User Guidelines
1. RMON function must be enabled and RMON event must be configured before configuring alarms.
2. Using no form to disable the history collection..

Example
```
switch(config-if)# rmon collection history 1 buckets 50 interval 10 owner trendnet
```

Command History

Version	History
1.00.001	This command was introduced

rmon collection stats

To enable and setup the RMON statistics collection on a port.

Command

rmon collection stats *<index (1-65535)>* **[owner** *<ownername (127)>***]**

no rmon collection stats *<index (1-65535)>*

Syntax Description

index (1-65535)	Specify the index of the RMON statistics collection.
owner *ownername (127)*	Specify the owner of the statistics

Command Modes

Interface Configuration Mode

User Guidelines

1. RMON function must be enabled and RMON event must be configured before configuring alarms.
2. Using no form to disable the statistics collection..

Example

```
switch(config-if)# rmon collection stats 1 owner trendnet
```

Command History

Version	History
1.00.001	This command was introduced

show rmon

To display the RMON statistics, alarms, events, and history configured on the interface

Command

show rmon [statistics [*<stats-index (1-65535)>***]] [alarms] [events] [history** *<history-index (1-65535)>* **[overview]]**

Syntax Description

statistics *stats-index (1-65535)*	To display the RMON collection stats data configured
alarms	To display the RMON alarms data configured
events	To display the RMON events data configured
history *history-index (1-65535)*	To display the RMON collection history data configured
overview	To display the overview of RMON entries

Command Modes

Privileged EXEC Mode

Example

```
switch# show rmon

RMON is enabled

switch# show rmon statistics 1 alarms events history overview

RMON is enabled
Collection 1 on Fa0/5 is active, and owned by trendnet,
 Monitors ifEntry.1.5 which has
 Received 0 octets, 0 packets,
 0 broadcast and 0 multicast packets,
 0 undersized and 0 oversized packets,
 0 fragments and 0 jabbers,
 0 CRC alignment errors and 0 collisions.
 # of packets received of length (in octets):
 64: 0, 65-127: 0, 128-255: 0,
 256-511: 0, 512-1023: 0, 1024-1518: 0
Alarm table is empty

Event 1 is active, owned by trendnet
 Description is trendnet
 Event firing causes log,
 Time last sent is Jan  1 00:07:41 2009
Entry 1 is active,  and owned by trendnet
 Monitors ifEntry.1.5 every 1 second(s)
 Requested # of time intervals, ie buckets, is 1,
 Granted # of time intervals, ie buckets, is 1,
```

Command History

Version	History
1.00.001	This command was introduced

Chapter 42
Statistics Command

Statistics Command List

clear interfaces

To clear counters of interfaces.

Command

clear interfaces [*<interface-type> <interface-id>* **] counters**

Syntax Description

interface-type	Specify which counters of which interface to clear.
interface-id	Interface-type including *Fa* (Fast Ethernet), *Gi* (Gigabit Ethernet) or port-channel. Interface-id is slot/port number or port channel ID.

Command Modes

Privileged EXEC Mode

User Guidelines

System will clear all interface counters when executing the command without a interface type and ID.

Example

```
switch# clear interfaces counters

switch# clear interfaces fa 0/1 counters
```

Command History

Version	History
1.00.001	This command was introduced

show ip traffic

To display the statistic of IP traffic and ICMP traffic

Command

show ip traffic

Command Modes

Privileged EXEC Mode

Example

```
switch# show ip traffic

IP Statistics:
--------------
 Rcvd:  1817 total, 0 header error discards
       0 bad ip address discards, 12 unsupported protocol
discards
 Frags: 0 reassembled, 30 timeouts, 0 needs reassembly
       0 fragmented, 0 couldn't fragment
 Bcast:  Sent:  0 forwarded, 2845 generated requests
 Drop:
ICMP Statistics:
----------------
 Rcvd:  4 total, 0 checksum errors,  0 unreachable, 0 redirects
       0 time exceeded, 0 param problems,  0 quench
       4 echo, 0 echo reply,  0 mask requests, 0 mask replies,
       0 timestamp , 0 time stamp reply,
 Sent:  4 total, 0 checksum errors,  0 unreachable, 0 redirects
       0 time exceeded, 0 param problems,  0 quench
       0 echo, 4 echo reply,  0 mask requests, 0 mask replies,
       0 timestamp , 0 time stamp reply,
```

