Allied Telesis™

IS230-10GP

Industrial Ethernet Layer 2 Switch

Reference Guide

613-002602 Rev. D

Acknowledgments
Intel and Pentium are trademarks of Intel Corporation.
Microsoft Windows and MS-DOS are registered trademarks of Microsoft Corp.
All other product names or trademarks are properties of their respective owners.

www.alliedtelesis.com
Please verify specifications before quoting. This guide is intended for reference purposes only.
All product specifications are subject to change without notice.
© Allied Telesis, Inc. 2020

Table of Contents

List of Tables

Preface

This guide describes the basic features of the CLI user interface, the commands associated with each feature and examples of how the commands are used. The chapters included in this book are:

- ❐ Chapter 1, “Command-Line Interface Overview” on page 11
- ❐ Chapter 2, “Layer 2 Features” on page 13
- ❐ Chapter 3, “Security” on page 55
- ❐ Chapter 4, “Quality of Service” on page 63
- ❐ Chapter 5, “Management” on page 67
- ❐ Chapter 6, “Diagnostics” on page 87

The preface contains the following sections:

- ❐ “Safety Symbols Used in this Document” on page 8
- ❐ “Contact Allied Telesis” on page 9

Safety Symbols Used in this Document

This document uses the following conventions.

Note
Notes provide additional information.

Caution
Cautions inform you that performing or omitting a specific action may result in equipment damage or loss of data.

Warning
Warnings inform you that performing or omitting a specific action may result in bodily injury.

Warning
Laser warnings inform you that an eye or skin hazard exists due to the presence of a Class 1 laser device.

Warning
Warnings inform you of hot surfaces.

Contact Allied Telesis

If you need assistance with this product, you may contact Allied Telesis technical support by going to the Support & Services section of the Allied Telesis web site at **www.alliedtelesis.com/support**. You can find links for the following services on this page:

- ❐ 24/7 Online Support - Enter our interactive support center to search for answers to your questions in our knowledge database, check support tickets, learn about Return Merchandise Authorizations (RMAs), and contact Allied Telesis technical experts.
- ❐ USA and EMEA phone support - Select the phone number that best fits your location and customer type.
- ❐ Hardware warranty information - Learn about Allied Telesis warranties and register your product online.
- ❐ Replacement Services - Submit an RMA request via our interactive support center.
- ❐ Documentation - View the most recent installation guides, user guides, software release notes, white papers and data sheets for your product.
- ❐ Software Updates - Download the latest software releases for your product.

For sales or corporate contact information, go to **www.alliedtelesis.com/purchase** and select your region.

Chapter 1

Command-Line Interface Overview

The command-line interface (CLI) is the primary user interface used to configure, monitor, and maintain the AT-S230-10GP switch. The user interface allows you to directly execute CLI commands.

The following topics are included in this chapter:

- ❒ ”Initially Configuring a Device”
- ❒ ”Understanding Command Syntax”
- ❒ “Understanding Enable and Enable Secret Passwords” on page 12
- ❒ “Abbreviating Commands” on page 12

Initially Configuring a Device

The initial configuration of a device varies by platform. This document provides configuration information for the listed devices.

After initially configuring and connecting the AT-S230-10GP switch to the network, you can configure the device by using the remote access method, such as Telnet or Secure Shell (SSH), to access the CLI or by using the configuration method provided on the switch, such as Security Device Manager.

Accessing the CLI

To access the CLI interface, establish Ethernet or serial connectivity to the switch.

To connect by Ethernet, open a command prompt window and type:

```
telnet <switchip> (where <switchip> is the IP address of the switch)
```

Note
The default IP address of the switch is 192.168.1.1.

At the login prompt, type ***manager*** for the username and ***friend*** for the password. The switch will respond with “Managed switch configuration CLI ready”.

Understanding Command Syntax

The command syntax is the format used for entering CLI commands. The commands are derived from the use of the command, keywords, and arguments. The keywords are alphanumeric strings used literally, while arguments are used as placeholders for required values.

Understanding Enable and Enable Secret Passwords

Some privileged EXEC commands are used for actions that impact the system, and it is recommended that you set a password for these commands to prevent unauthorized use. Two types of passwords, enable (not encrypted) and enable secret (encrypted), can be set.

The following commands set these passwords and are issued in global configuration mode:

- enable password
- enable secret password

Abbreviating Commands

The CLI commands can be used in an abbreviated form to execute. The CLI recognizes the abbreviates uniquely identifying the command. In the following example the `show version` command is used to illustrate the correct usage:

Full command: `show version`

Correct abbreviation: `sh ver`

However, attempting to execute the `show` command by using the single letter `s` would be invalid as s may refer to the commands `show` or `save`. For the same reason the variable `version` cannot be abbreviated to a single `v` as it may represent the variable `vlan`, etc.

Full command: `show version`

Incorrect abbreviation: `s version`, `s ver`, `sh v`

Chapter 2

Layer 2 Features

The following feature commands are included in this chapter:

Port Configuration

Port Configuration describes how to use the user interface to configure switch port parameters.

Table 1.   Port Configuration

Function	Privilege	Description	Example
`[no] shutdown`	Admin EXEC	Use "shutdown" command to disable port and use "no shutdown" to enable port. If port is error disabled for any reason, use "no shutdown" command to recover the port manually.	This example shows how to modify port duplex configuration. switch(config)# interface fa1 switch(config-if)# shutdown"
`speed (10|100)`	Admin EXEC	Use "speed" command to change port speed configuration. The speed is only able to configure to the physical maximum speed. For example, in fast Ethernet port, speed 1000 is not available.	This example shows how to modify port speed configuration. switch(config)# interface fa2 switch(config-if)# speed auto 10/100
`speed (1000|)`	Admin EXEC		
`speed auto [(10|100|10/100)]`	Admin EXEC		
`speed auto [(1000|)]`	Admin EXEC		
`duplex (auto|full|half)`	Admin EXEC	Use "duplex" command to change port duplex configuration.	This example shows how to modify port duplex configuration. switch(config)# interface fa1 switch(config-if)# duplex full switch(config-if)# exit switch(config)# interface fa2 switch(config-if)# duplex half
`description WORD<1-" SYS_STR_CONST(SYS_PORTDESC_STR_LEN) ">`	Admin EXEC	Use "description" command to give the port a name to identify it easily. If description includes space character, please use double quotes to wrap it.	This example shows how to modify port descriptions. switch(config)# interface fa2 switch(config-if)# description "uplink port"
`no description`	Admin EXEC	Use no form to restore description to empty string.	

Table 1. Port Configuration (Continued)

Function	Privilege	Description	Example
[no] protected	Admin EXEC	Use "protected" command to protect port. Protected port is only allowed to communicate with unprotected port. In other words, protected port is not allowed to communicate with another protected port. Use no form to make port unprotected	This example shows how to configure ports fa1 and fa2 as protected ports. switch(config)# interface range fa1-2 switch(config-if-range)# protected

Flow Control

The switch maintains the orderly movement of data from an end-node through Flow Control in full duplex mode and Back Pressure in half duplex mode.

Table 2. Flow Control

Function	Privilege	Description	Example
[no] back-pressure	Admin EXEC	Use "back-pressure" command to change port back-pressure configuration. Use no form to restore back-pressure to default (off) configuration.	This example shows how to modify port duplex configuration. switch(config)# interface fa1 switch(config-if)# back-pressure switch(config-if)# no back-pressure
flowcontrol (off|on)	Admin EXEC	Use "flow-control" command to change port flow control configuration. Use off form to restore flow control to default (off) configuration.	This example shows how to modify port duplex configuration. switch(config)# interface fa1 switch(config-if)# flow-control on switch(config-if)# flow-control off

Port Mirror

Port mirroring function allows the sending of a copy of network packets seen on one switch port to a network monitoring connection on another switch port. Port mirroring can be used to analyze and debug data or diagnose errors on a network or to mirror either inbound or outbound traffic (or both).