Command History

Version	History
1.00.001	This command was introduced

Chapter 43
System Operation Command

System Operation Command List

watchdog

To auto-recover the Switch if Switch was found hanging up.

Command

```
watchdog { enable | disable}
```

Syntax Description

enable	Enables the watchdog.
disable	Disables the watchdog.

Default Settings

Disable

Command Modes

Privileged EXEC Mode

Example

```
switch# watchdog
```

Command History

Version	History
1.00.001	This command was introduced

copy

To download a file from TFTP server to local flash or upload a local file to TFTP server.

Command

copy { *tftp://ip-address/filename* | *flash: filename*}{ *tftp://ip-address/filename* | *flash: filename*}

Syntax Description

tftp://ip-address/filename	The IP address the remote tftp server and the filename you would like to copy from.
flash: filename	The path and filename of the local file you would like to copy from.
tftp://ip-address/filename	The IP address the remote tftp server and the file name to be saved.
flash: filename	The path and filename you would like to saved in local flash

Command Modes

Privileged EXEC Mode

Example

```
switch# copy tftp://172.17.0.100/syslog1 flash:backuplog
```

Command History

Version	History
1.00.001	This command was introduced

ping

Sending out ICMP echo request to verify a specific IP address is available.

Command

ping [ip] <*destination-address***> [size** *<packet_size (0-2080)>***] [count** *<packet_count (1-10)>***] [timeout** *<time_out (1-100)>***]**

Syntax Description

ip *destination-address*	Specify which IP address to send echo request.
size *packet_size (0-2080)*	Specify the size of ping packet to send.
count *packet_count (1-10)*	Specify how mand echo request to send.
timeout *time_out (1-100)*	Specify the timeout in seconds to wait each ICMP echo reply.

Default Settings

Packet count: 3
Timeout: 5

Command Modes

Privileged EXEC Mode

Example

```
switch# ping ip 192.168.0.2 size 2080
Reply Received From :192.168.0.2, TimeTaken : 10 msecs
Reply Received From :192.168.0.2, TimeTaken : 20 msecs
Reply Received From :192.168.0.2, TimeTaken : 20 msecs

--- 192.168.0.2 Ping Statistics ---
3 Packets Transmitted, 3 Packets Received, 0% Packets Loss
```

Command History

Version	History
1.00.001	This command was introduced

help

To list all the command starting with the given keyword and also display the description of the command.

Command

help *<command>*

Syntax Description

command	Specify which command you would like to get the help.

Command Modes

All Modes

User Guidelines

System will display all commands under the command mode without descriptions when executing the command without a keyword.

Example

```
switch(config)# help sys

CONFIGURE commands :
  system cli-timeout <1-18000 seconds>
  [Desc]: Sets Cli auto timeout interval
  system contact <contact info>
  [Desc]: Sets the system contact information
  system location <location info>
  [Desc]: Sets the system location
  system name <identify info>
  [Desc]: Sets the system name
  system web-timeout <180-3600 seconds>
  [Desc]: Sets Web auto timeout interval

switch(config-cmap)# help

CLASSMAP commands :
  clear screen
  end
  exit
  help [ command ]
  match access-group { mac-access-list | ip-access-list }
<acl-index-num (1-65535) >
```

Command History

Version	History
1.00.001	This command was introduced

clear screen

To clear the screen.

Command

clear screen

Command Modes

All Modes

Example

```
switch# clear screen
```

Command History

Version	History
1.00.001	This command was introduced

lock

To lock the command line interface to prevent unauthorized user accessing the Switch.

Command

lock

Command Modes

Privileged EXEC Mode

User Guidelines

Entering the password of any privilege 15 user to unlock.

Example

```
switch# lock
CLI console locked
Enter Password to unlock the console:
```

Command History

Version	History
1.00.001	This command was introduced

logout

To logout the Switch.

Command

logout

Command Modes

Privileged EXEC Mode

Example

```
switch# logout
```

Command History

Version	History
1.00.001	This command was introduced

cmdbuffs

To configure the syslog buffer size for a particular user.

Command

cmdbuffs *<user name> <no.of buffers (1-200)>*

Syntax Description

user name	Specify which user to configure the buffer size.
no.of buffers (1-200)	Specify the number of buffer size.

Command Modes Global Configuration Model

Example

```
switch(config)# cmdbuffs root 200
```

Command History

Version	History
1.00.001	This command was introduced

show history

To display the command history had been executed.

Command

```
show history
```

Command Modes Privileged EXEC Mode

User Guidelines The command history is listed form the first executed command to the latest one.

Example

```
switch#
```

Command History

Version	History
1.00.001	This command was introduced

dir flash:

To display the files stored in NV-RAM.

Command

```
dir flash:
```

Command Modes Privileged EXEC Mode

Example

```
switch# dir flash:
```

Command History

Version	History
1.00.001	This command was introduced

space flash:

To display the space of NV-RAM remained

Command **space flash:**

Command Modes Privileged EXEC Mode

Example

```
switch# space flash:
```

Command History

Version	History
1.00.001	This command was introduced

space memory:

To display the space of DRAM remained

Command **space memory:**

Command Modes Privileged EXEC Mode

Example

```
switch# space memory:
```

Command History

Version	History
1.00.001	This command was introduced

?

To display the next possible keyword or parameter of the command

Command **?**

Command Modes All Modes

Example

```
switch# space ?
EXEC commands :
  space flash:
  space memory:
```

Command History

Version	History
1.00.0010	This command was introduced

Chapter 44
Interface Command

Interface Command List

interface

To create or enter a physical or logical network interface.

Command

interface { vlanMgmt | Port-Channel *<port-channel-id(1-65535)>* **|** *<interface-type> <interface id>* **}**

no interface { vlanMgmt | Port-Channel *<port-channel-id (1-65535)>* **|** *<interface-type> <interface id>* **}**

Syntax Description

vlanMgmt	To enter the management VLAN of the Switch.
Port-Channel *port-channel-id (1-65535)*	To enter a port channel interface. If the channel ID specified doesn't exist, system will create a new port channel.
interface-type interface id	To enter a physical port. Interface-type including *Fa* (Fast Ethernet) or *Gi* (Gigabit Ethernet). Interface-id is slot/port number.

Command Modes

Global Configuration Mode

User Guidelines

To create or entering a port channel, port-channel function must be enabled first.

Example

```
switch(config)# interface fa 0/1
switch(config-if)#
```

Command History

Version	History
1.00.001	This command was introduced.

shutdown

Shutting down the network interface.

Command

shutdown

no shutdown

Default Settings

Interfaces had been created are active by default.

Command Modes

Interface Configuration Mode

User Guidelines

The no form reactivates the interface.

Example

```
switch(config-if)# shut down
```

Command History

Version	History
1.00.001	This command was introduced.

mtu

To setup the Maximum Transmission Unit (MTU) frame size of the interface.

Command

mtu *<frame-size(90-1522)>*

Syntax Description

frame-size(90-1522)

Default Settings

1500

Command Modes

Interface Configuration Mode

User Guidelines

Interface must be shutdown before configuring MTU size.