Table 3. Port Mirror

Function	Privilege	Description	Example
`show mirror`	User EXEC	Display all mirror sessions.	switch# show mirror
`show mirror session <1-4>`	User EXEC	Specify the mirror session to display.	switch# show mirror session 1
`mirror session <1-4> source interfaces IF_PORTS (both|rx|tx)`	Admin EXEC	Specify the mirror session to configure. Specify the source interface, include physical ports and LA port. Specify the traffic direction to mirror.	switch# configure switch(config)# mirror session 1 source interface fa2-5 both switch(config)# exit
`mirror session <1-4> destination interface IF_NMLPORT [allow-ingress]`	Admin EXEC	Specify the mirror session to configure. Specify the SPAN destination. A destination must be a physical port. Enable ingress traffic forwarding.	switch# configure switch(config)# mirror session 1 destination interface fa1 switch(config)# exit
`no mirror session (<1-4>|all)`	Admin EXEC	Clear the configuration of specified mirror session. Clear the configuration of all the mirror sessions.	switch# configure switch(config)# no mirror session 1 switch(config)# exit
`no mirror session <1-4> destination interface IF_NMLPORT`	Admin EXEC	Delete the destination interface of the mirror session.	switch# configure switch(config)# no mirror session 1 destination interface fa1 switch(config)# exit
`no mirror session <1-4> source interfaces IF_PORTS (both|rx|tx)`	Admin EXEC	Delete the source interface of the mirror session. Delete the traffic direction of the mirror port.	switch# configure switch(config)# no mirror session 1 source interface fa2-5 both switch(config)# exit

Link Aggregation

The Link Aggregation function provides LAG information for each trunk. It displays membership status, link state and membership type for each port.

Table 4.   Link Aggregation

Function	Privilege	Description	Example
`show lag`	User EXEC	Use "show lag" command to show current LAG load balance algorithm and members active/inactive status.	This example shows how to show current LAG status. switch# show lag
`lag load-balance (src-dst-mac|src-dst-mac-ip|src-port)`	Admin EXEC	Link aggregation group port should transmit packets spread to all ports to balance traffic loading. Two algorithms are supported; use this command to select the required algorithm.	This example shows how to change load balance algorithm to src-dst-mac-ip. switch(config)# lag load-balance src-dst-mac-ip
`no lag load-balance`	Admin EXEC	Use no form to disable load-blance.	This example shows how to disable load balance algorithm. switch(config)# no lag load-balance
`lag <1-8> mode (static | active | passive)`	Admin EXEC	Link aggregation group function aggregates multiple physical ports into one logic port to increase bandwidth. This command makes normal port joins a normal port to a specific LAG logic port in static or dynamic mode.	This example shows how to create a dynamic LAG and join fa1-fa3 to this LAG. switch(config)# interface range fa1-3 switch(config-if)# lag 1 mode active
`no lag`	Admin EXEC	Use "no lag" to leave the LAG logic port.	This example shows how to remove gi1 from LAG. switch(config)# interface GigabitEthernet 1 switch(config-if)# no lag
`show lacp sys-id`	User EXEC		switch# show lacp sys-id 32768, 00e0.4c00.0000

Table 4. Link Aggregation (Continued)

Function	Privilege	Description	Example
show lacp (internal | neighbor) [detail]	User EXEC		switch# show lacp <1-8> LAG number counters Traffic information internal Internal information neighbor Neighbor information sys-id LACP System ID switch# show lacp internal detail Flags: S - Device is requesting Slow LACPDUs F - Device is requesting Fast LACPDUs A - Device is in Active mode P - Device is in Passive mode
show lacp counters	User EXEC		switch# show lacp counters LACPDUs LACPDUs Port Sent Recv Pkts Err --------------------------------------
clear lacp counters	User EXEC		switch# clear lacp counters <cr>
lacp system-priority <1-65535>	Admin EXEC	LACP system priority is used for two connected DUT to select master switch. Lower system priority value has higher priority. The DUT with higher priority can decide which ports are able to join the LAG.	This example shows how to configure lacp system priority to 1000. switch(config)# lacp system-priority 1000
no lacp system-priority	Admin EXEC	Use "no lacp system-priority" to restore to the default priority value. Use "show running-config" command to show configuration.	This example shows how to restore lacp system priority to default value. switch(config)# no lacp system-priority

Table 4. Link Aggregation (Continued)

Function	Privilege	Description	Example
`lacp port-priority <1-65535>`	Admin EXEC	LACP port priority is used for two connected DUT to select aggregation ports. Lower port priority value has higher priority. The port with higher priority will be selected into LAG first. Use "show running-config" command to show configuration.	This example shows how to configure interface fa1 lacp port priority to 100. switch(config)# interface fa1 switch(config-if)# lacp port-priority 100
`no lacp port-priority`	Admin EXEC	Use no form to restore port-priority to default value.	
`lacp timeout (long|short)`	Admin EXEC	LACP must send LACP packet to partner switch to check the link status. This command configures the LACP packet sending interval.	This example shows how to configure interface fa1 lacp timeout to short. switch(config)# interface fa1 switch(config-if)# lacp timeout short
`no lacp timeout`	Admin EXEC		

802.1Q VLAN

The 802.1Q VLAN feature allows for a single VLAN to support multiple VLANs. With the 802.1Q feature you can preserve VLAN IDs and segregate different VLAN traffic.

The 802.1Q VLAN tag feature encapsulates the 802.1Q VLAN tagging within another 802.1Q VLAN tag. The outer tag is assigned following the AP group, while the inner VLAN ID is assigned dynamically by the AAA server.

Table 5. 802.1Q VLAN

Function	Privilege	Description	Example
`show vlan default-vlan`	User EXEC	Display information about default VLAN.	switch# show vlan default-vlan
`show vlan VLAN-LIST interfaces IF_PORTS membership`	User EXEC	Display information about VLAN list.	switch# show vlan 1 interfaces GigabitEthernet 10 membership
`show vlan [(VLAN-LIST|dynamic|static)]`	User EXEC	Display information about VLAN list or dynamic or static.	switch# show vlan 1 switch# show vlan dynamic switch# show vlan static
`show interfaces IF_PORTS`	User EXEC	Use "show interface" command to show port counters, parameters and status.	show interfaces GigabitEthernet 1
`show interfaces IF_PORTS status`	User EXEC	Use "show interface" command to show port status.	show interfaces GigabitEthernet 1 status
`show interfaces IF_PORTS protected`	User EXEC	Use "show interface" command to show port protected status.	show interfaces GigabitEthernet 1 protected
`show interfaces switchport IF_PORTS`	User EXEC	Use "show interface switchport" command to show port VLAN status.	switch# show interfaces switchport GigabitEthernet 1
`[no] vlan VLAN-LIST`	Admin EXEC	Create or remove a VLAN entry. Using “vlan” command to enter the VLAN configuration mode.	switch (config)# vlan 100 switch (config)# no vlan 100
`name NAME`	Admin EXEC	Configure the name of a VLAN entry.	switch(config)# vlan 100 switch(config-vlan)# name VLAN-one-hundred

Table 5. 802.1Q VLAN (Continued)

Function	Privilege	Description	Example
`switchport mode hybrid`	Admin EXEC	Hybrid port: Support all functions as defined in IEEE 802.1Q specification.	switch(config-if)# switchport mode hybrid
`show management-vlan`	User EXEC	Display information about management VLAN.	switch(config)# show management-vlan
`switchport hybrid pvid <1-4094>`	Admin EXEC	This command configures the hybrid port's PVID. Use "show interface switchport" command to show configuration.	switch(config)# interface GigabitEthernet 1 switch(config-if)# switchport mode hybrid switch(config-if)# switchport hybrid pvid 100
`[no] switchport hybrid ingress-filtering`	Admin EXEC	This command per port configures the ingress-filtering status. This filtering is used to filter the frames come from the non-member ingress port. Use "show interface switchport" command to show configuration.	switch(config)# interface GigabitEthernet 1 switch(config-if)# switchport mode hybrid switch(config-if)# switchport hybrid ingress-filtering
`switchport hybrid acceptable-frame-type (all|tagged-only|untagged-only)`	Admin EXEC	This command per port configures the acceptable-frame-type. Use "show interface switchport" command to show configuration.	switch(config)# interface GigabitEthernet 1 switch(config-if)# switchport mode hybrid switch(config-if)# switchport hybrid acceptable-frame-type tagged-only
`switchport hybrid allowed vlan add VLAN-LIST [(tagged|untagged)]`	Admin EXEC	This command per hybrid port configures adds the allowed VLAN list. Use "show interface switchport" command to show configuration.	switch(config)# interface GigabitEthernet 1 switch(config-if)# switchport mode hybrid switch(config-if)# switchport hybrid allowed vlan add 1 tagged
`switchport hybrid allowed vlan remove VLAN-LIST`	Admin EXEC	This command per hybrid port configures removes the allowed VLAN list. Use "show interface switchport" command to show configuration.	switch(config)# interface GigabitEthernet 1 switch(config-if)# switchport mode hybrid switch(config-if)# switchport hybrid allowed vlan remove 100

Table 5. 802.1Q VLAN (Continued)

Function	Privilege	Description	Example
`[no] switchport default-vlan tagged`	Admin EXEC	This command per port configures the membership of the default VLAN to tagged. Use "show interface switchport" command to show configuration.	switch(config)# interface GigabitEthernet 1 switch(config-if)# switchport mode hybrid switch(config-if)# switchport default-vlan tagged
`[no] switchport forbidden default-vlan`	Admin EXEC	This command per port configures the membership of the default VLAN to forbidden. Use "show interface switchport" command to show configuration.	switch(config)# interface GigabitEthernet 1 switch(config-if)# switchport mode hybrid switch(config-if)# switchport forbidden default-vlan
`switchport forbidden vlan (add|remove) VLAN-LIST`	Admin EXEC	This command per port configures the membership of the specified VLANs to forbidden. Use "show interface switchport" command to show configuration.	switch(config)# interface GigabitEthernet 1 switch(config-if)# switchport mode hybrid switch(config-if)# switchport forbidden vlan 100

`management-vlan vlan <1-4094>`
`no management-vlan`
	Admin EXEC	(1) Set <1-4094> as management VLAN ID; it is recommended to first create the VLAN and then assign the port to it.
		(2) When using no command, restore management VLAN to default VLAN.
		(3) To view the created management VLAN, use "show management-vlan".
			(1) The following example specifies that management VLAN 2 is created.
			switch(config)# management-vlan vlan 2
			(2) The following example specifies that management-VLAN is restored to be default VLAN.
			switch(config)# no management-vlan

MAC Address Table

The MAC Address Table stores the information for the Static MAC Settings, MAC Aging Time, and Dynamic Forwarding for Ethernet traffic.

Table 6. MAC Address Table

Function	Privilege	Description	Example
`show mac address-table aging-time`	User EXEC	View the aging time of the address table.	switch# show mac address-table aging-time
`show mac address-table A:B:C:D:E:F [vlan <1-4094>]`	User EXEC	Displays entries for a specific MAC address (for all or VLAN).	switch# show mac address-table 0:1:2:3:4:5 vlan 1
`show mac address-table [vlan <1-4094>] [interfaces IF_PORTS]`	User EXEC	View MAC entry on specified interface or VLAN or all dynamic MAC entries in MAC address table.	switch# show mac address-table vlan 1 interface fa5
`show mac address-table static [vlan <1-4094>] [interfaces IF_PORTS]`	User EXEC	View static MAC entry on specified interface or VLAN or all dynamic MAC entries in MAC address table.	switch# show mac address-table static vlan 1 interface fa5
`show mac address-table dynamic [vlan <1-4094>] [interfaces IF_PORTS]`	User EXEC	View dynamic MACentry on specified interface or VLAN or all dynamic MAC entries in MAC address table.	switch# show mac address-table dynamic vlan 1 interface fa5
`show mac address-table counters`	User EXEC	Display the number of addresses present in MAC address table.	switch# show mac address-table counters
`clear mac address-table dynamic [interfaces IF_PORTS]`	Admin EXEC	Delete dynamic MAC entry on specified interface or all dynamic MAC entries in MAC address table.	switch(config)# clear mac address-table dynamic interfaces fa5
`clear mac address-table dynamic vlan <1-4094>`	Admin EXEC	Delete dynamic MAC entry on specified VLAN dynamic MAC entry in MAC address table.	switch(config)# clear mac address-table dynamic vlan 1
`mac address-table aging-time <10-630>`	Admin EXEC	Set the aging time of the address table.	switch(config)# mac address-table aging-time 300

Table 6. MAC Address Table (Continued)

Function	Privilege	Description	Example
`mac address-table static A:B:C:D:E:F vlan <1-4094> interfaces IF_PORTS`	Admin EXEC	Add static addresses to the MAC address table.	switch(config)# mac address-table static 0:1:2:3:4:5 vlan 1 interfaces fa5
`no mac address-table static A:B:C:D:E:F vlan <1-4094>`	Admin EXEC	Delete static addresses from the MAC address table.	switch(config)# no mac address-table static 0:1:2:3:4:5 vlan 1 interfaces fa5

Q-in-Q

Q-in-Q is commonly referred as VLAN stacking in which VLANs are nested by adding two tags to each frame instead of one. Network service provider and users both can use VLANs and makes it possible to have more than the 4094 separate VLANs allowed by 802.1Q.

There are three ways in which a machine can be connected to a network carrying double-tagged 802.1ad traffic:

- via a untagged port, where both inner and outer VLANs are handled by the switch or switches (so the attached machine sees ordinary Ethernet frames);
- via a single-tagged (tunnel) port, where the outer VLAN only is handled by the switch (so the attached machine sees single-tagged 802.1Q VLAN frames); or
- via a double-tagged (trunk) port, where both inner and outer VLANs are handled by the attached machine (which sees double-tagged 802.1ad VLAN frames).

Table 7. Q-in-Q

Function	Privilege	Description	Example
`switchport outerpvid <1-4094>`	Admin EXEC	This command configures the hybrid port’s Outer PVID. Use "show interface switchport" command to show configuration.	This example sets gi2's Outer PVID to 1024. switch(config)# interface GigabitEthernet 2 switch(config-if)# switchport outerpvid 1024
`switchport qinqmode (nni|uni)`	Admin EXEC	The qinqmode is used to configure the hybrid port for different port roles. Nni: transfer frame will be add outer tag Vlan-Identifier Uni: transfer frame will not be add outer tag Vlan-Identifier.	This example shows how to change gi1 to nni mode and gi2 to uni mode. switch(config)# interface GigabitEthernet 1 switch(config-if)# switchport qinqmode nni switch(config-if)# exit switch(config)# interface GigabitEthernet 2 switch(config-if)# switchport qinqmode uni
`vlan outertpid <0x0000-0xFFFF>`	Admin EXEC	Use "vlan outertpid" command to change outer VLAN's Tag Protocol Identifier (tpid) configuration.	This example shows how to modify Tag Protocol Identifier configuration. switch(config)# vlan outertpid 0x9100

GARP

The Generic Attribute Registration Protocol (GARP) is a local area network (LAN) protocol. The protocol defines procedures for the registration and de-registration of attributes (network identifiers or addresses) by end stations and switches with each other.

Table 8. GARP

Function	Privilege	Description	Example
`show garp`	User EXEC	Display GARP status.	switch# show garp
`garp join-time <6-600>`	Admin EXEC	Set interval of join timer.	switch(config)# garp join-time 10
`garp leave-time <12-3000>`	Admin EXEC	Set interval of leave timer.	switch(config)# garp leave-time 30
`garp leaveall-time <12-12000>`	Admin EXEC	Set interval of leave all timer.	switch(config)# garp leaveall-time 240
`garp timer join <6-600> leave <12-3000> leaveall <12-12000>`	Admin EXEC	Set interval of all timers.	switch(config)# garp timer join 10 leave 30 leaveall 240

GVRP

The GVRP Settings page allows you to enable or disable the GVRP (GARP VLAN Registration Protocol or Generic VLAN Registration Protocol) protocol which facilitates control of virtual local area networks (VLANs) within a larger network.