Example

```
switch(config-if)# mtu 90
```

Command History

Version	History
1.00.001	This command was introduced.

show interfaces

To display the status, configurations or statistics of the interface

Command

show interfaces [{ [*<interface-type> <interface-id>***] [{ description | flowcontrol | capabilities | status }] | port-channel** *<port-channel-id (1-65535)>* **}]**

Syntax Description

interface-type interface-id	Specify the information of which interface to display. Interface-type including *Fa* (Fast Ethernet) or *Gi* (Gigabit Ethernet). Interface-id is slot/port number.
description	Display the link status and protocol status of the interface
flowcontrol	Display the flow control setting and pause frame statistic of the interface
capabilities	Display the capabilities of the interface
status	Display the current status of the interface
port-channel *port-channel-id (1-65535)*	Port channel ID

Command Modes

Privileged EXEC Mode

User Guidelines

System will display information of all interfaces when executing the command without given parameters.

Example

```
switch# show interface fa 0/5 description

Interface    Status   Protocol
---------    ------   --------
Fa0/5        up       up

switch# show interface fa 0/5 flowcontrol

Port     Tx FlowControl   Rx FlowControl   Tx Pause   Rx Pause
----     --------------   -------------    --------   --------
Fa0/5    off              off              0          0

switch# show interface fa 0/5 capabilities

Fa0/5
Type        : 10/100/1000 Base TX
Speed       : 10, 100, 1000, Auto
Duplex      : Half, Full
FlowControl : Send, Receive

switch# show interface fa 0/5 status

Port       Status          Duplex   Speed      Negotiation
----       ------          ------   -----      -----------
Fa0/5         connected          Full       100 Mbps     Auto
Copper
```

Command History

Version	History
1.00.001	This command was introduced.

show interface mtu

To display the MTU setting of the interface.

Command

show interface mtu [{ Vlan *<vlan-id (1-4094)>* **| port-channel** *<port-channel-id (1-65535)>* **|** *<interface-type> <interface-id>* **}]**

Syntax Description

Vlan *vlan-id (1-4094)*	VLAN ID
port-channel *port-channel-id (1-65535)*	Port channel ID
interface-type interface-id	Specify which interface to show the mtu setting. Interface-type including *Fa* (Fast Ethernet) or *Gi* (Gigabit Ethernet). Interface-id is slot/port number.

Command Modes

Privileged EXEC Mode

User Guidelines

System will display MTU settings for all interface when executing the command without given parameters.

Example

```
switch# show interface mtu fa 0/1

Fa0/1   MTU size is 1522
```

Command History

Version	History
1.00.001	This command was introduced.

show interfaces counters

To display the statistics of interfaces.

Command

show interfaces [{ *<interface-type> <interface-id>* **}] counters**

Syntax Description

interface-type interface-id	Specify the counter information of which interface to display. Interface-type including *Fa* (Fast Ethernet), *Gi* (Gigabit Ethernet) or port-channel. Interface-id is slot/port number or port-channel ID.

Command Modes

Privileged EXEC Mode

User Guidelines

System will display statistics for all interfaces when executing the command without interface-type and interface-id.

Example

```
switch# show interface fa 0/12 counters

Port         InOctet         InUcast      InDiscard    InErrs
InHCOctet
----         -------         -------      ---------    ------
---------
Fa0/12    30159626   8763       0         0
30159626

Port         OutOctet        OutUcast     OutDiscard   OutErrs
OutHCOctet
----         --------        --------     ----------   -------
----------
Fa0/12    226671     2858       0          0
```

Command History

Version	History
1.00.001	This command was introduced

Technical Specifications

Hardware	
Standards	IEEE 802.3 10BASE-T IEEE 802.3u 100BASE-TX IEEE 802.3ab 1000BASE-T IEEE 802.3z 1000BASE-X SX/LX IEEE 802.3x Flow Control and Back Pressure IEEE 802.3ad Link Aggregation/Port Trunking (LACP) IEEE 802.1d Spanning Tree (STP) IEEE 802.1w Rapid Spanning Tree (RSTP) IEEE 802.1s Multiple Spanning Tree (MSTP) IEEE 802.1p Quality of Service/Class of Service (QoS/CoS) IEEE 802.1Q VLAN Tagging and GVRP IEEE 802.1X Port-Based Network Access Control
Interface	24 x 10/100Mbps Auto-MDIX Fast Ethernet ports 4 x 10/100/1000Mbps Auto-MDIX Gigabit ports 2 x shared SFP (Mini-GBIC) slots 1 x RS-232 console port for switch management
Cabling	Network: 10Base-T: UTP/STP Cat. 5 cable (100m) 100Base-TX: UTP/STP Cat. 5, 5e cable (100m) 1000Base-T: UTP/STP Cat 5e, 6 cable (100m) Mini-GBIC: LC (Multi-Mode): 50/125um~62.5/125um LC (Single Mode): 9/125um~10/125um
Switching Method	Store-and-Forward
Protocol/Topology	(CSMA/CD) / Star
Buffer Memory	256KByte data buffer
Filtering Address Table	8K MAC address entries
Switch Fabric/Capacity	Up to 12.8Gbps
LED Display	PWR (Green): Power, SYS (Green): System 10M Link/ACT (Amber): 10Mbps Link/Activity (per Ethernet port) 100M Link/ACT (Green): 100Mbps Link/Activity (per Ethernet port) 10/100M Link/ACT (Amber): 10/100Mbps Link/Activity (per Gigabit port) 1000M Link/ACT (Green): 1000Mbps Link/Activity (per Gigabit port)
Power	Input: 100~240VAC, 50/60Hz internal power supply
Power Consumption	16.8 W
Dimensions	440 x 140 x 44 mm (17.3 x 5.5 x 1.7 in.)
Weight	2 kg (4.5 lbs.)
Temperature	Operating: 0° ~ 40° C (32° ~ 104° F) Storage: -10° ~ 70° C (14° ~ 158° F)
Humidity	Max. 90% (non-condensing)
Certifications	CE, FCC
Software	
Management	SNMP v1, v2c, v3, HTTP/HTTPS Web, Telnet, SSH, console
Spanning Tree	802.1d STP (Spanning Tree Protocol) 802.1w RSTP (Rapid Spanning Tree Protocol) 802.1s MSTP (Multiple Spanning Tree Protocol)
Link Aggregation	Static Link Aggregation 802.3ad Dynamic LACP
Quality of Service	802.1p Class of Service Port Based QoS

	DSCP (Differentiated Services Code Point)
VLAN	Asymmetric VLAN 802.1Q Tagged VLAN & Dynamic GVRP Up to 256 static/dynamic groups
IGMP	Support IGMP Snooping v1/2 Up to 64 multicast entries
Port Mirror	RX, TX, or both
Security	MAC Address learning, ACL L2/L3/L4 User Authentication: 802.1X Port-Based Network Access Control, Local User Database
Frame Size	1522 bytes (max.)
Bandwidth Control	Bandwidth control per port
Flow Control	802.3x Flow Control for Full-Duplex and back pressure for Half-Duplex
Firmware Update	Support TFTP firmware update, TFTP backup and restore, via Web Browser

Limited Warranty

TRENDnet warrants its products against defects in material and workmanship, under normal use and service, for the following lengths of time from the date of purchase.

TL2-E284 – 3 Years Warranty

AC/DC Power Adapter, Cooling Fan, and Power Supply carry 1 year warranty.

If a product does not operate as warranted during the applicable warranty period, TRENDnet shall reserve the right, at its expense, to repair or replace the defective product or part and deliver an equivalent product or part to the customer. The repair/replacement unit's warranty continues from the original date of purchase. All products that are replaced become the property of TRENDnet. Replacement products may be new or reconditioned. TRENDnet does not issue refunds or credit. Please contact the point-of-purchase for their return policies.

TRENDnet shall not be responsible for any software, firmware, information, or memory data of customer contained in, stored on, or integrated with any products returned to TRENDnet pursuant to any warranty.