Table 9. GVRP

Function	Privilege	Description	Example
`show gvrp`	User EXEC	Display GVRP status.	switch# show gvrp
`[no] gvrp`	Admin EXEC	Enable or disable GVRP function.	switch(config)# gvrp

802.3az Energy Efficient Ethernet (EEE)

The EEE innovative green feature reduces energy consumption through intelligent functionality:

- Traffic detection — Energy Efficient Ethernet (EEE) compliance
- Inactive link detection

Inactive link detection function automatically reduces power usage when inactive links or devices are detected.

Figure 1. 802.3az Energy Efficient Ethernet (EEE)

Function	Privilege	Description	Example
eee	Admin EXEC	Enable EEE function.	switch(config)# interface GigabitEthernet 1 switch(config-if)# eee <cr>
[no] eee	Admin EXEC	Disable EEE function.	switch(config)# no eee

Multicast

Multicast forwarding allows a single packet to be forwarded to multiple destinations. The service is based on L2 switch receiving a single packet addressed to a specific Multicast address. Multicast forwarding creates copies of the packet, and transmits the packets to the relevant ports.

This section contains the following features:

- ❒ ”IGMP Snooping”
- ❒ “MLD Snooping” on page 34

IGMP Snooping

IGMP Snooping is defined as the process of listening to Internet Group Management Protocol (IGMP) network traffic. IGMP Snooping allows a network switch to listen in on the IGMP conversation between hosts and routers and maintain a map of which links need which IP multicast streams. Multicasts can be filtered from the links which do not need them in turn controlling which ports receive specific multicast traffic.

Table 10. IGMP Snooping

Function	Privilege	Description	Example
`show ip igmp snooping`	User EXEC	This command will display IP IGMP snooping global info.	switch# show ip igmp snooping
`show ip igmp snooping router`	User EXEC	This command will display the IP IGMP router info.	switch# show ip igmp snooping router
`show ip igmp snooping groups [(dynamic | static)]`	User EXEC	This command will display the IP IGMP groups for dynamic or static or all types.	switch# show ip igmp snooping groups switch# show ip igmp snooping groups dynamic switch# show ip igmp snooping groups static
`show ip igmp snooping vlan [VLAN-LIST]`	User EXEC	This command will display IP IGMP snooping VLAN info.	switch# show ip igmp snooping vlan
`show ip igmp snooping groups counters`	User EXEC	This command will display the IP IGMP group counter include static group.	switch# show ip igmp snooping counters
`show ip igmp snooping querier`	User EXEC	This command will display all of the static VLAN IP IGMP querier info.	switch# show ip igmp snooping querier

Table 10. IGMP Snooping (Continued)

Function	Privilege	Description	Example
`clear ip igmp snooping groups [(dynamic |static)]`	Admin EXEC	This command will clear the IP IGMP groups for dynamic or static or all types.	switch# clear ip igmp snooping groups static
`clear ip igmp snooping statistics`	Admin EXEC	This command will clear the IGMP statistics.	switch# clear ip igmp snooping statistics
`[no] ip igmp snooping`	Admin EXEC	"No IP IGMP snooping" will clear all ip igmp snooping dynamic groups and dynamic router ports, and make the static IP IGMP group invalid. Subsequently, dynamic group and router port will not be learned via IGMP message.	switch(config)# ip igmp snooping switch(config)# no ip igmp snooping
`[no] ip igmp snooping report-suppression`	Admin EXEC	"No IP IGMP snooping report-suppression" will disable IGMP v1/v2 IGMP report suppression function. When received, report will be forwarded to the VLAN router ports.	switch(config)# ip igmp snooping report-suppression switch(config)# no ip igmp snooping report-suppression

Table 10. IGMP Snooping (Continued)

Function	Privilege	Description	Example
`no ip igmp snooping vlan VLAN-LIST group A.B.C.D`	Admin EXEC	"IP IGMP snooping vlan 1 static-group 224.1.1.1 interfaces gi1" will add static group. The static group will not learn other dynamic ports. If the dynamic group exists, the static group will overlap the dynamic group. If the last member of the static group is removed, the static group will be deleted. To validate the static group, IGMP snooping VLAN and IP IGMP snooping must be enabled. Use "Show IP IGMP snooping group [(dynamic | static)]" command to display configuration. Use "No IP IGMP snooping vlan 1 group 224.1.1.1" command to delete the static group. The "clear ip igmp snooping groups" command can also be used to delete the static group.	switch(config)# ip igmp snooping vlan 1 static-group 224.1.1.1 interfaces gi1-2
`no ip unknown-multicast action`	Admin EXEC	When IGMP snooping and MLD snooping are disabled, router port actions cannot be set. Disabling IGMP snooping & MLD snooping will flood multicast traffic to all members of the VLAN. When the action is a router port flood or drop, it will delete the unknown multicast group entry.	switch(config)# ip unknown-multicast action router-port switch(config)# no ip unknown-multicast action

Table 10.   IGMP Snooping (Continued)

Function	Privilege	Description	Example
`ip unknown-multicast action (drop|flood|router-port)`	Admin EXEC	When igmp snooping and mld snooping disabled, it can’t set action router-port. When disable igmp snooping & mld snooping, it set unknown multicast action flood. When action is router-port to flood or drop, it will delete the unknown multicast group entry.	switch(config)# ip unknown-multicast action drop Drop the packets flood Flood the packets router-port Forward to router ports

Table 10. IGMP Snooping (Continued)

Function	Privilege	Description	Example

`[no] ip igmp snooping vlan VLAN-LIST fastleave`
`[no] ip igmp snooping vlan VLAN-LIST router learn pim-dvmrp`
`ip igmp snooping vlan VLAN-LIST robustness-variable <1-7>`
`no ip igmp snooping vlan VLAN-LIST robustness-variable`
`ip igmp snooping vlan VLAN-LIST response-time <5-20>`
`no ip igmp snooping vlan VLAN-LIST response-time`
`ip igmp snooping vlan VLAN-LIST query-interval <30-18000>`
`no ip igmp snooping vlan VLAN-LIST query-interval`
`ip igmp snooping vlan VLAN-LIST last-member-query-interval <1-25>`
`no ip igmp snooping vlan VLAN-LIST last-member-query-interval`
`ip igmp snooping vlan VLAN-LIST last-member-query-count <1-7>`
`no ip igmp snooping vlan VLAN-LIST last-member-query-count`
	Admin EXEC	"No IP IGMP snooping vlan 1 (last-member-query-count | last-member-query-interval | query-interval | response-time | robustness-variable)" will set the VLAN parameters to default.
		The CLI setting will change the IP IGMP VLAN parameters admin settings.
			switch(config)# ip igmp snooping vlan 1 fastleave
			switch(config)# ip igmp snooping vlan 1 last-member-query-count 5
			switch(config)# ip igmp snooping vlan 1 last-member-query-interval 3
			switch(config)# ip igmp snooping vlan 1 query-interval 100
			switch(config)# ip igmp snooping vlan 1 response-time 12
			switch(config)# ip igmp snooping vlan 1 robustness-variable 4

Table 10. IGMP Snooping (Continued)

Function	Privilege	Description	Example
`[no] ip igmp snooping vlan VLAN-LIST`	Admin EXEC	"No IP IGMP snooping vlan 1" will clear all VLAN IP IGMP snooping dynamic groups and dynamic router ports, and invalidate any static IP IGMP groups with a VLAN ID of 1. Subsequently, the dynamic groups and router ports will not be learned via IGMP message for VLAN 1.	switch(config)# ip igmp snooping vlan 1
`ip igmp snooping version (2|3)`	Admin EXEC	"IP IGMP snooping version 3" supports v3 basic mode. When the version changes from v3 to v2, all querier versions will update to version 2.	switch(config)# ip igmp snooping version 3

`ip igmp snooping vlan VLAN-LIST querier [version (2|3)]`
`no ip igmp snooping vlan VLAN-LIST querier`
	Admin EXEC	When IP IGMP vlan querier is enabled, a router selection process will be triggered. The selected router will send a general and specific query.	switch(config)# ip igmp snooping vlan 2 querier

MLD Snooping

The MLD Snooping page allows you to select the snooping status (enable or disable), the version (v1 or v2) and the enabling/disabling of the report suppression for the MLD querier, which sends out periodic general MLD queries and are forwarded through all ports in the VLAN.

Table 11. MLD Snooping

Function	Privilege	Description	Example
`show ip mld snooping`	User EXEC	This command will display IP MLD snooping global info.	switch# show ip mld snooping
`show ip mld snooping router`	User EXEC	This command will display the IP MLD router info.	switch# show ip mld snooping router
`show ip mld snooping groups [(dynamic | static)]`	User EXEC	This command will display the IP MLD groups for dynamic or static ports, or for all types.	switch# show ip mld snooping groups switch# show ip mld snooping groups dynamic Switch# show ip mld snooping groups static
`show ip mld snooping vlan [VLAN-LIST]`	User EXEC	This command will display IP MLD snooping VLAN info.	switch# show ip mld snooping vlan
`show ip mld snooping groups counters`	User EXEC	This command will display the IP MLD group counter include static group.	switch# show ip mld snooping counters
`show ip mld snooping querier`	User EXEC	This command will display all of the static VLAN IP MLD querier info.	switch# show ip mld snooping querier
`clear ip mld snooping groups [(dynamic |static)]`	Admin EXEC	This command will clear the IP MLD groups for dynamic or static ports, or for all types.	switch# clear ip mld snooping groups static
`clear ip mld snooping statistics`	Admin EXEC	This command will clear the MLD statistics.	switch# clear ip mld snooping statistics

Table 11. MLD Snooping (Continued)

Function	Privilege	Description	Example
`[no] ip mld snooping`	Admin EXEC	"No IP MLD snooping" will clear all IP MLD snooping dynamic groups and dynamic router ports, and make the static IP MLD group invalid. Subsequently, the dynamic group and router ports will not be learned via MLD message.	switch(config)# ip mld snooping switch(config)# no ip mld snooping
`[no] ip mld snooping report-suppression`	Admin EXEC	"No IP MLD snooping report-suppression" will disable MLD v1/v2 MLD report suppression function. Reports received will be forwarded to the VLAN router ports.	switch(config)# ip mld snooping report-suppression switch(config)# no ip mld snooping report-suppression

Table 11. MLD Snooping (Continued)

Function	Privilege	Description	Example

`[no] ip mld snooping vlan VLAN-LIST static-group X:X::X:X interfaces IF_PORTS`
`no ip mld snooping vlan VLAN-LIST group X:X::X:X`
	Admin EXEC	IP MLD snooping vlan 1 static-group ff0e:dd::00:dd interfaces gi1" will add static group. The static group willl not learn other dynamic ports. If the dynamic group exists, the static group will overlap the dynamic group. If the last member of the static group is removed, the static group will be deleted.
		For the static group to be valid, IGMP snooping VLAN and IP IGMP snooping must both be enabled.
		Use "Show IP IGMP snooping group [(dynamic | static)]" to display the configuration.
		Use "No IP MLD snooping vlan 1 group ff0e:dd::00:dd" or "Clear IP MLD snooping groups" to delete the static group.
			switch(config)# ip mld snooping vlan 1 static-group ff0e:dd::00:dd interfaces gi1-2

Table 11. MLD Snooping (Continued)

Function	Privilege	Description	Example

`[no] ip mld snooping vlan VLAN-LIST fastleave`
`[no] ip mld snooping vlan VLAN-LIST router learn pim-dvmrp`
`ip mld snooping vlan VLAN-LIST robustness-variable <1-7>`
`no ip mld snooping vlan VLAN-LIST robustness-variable`
`ip mld snooping vlan VLAN-LIST response-time <5-20>`
`no ip mld snooping vlan VLAN-LIST response-time`
`ip mld snooping vlan VLAN-LIST query-interval <30-18000>`
`no ip mld snooping vlan VLAN-LIST query-interval`
`ip mld snooping vlan VLAN-LIST last-member-query-interval <1-25>`
`no ip mld snooping vlan VLAN-LIST last-member-query-interval`
`ip mld snooping vlan VLAN-LIST last-member-query-count <1-7>`
`no ip mld snooping vlan VLAN-LIST last-member-query-count`
	Admin EXEC	"No IP MLD snooping vlan 1 (last-member-query-count | last-member-query-interval | query-interval | response-time | robustness-variable)" will set the VLAN parameters to default.
		The CLI setting will change the IP MLD vlan parameters admin settings.
			switch(config)# ip mld snooping vlan 1 fastleave
			switch(config)# ip mld snooping vlan 1 last-member-query-count 5
			switch(config)# ip mld snooping vlan 1 last-member-query-interval 3
			switch(config)# ip mld snooping vlan 1 query-interval 100
			switch(config)# ip mld snooping vlan 1 response-time 12
			switch(config)# ip mld snooping vlan 1 robustness-variable 4

Table 11. MLD Snooping (Continued)

Function	Privilege	Description	Example
`[no] ip mld snooping vlan VLAN-LIST`	Admin EXEC	"No IP MLD snooping vlan 1" will clear vlan all IP MLD snooping dynamic group and dynamic router ports, and invalidate any static IP MLD group invalid with a VLAN ID of 1. Subsequently, the dynamic group and router ports will not be learned via MLD message for VLAN 1.	switch(config)# ip mld snooping vlan 1
`ip mld snooping version (1|2)`	Admin EXEC	"IP MLD snooping version 2", supports v2 basic mode. When the version changes from v2 to v1, all querier versions will update to version 2.	switch(config)# ip mld snooping version 2

`ip mld snooping vlan VLAN-LIST querier [version (1|2)]`
`no ip mld snooping [vlan VLAN-LIST] querier`
	Admin EXEC	When enable IP MLD vlan querier is enabled, a router selection process will be triggered. The selected router will send a general and specific query.	switch(config)# ip mld snooping vlan 2 querier

Jumbo Frame

Jumbo frames are frames larger than the standard Ethernet frame size of 1518 bytes. The Jumbo Frame function allows the configuration of Ethernet frame size.

Table 12. Jumbo Frame

Function	Privilege	Description	Example
`jumbo-frame <1518-9216>`	Admin EXEC	Use "jumbo-frame" command to modify maximum frame size. The only way to show this configuration is by using "show running-config" command.	This example shows how to modify maximum frame size to 9216 bytes. switch(config)#jumbo-frame 9216
`no jumbo-frame`	Admin EXEC	Use no form to disable jumbo-frame.	switch(config)# no jumbo-frame

Spanning Tree

The Spanning Tree Protocol (STP) is a network protocol to ensure loop-free topology for any bridged Ethernet local area network.

Table 13. Spanning Tree

Function	Privilege	Description	Example
`show spanning-tree [instance <0-15>]`	User EXEC	Show spanning-tree instance information.	switch# show spanning-tree instance 10
`show spanning-tree interfaces IF_PORTS [instance <0-15>]`	User EXEC	Show spanning-tree instance information per port.	switch# show spanning-tree interface gi1 instance 10
`show spanning-tree`	User EXEC	Show spanning-tree information.	switch# show spanning-tree
`show spanning-tree interfaces IF_PORTS`	User EXEC	Show spanning-tree state of one port.	switch# show spanning-tree interface gi1
`show spanning-tree interfaces IF_PORTS statistic`	User EXEC	Show spanning-tree statistics of one port.	switch# show spanning-tree interface gi1 statistic

Table 13. Spanning Tree (Continued)