There are no user serviceable parts inside the product. Do not remove or attempt to service the product by any unauthorized service center. This warranty is voided if (i) the product has been modified or repaired by any unauthorized service center, (ii) the product was subject to accident, abuse, or improper use (iii) the product was subject to conditions more severe than those specified in the manual.

Warranty service may be obtained by contacting TRENDnet within the applicable warranty period and providing a copy of the dated proof of the purchase. Upon proper submission of required documentation a Return Material Authorization (RMA) number will be issued. An RMA number is required in order to initiate warranty service support for all TRENDnet products. Products that are sent to TRENDnet for RMA service must have the RMA number marked on the outside of return packages and sent to TRENDnet prepaid, insured and packaged appropriately for safe shipment. Customers shipping from outside of the USA and Canada are responsible for return shipping fees. Customers shipping from outside of the USA are responsible for custom charges, including but not limited to, duty, tax, and other fees.

WARRANTIES EXCLUSIVE: IF THE TRENDNET PRODUCT DOES NOT OPERATE AS WARRANTED ABOVE, THE CUSTOMER'S SOLE REMEDY SHALL BE, AT TRENDNET'S OPTION, REPAIR OR REPLACE. THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ALL OTHER WARRANTIES, EXPRESSED OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. TRENDNET NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION MAINTENANCE OR USE OF TRENDNET'S PRODUCTS.

TRENDNET SHALL NOT BE LIABLE UNDER THIS WARRANTY IF ITS TESTING AND EXAMINATION DISCLOSE THAT THE ALLEGED DEFECT IN THE PRODUCT DOES NOT EXIST OR WAS CAUSED BY CUSTOMER'S OR ANY THIRD PERSON'S MISUSE, NEGLECT, IMPROPER INSTALLATION OR TESTING, UNAUTHORIZED ATTEMPTS TO REPAIR OR MODIFY, OR ANY OTHER CAUSE BEYOND THE RANGE OF THE INTENDED USE, OR BY ACCIDENT, FIRE, LIGHTNING, OR OTHER HAZARD.

LIMITATION OF LIABILITY: TO THE FULL EXTENT ALLOWED BY LAW TRENDNET ALSO EXCLUDES FOR ITSELF AND ITS SUPPLIERS ANY LIABILITY, WHETHER BASED IN CONTRACT OR TORT (INCLUDING NEGLIGENCE), FOR INCIDENTAL, CONSEQUENTIAL, INDIRECT, SPECIAL, OR PUNITIVE DAMAGES OF ANY KIND, OR FOR LOSS OF REVENUE OR PROFITS, LOSS OF BUSINESS, LOSS OF INFORMATION OR DATE, OR OTHER FINANCIAL LOSS ARISING OUT OF OR IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE, USE, PERFORMANCE, FAILURE, OR INTERRUPTION OF THE POSSIBILITY OF SUCH DAMAGES, AND LIMITS ITS LIABILITY TO REPAIR, REPLACEMENT, OR REFUND OF THE PURCHASE PRICE PAID, AT TRENDNET'S OPTION. THIS DISCLAIMER OF LIABILITY FOR DAMAGES WILL NOT BE AFFECTED IF ANY REMEDY PROVIDED HEREIN SHALL FAIL OF ITS ESSENTIAL PURPOSE.

Governing Law: This Limited Warranty shall be governed by the laws of the state of California.

Some TRENDnet products include software code written by third party developers. These codes are subject to the GNU General Public License ("GPL") or GNU Lesser General Public License ("LGPL").

Go to http://www.trendnet.com/gpl or http://www.trendnet.com Download section and look for the desired TRENDnet product to access to the GPL Code or LGPL Code. These codes are distributed WITHOUT WARRANTY and are subject to the copyrights of the developers. TRENDnet does not provide technical support for these codes. Please go to http://www.gnu.org/licenses/gpl.txt or http://www.gnu.org/licenses/lgpl.txt for specific terms of each license.

PWP05202009v2

TRENDnet®

Product Warranty Registration

Please take a moment to register your product online.
Go to TRENDnet's website at http://www.trendnet.com/register