Function	Privilege	Description	Example
`[no] spanning-tree`	Admin EXEC	Enable or Disable Spanning-Tree Protocol.	switch# configure switch(config)# spanning-tree switch(config)# exit
`spanning-tree bpdu (filtering|flooding)`	Admin EXEC	Specify the forwarding action of BPDU to filtering or flooding.	switch# configure switch(config)# spanning-tree bpdu filtering switch(config)# exit
`no spanning-tree bpdu`	Admin EXEC	Restore to default BPDU action. Default action is flooding.	switch# configure switch(config)# no spanning-tree bpdu switch(config)# exit"
`spanning-tree mode (stp|rstp|mstp)`	Admin EXEC	Specify the mode to Spanning Tree Protocol. Specify the mode to Rapid Spanning Tree Protocol. Specify the mode to Multiple Spanning Tree Protocol.	switch# configure switch(config)# spanning-tree mode stp switch(config)# exit
`no spanning-tree force-version`	Admin EXEC	Restore to default stp version. Default stp version is rstp.	switch# configure switch(config)# no spanning-tree force-version switch(config)# exit
`spanning-tree priority <0-61440>`	Admin EXEC	Specify the bridge priority; must use multiples of 4096.	switch# configure switch(config)# spanning-tree priority 16384 switch(config)# exit
`no spanning-tree priority`	Admin EXEC	Restore to default priority. Default priority is 32768.	switch# configure switch(config)# no spanning-tree priority switch(config)# exit
`spanning-tree hello-time <1-10>`	Admin EXEC	Specify the hello-time interval (seconds).	switch# configure switch(config)# spanning-tree hello-time 5 switch(config)# exit
`no spanning-tree hello-time`	Admin EXEC	Restore to default hello-time. Default hello-time is 2.	switch# configure switch(config)# no spanning-tree hello-time switch(config)# exit

Table 13. Spanning Tree (Continued)

Function	Privilege	Description	Example
`spanning-tree forward-delay <4-30>`	Admin EXEC	Specify the forward-delay interval (seconds).	switch# configure switch(config)# spanning-tree forward-delay 30 switch(config)# exit
`no spanning-tree forward-delay`	Admin EXEC	Restore to default forward-delay. Default forward-delay is 15.	switch# configure switch(config)# no spanning-tree forward-delay switch(config)# exit
`spanning-tree maximum-age <6-40>`	Admin EXEC	Specify the maximum-age time (seconds).	switch# configure switch(config)# spanning-tree maximum-age 10 switch(config)# exit
`no spanning-tree maximum-age`	Admin EXEC	Restore to default maximum-age. Default maximum-age is 20.	switch# configure switch(config)# no spanning-tree maximum-age switch(config)# exit
`spanning-tree tx-hold-count <1-10>`	Admin EXEC	Specify the tx-hold-count value.	switch# configure switch(config)# spanning-tree tx-hold-count 10 switch(config)# exit
`no spanning-tree tx-hold-count`	Admin EXEC	Restore to default tx-hold-count. Default tx-hold-count is 6.	switch# configure switch(config)# no spanning-tree tx-hold-count switch(config)# exit
`spanning-tree pathcost method (long|short)`	Admin EXEC	Specify the type of pathcost value as 32 bits (long). Specify the type of pathcost value as 16 bits (short).	switch# configure switch(config)# spanning-tree pathcost method short switch(config)# exit
`[no] spanning-tree`	Admin EXEC	Enable or Disable Spanning-Tree Protocol per port.	switch# configure switch(config)# interface gi1 switch(config-if)# spanning-tree switch(config-if)# exit switch(config)# exit
`spanning-tree port-priority <0-240>`	Admin EXEC	Specify the STP port priority; must use multiples of 16.	switch# configure switch(config)# interface gi1 switch(config-if)# spanning-tree port-priority 64 switch(config-if)# exit switch(config)# exit

Table 13. Spanning Tree (Continued)

Function	Privilege	Description	Example
`no spanning-tree port-priority`	Admin EXEC	Restore to default port-priority. Default port-priority is 128.	switch# configure switch(config)# interface gi1 switch(config-if)# no spanning-tree port-priority switch(config-if)# exit switch(config)# exit
`spanning-tree cost long <0-200000000>`	Admin EXEC	Specify the STP port cost. In long pathcost method, the range is from 0 to 20000000. (0 = Auto)	switch# configure switch(config)# interface gi1 switch(config-if)# spanning-tree cost long 200000 switch(config-if)# exit switch(config)# exit
`spanning-tree cost short <0-65535>`	Admin EXEC	Specify the STP port cost. In short pathcost method, the range is from 0 to 65535. (0 = Auto).	switch# configure switch(config)# interface gi1 switch(config-if)# spanning-tree cost short 1000 switch(config-if)# exit switch(config)# exit
`no spanning-tree cost`	Admin EXEC	Restore to default cost per port. Default cost is 0.	switch# configure switch(config)# interface gi1 switch(config-if)# no spanning-tree cost switch(config-if)# exit switch(config)# exit
`[no] spanning-tree edge`	Admin EXEC	Enable or Disable Spanning-Tree edge.	switch# configure switch(config)# interface gi1 switch(config-if)# spanning-tree edge switch(config-if)# exit switch(config)# exit
`spanning-tree link-type point-to-point`	Admin EXEC	Specify the STP port link-type to point-to-point.	switch# configure switch(config)# interface gi1 switch(config-if)# spanning-tree link-type point-to-point switch(config-if)# exit switch(config)# exit
`no spanning-tree link-type point-to-point`	Admin EXEC	Disable the STP port link-type from point-to-point.	switch# configure switch(config)# interface gi1 switch(config-if)# no spanning-tree link-type point-to-point switch(config-if)# exit switch(config)# exit

Table 13. Spanning Tree (Continued)

Function	Privilege	Description	Example
`spanning-tree mcheck`	Admin EXEC	Specify the STP port to migrate port.	switch# configure switch(config)# interface gi1 switch(config-if)# spanning-tree mcheck switch(config-if)# exit switch(config)# exit
`spanning-tree mst-config-id revision-level LEVEL<0-65535>`	Admin EXEC	Specify the MSTP mst-config-id revision level.	switch# configure switch(config)# spanning-tree mst-config-id revision-level 100 switch(config)# exit
`spanning-tree mst-config-id name NAME<32>`	Admin EXEC	Specify the MSTP mst-config-id name.	switch# configure switch(config)# spanning-tree mst-config-id name MST1 switch(config)# exit
`[no] spanning-tree instance-id INST<1-15>`	Admin EXEC	Create or delete MSTP instance ID.	switch# configure switch(config)# spanning-tree instance-id 10 switch(config)# exit
`spanning-tree instance-id INST<1-15> vlan (add|remove) VLAN-LIST`	Admin EXEC	Add or remove VLAN from instance.	switch# configure switch(config)# spanning-tree instance-id 10 vlan add 10-20 switch(config)# exit
`spanning-tree instance-id INST<1-15> priority VALUE<0-61440>`	Admin EXEC	Specify the instance priority.	switch# configure switch(config)# spanning-tree instance-id 10 priority 1000 switch(config)# exit

X-Ring Elite

The X-Ring Elite function provides an improvement over Spanning Tree and Rapid Spanning Tree and a rapid auto recovery in the event that the network suffers a corrupt or broken link and prevents network loops.

Table 14. X-Ring Elite

Function	Privilege	Description	Example
`show xring-elite`	User EXEC	Display xring-elite status.	switch# show xring-elite
`[no] xring-elite`	Admin EXEC	Disable or enable xring-elite function.	switch(config)# no xring-elite switch(config)# xring-elite
`xring-elite ring-id <1-255> ports IF_PORTS`	Admin EXEC	Create a normal ring.	switch(config)# xring-elite ring-id 1 ports GigabitEthernet 1,2
`xring-elite legacy ring-id <1-255> ports IF_PORTS`	Admin EXEC	Create a legacy ring.	switch(config)# xring-elite legacy ring-id 2 ports GigabitEthernet 3,4
`no xring-elite ring-id <1-255>`	Admin EXEC	Delete a normal ring or legacy ring.	switch(config)# no xring-elite ring-id 1
`show xring-plus`	User EXEC	Display xring-plus status.	switch# show xring-plus
`[no] xring-plus`	Admin EXEC	Disable or enable xring-plus function.	switch(config)# no xring-plus switch(config)# xring-plus
`xring-plus create ring-id <1-255> interface IF_PORT interface IF_PORT`	Admin EXEC	Create a ring.	switch(config)# xring-plus create ring-id 5 interface GigabitEthernet 1 interface GigabitEthernet 2
`xring-plus create ring-id <1-255> coupling interfaces IF_PORTS master-ring ring-id <1-255>`	Admin EXEC	Create a coupling.	switch(config)# xring-plus create ring-id 6 coupling interfaces 3 master-ring ring-id 5 switch(config)# xring-plus create ring-id 6 coupling interfaces 3,4 master-ring ring-id 5
`xring-plus delete ring-id <1-255>`	Admin EXEC	Delete a ring or coupling.	switch(config)# xring-plus delete ring-id 5

Loop Detection / Prevention

The Loopback Detection function is used to detect looped links. By sending detection frames and then checking to see if the frames returned to any port on the device, the function is used to detect loops.

Table 15. Loop Detection / Prevention

Function	Privilege	Description	Example
`show loopback-detection`	User EXEC	Display loopback-detection global status.	switch# show loopback-detection
`show loopback-detection interfaces IF_PORTS state`	User EXEC	Display loopback-detection status of specified ports.	show loopback-detection interfaces GigabitEthernet 1,2 state
`[no] loopback-detection`	Admin EXEC	Enable or disable loopback-detection.	switch(config)# loopback-detection switch(config)# no loopback-detection
`loopback-detection interval <1-32767>`	Admin EXEC	Set loopback detection interval.	switch(config)# loopback-detection interval 1
`loopback-detection recover-time <60-1000000>`	Admin EXEC	Set block port recover time.	switch(config)# loopback-detection recover-time 60
`[no] loopback-detection`	Admin EXEC	Enable or disable loopback-detection of a specified port.	switch(config-if)# loopback-detection switch(config-if)# no loopback-detection

Ethernet CFM

Ethernet Connectivity Fault Management (CFM) is an operation, administration, and management (OAM) protocol. Ethernet CFM provides the network operator with a way to detect faults in the network, and to isolate the location of the fault at either the link level (i.e., port) or at the VLAN level.

Table 16. Ethernet CFM

Function	Privilege	Description	Example
`show cfm hierarchy`	User EXEC	Display CFM hierarchy.	switch# show cfm hierarchy
`show cfm [mep <1-255>]`	User EXEC	Display CFM information.	switch# show cfm switch# show cfm mep 1
`show cfm statistics`	User EXEC	Display CFM statistics.	switch# show cfm statistics
`[no] cfm`	Admin EXEC	Enable or Disable CFM Protocol.	switch(config)# cfm switch(config)# no cfm

Table 16. Ethernet CFM (Continued)

Function	Privilege	Description	Example
`cfm md WORD<1-22> level <0-7>`	Admin EXEC	Create an MD and set the level of an MD.	switch(config)# cfm md test0 level 1
`no cfm md WORD<1-22>`	Admin EXEC	Delete an MD.	switch(config)# no cfm md test0
`cfm ma WORD<1-22> md WORD<1-22> interval (100ms | 1s | 10s | 1min | 10min) primary-vlan <1-4094>`	Admin EXEC	Create an MA in an MD and set the interval, primary-vlan.	switch(config)# cfm ma test1 md test0 interval 1min primary-vlan 10
`no cfm ma WORD<1-22>`	Admin EXEC	Delete an MA.	switch(config)# no cfm ma test1
`cfm mep <1-255> ma WORD<1-22>`	Admin EXEC	Create an MEP in an MA.	switch(config)# cfm mep 1 ma test1
`no cfm mep <1-255>`	Admin EXEC	Delete an MEP.	switch(config)# no cfm mep 1
`cfm mep <1-255> port IF_PORT`	Admin EXEC	Set the port of an MEP	switch(config)# cfm mep 1 port GigabitEthernet 1
`cfm mep <1-255> direction (down | up)`	Admin EXEC	Set the direction (up or down) of an MEP	switch(config)# cfm mep 1 direction up
`[no] cfm mep <1-255> peer-mep <1-255>`	Admin EXEC	Set the mep and peer-mep. Use no form to delete mep and peer-mep.	switch(config)# cfm mep 1 peer-mep 2 switch(config)# no cfm mep 1 peer-mep 2
`[no] cfm mep <1-255> enable (cc | lb)`	Admin EXEC	Set the enable setting to cc or lb of the MEP. Use no form to clear enable setting of the MEP.	switch(config)# cfm mep 1 enable cc switch(config)# no cfm mep 1 enable cc
`cfm mep <1-255> start lb`	Admin EXEC	Start sending lb packet to test.	switch(config)# cfm mep 1 start lb
`cfm mep <1-255> start lb peer-mep <1-255>`	Admin EXEC	Start sending lb packet to peer-mep to test.	switch(config)# cfm mep 1 start lb peer-mep 2
`[no] cfm debug (handler | state | action | logic | packet | database | timer | identify)`	Admin EXEC	Set the debug mode for CFM. Use no form to delete debug from CFM.	switch(config)# cfm debug state switch(config)# no cfm debug state

EPSR Transit

Ethernet Protection Switched Ring (ESPR) provides extremely fast failover between nodes in a resilient ring. EPSR enables rings to recover within as little as 50ms, preventing a node or link failure from affecting customer experience, even with demanding applications such as IP telephony and streaming video.

Table 17. EPSR Transit

Function	Privilege	Description	Example
`show epsr [NAME]`	User EXEC	Display EPSR domain information.	switch# show epsr switch# show epsr epsr-name
`show epsr [NAME] config-check`	User EXEC	Display EPSR config error check.	switch# show epsr config-check switch# show epsr epsr-name config-check
`show epsr [NAME] counter`	User EXEC	Display EPSR counters.	switch# show epsr counter switch# show epsr epsr-name counter
`epsr configuration`	Admin EXEC	Configure EPSR function.	switch(config)# epsr configuration
`epsr NAME mode transit controlvlan <2-4094>`	Admin EXEC	Create the EPSR domain transit mode entry.	switch(config-epsr)# epsr epsr-name mode transit controlvlan 2
`no epsr NAME`	Admin EXEC	Delete the EPSR domain transit mode entry.	switch(config-epsr)# no epsr epsr-name
`[no] epsr NAME datavlan VLAN-LIST`	Admin EXEC	Add data VLANs of a EPSR domain entry. Use no form to remove data VLANs from a EPSR domain entry.	switch(config-epsr)# epsr epsr-name datavlan 10,12-14 switch(config-epsr)# no epsr epsr-name datavlan 10,12-14
`[no] epsr NAME trap`	Admin EXEC	Enable or Disable the trap setting of a EPSR domain entry.	switch(config-epsr)# epsr epsr-name trap switch(config-epsr)# no epsr epsr-name trap
`[no] epsr NAME topology-change g8032`	Admin EXEC	Enable or Disable the topology change by g8032 setting of a EPSR domain entry.	switch(config-epsr)# epsr epsr-name topology-change g8032 switch(config-epsr)# no epsr epsr-name topology-change g8032
`epsr NAME state (enable | disable)`	Admin EXEC	Enable or Disable the state of a EPSR domain entry.	switch(config-epsr)# epsr epsr-name state enable switch(config-epsr)# epsr epsr-name state disable

ERPS (G.8032)

The International Telecommunication Union (ITU)-T G.8032 Ethernet Ring Protection Switching (ERPS) prevents loops on a per-VLAN basis with networks that are wired in a simple ring topology, and multiple ring and ladder topologies. G.8032 offers a rapid detection and recovery time if a link or node fails (in the order of 50 ms, depending on configuration).

Table 18. ERPS (G.8032)

Function	Privilege	Description	Example
`show erps`	User EXEC	Display ERPS information.	switch# show erps
`[no] erps`	Admin EXEC	Enable or Disable ERPS Protocol.	switch(config)# erps switch(config)# no erps
`[no] erp instance <1-8>`	Admin EXEC	Add or delete erps instance.	switch(config)# erp instance 1 switch(config)# no erp instance 1
`ring-id <1-255> rpl-owner east-link IF_PORT [rpl] west-link IF_PORT [rpl]`	Admin EXEC	Set the RING ID, RPL owner and ports for the ERPS ring	switch(config-erp-inst)# ring-id 1 rpl-owner east-link GigabitEthernet 1 west-link GigabitEthernet 2 switch(config-erp-inst)# ring-id 1 rpl-owner east-link GigabitEthernet 1 rpl west-link GigabitEthernet 2 rpl
`ring-id <1-255> rpl-neighbor east-link IF_PORT [rpl] west-link IF_PORT [rpl]`	Admin EXEC	Set the RING ID, RPL neighbor and ports for the ERPS ring	switch(config-erp-inst)# ring-id 1 rpl-neighbor east-link GigabitEthernet 1 west-link GigabitEthernet 2 switch(config-erp-inst)# ring-id 1 rpl-neighbor east-link GigabitEthernet 1 rpl west-link GigabitEthernet 2 rpl
`ring-id <1-255> other east-link IF_PORT [rpl] west-link IF_PORT [rpl]`	Admin EXEC	Set the RING ID, other roles and ports for the ERPS ring	switch(config-erp-inst)# ring-id 1 other east-link GigabitEthernet 1 west-link GigabitEthernet 2 switch(config-erp-inst)# ring-id 1 other east-link GigabitEthernet 1 rpl west-link GigabitEthernet 2 rpl
`aps-message-level <0-7>`	Admin EXEC	Set the APS message level in the range of 0 to 7	switch(config-erp-inst)# aps-message-level 1
`aps-channel-vlan <1-4094>`	Admin EXEC	Set the APS channel VLAN in the range of 1-4094	switch(config-erp-inst)# aps-channel-vlan 100
`traffic-channel-instance INST<0-15>`	Admin EXEC	Set the traffic channel instance in the range of 0-15	switch(config-erp-inst)# traffic-channel-instance 1

Table 18. ERPS (G.8032) (Continued)

Function	Privilege	Description	Example
`[interconnected] major-ring`	Admin EXEC	Set the major ring mode for an ERPS ring. Use interconnected form to assign device to "interconnected". It should set "sub-ring", too.	switch(config-erp-inst)# interconnected major-ring switch(config-erp-inst)# major-ring
`[interconnected] sub-ring [(with-virtual-channel | without-virtual-channel)] [tc-propagation]`	Admin EXEC	Set the sub ring mode for an ERPS ring and set with-virtual-channel or without-virtual-channel, or set tc-propagation. Use interconnected form to assign device is "interconnected". It should set "major ring", too.	switch(config-erp-inst)# interconnected sub-ring without-virtual-channel tc-propagation switch(config-erp-inst)# sub-ring with-virtual-channel tc-propagation switch(config-erp-inst)# interconnected sub-ring tc-propagation switch(config-erp-inst)# sub-ring
`[no] revertive`	Admin EXEC	Set the revertive mode for an ERPS ring. Use no form to delete entries from an ERPS ring.	switch(config-erp-inst)# revertive switch(config-erp-inst)# no revertive
`wtr <1-12>`	Admin EXEC	Set WTR timer (1 Unit = 1 minute, between 1 and 12 mins)	switch(config-erp-inst)# wtr 1
`guard <1-200>`	Admin EXEC	Set Guard timer (1 Unit = 10 ms, between 10 ms and 2 seconds).	switch(config-erp-inst)# guard 10
`hold-off <0-100>`	Admin EXEC	Set Hold-off timer (1 Unit = 100 ms, between 0 and 10 seconds).	switch(config-erp-inst)# hold-off 10
`clear`	Admin EXEC	Clear the settings of the ERPS instance.	switch(config-erp-inst)# clear
`port IF_PORT (fs | ms)`	Admin EXEC	Set the port in FS or MS mode	switch(config-erp-inst)# port GigabitEthernet 1 fs
`port IF_PORT monitor-instance <1-255>`	Admin EXEC	Set the port to monitor instance	switch(config-erp-inst)# port GigabitEthernet 1 monitor-instance 1
`[no] erps debug (handler | state | action | logic | packet | database | timer)`	Admin EXEC	Set the debug mode for an ERPS ring. Use no form to delete debug from an ERPS ring.	switch(config)# erps debug handler switch(config)# no erps debug handler

IP Source Guard

Dynamic Host Configuration Protocol (DHCP) servers allocate IP addresses to clients, and the switch keeps a record of addresses issued on each port. IP Source Guard checks against this DHCP snooping database to ensure only clients with specific IP and/or MAC address can access the network.

Table 19. IP Source Guard

Function	Privilege	Description	Example
`show ip-source verify`	User EXEC	Display IP Source Guard information.	switch# show ip-source verify
`ip-source binding src-mac A:B:C:D:E:F src-ip A.B.C.D interfaces IF_NMLPORT`	Admin EXEC	Add binding entries to IP Source Guard table.	switch(config)# ip-source binding src-mac 00:00:00:11:22:33 src-ip 192.168.1.20 interface GigabitEthernet 1
`no ip-source binding src-mac A:B:C:D:E:F src-ip A.B.C.D`	Admin EXEC	Delete binding entries from IP Source Guard table.	switch(config)# no ip-source binding src-mac 00:00:00:11:22:33 src-ip 192.168.1.20
`ip-source verify interface IF_NMLPORT`	Admin EXEC	Set the verify interfaces.	switch(config)# ip-source verify interface GigabitEthernet 1
`no ip-source verify`	Admin EXEC	Clear the verify interfaces	switch(config)# no ip-source verify

ARP Spoofing

Allied Telesis switches use Dynamic Host Configuration Protocol (DHCP) Snooping with Address Resolution Protocol (ARP) Security to protect your network from ARP spoofing attacks. All ARP replies from untrusted ports are checked to ensure they contain legitimate network addressing information, safeguarding the network and the business.

Table 20. ARP Spoofing

Function	Privilege	Description	Example
`show arp-spoofing`	User EXEC	Display ARP snooping information.	switch# show arp-spoofing
`[no] arp-spoofing src-mac A:B:C:D:E:F src-ip A.B.C.D`	Admin EXEC	Add entries to the arp-spoofing table. Use no form to delete entries from the arp-spoofing table.	switch(config)# arp-spoofing src-mac 00:11:22:33:44:55 src-ip 192.168.1.20 switch(config)# no arp-spoofing src-mac 00:11:22:33:44:55 src-ip 192.168.1.20

DHCP Snooping

Dynamic Host Configuration Protocol (DHCP) dynamically assigns IP addresses to client devices. The use of dynamically assigned addresses requires traceability, so that a service provider can determine which clients own a particular IP address at a certain time.

With DHCP snooping, IP sources are dynamically verified, and filtered accordingly. IP packets that are not sourced from recognized IP addresses can be filtered out. This ensures the required traceability because the packets that are allowed into the network are using their officially allocated IP addresses.

Table 21. DHCP Snooping

Function	Privilege	Description	Example
show dhcp-snooping	User EXEC	Display DHCP snooping information.	switch# show dhcp-snooping
[no] dhcp-snooping	Admin EXEC	Enable or Disable DHCP snooping Protocol.	switch(config)# dhcp-snooping switch(config)# no dhcp-snooping
[no] dhcp-snooping binding mode interfaces IF_NMLPORTS	Admin EXEC	Add dhcp snooping binding mode interfaces. Use no form to remove dhcp snooping binding mode interfaces.	switch(config)# dhcp-snooping binding mode interface GigabitEthernet 1 switch(config)# no dhcp-snooping binding mode interface GigabitEthernet 1
[no] dhcp-snooping interfaces IF_NMLPORTS	Admin EXEC	Add dhcp snooping interfaces. Use no form to remove dhcp snooping interfaces.	switch(config)# dhcp-snooping interface GigabitEthernet 1 switch(config)# no dhcp-snooping interface GigabitEthernet 1

Hardware ACL

Hardware Access Control Lists (ACLs) are applied directly to interfaces, or are used for QoS classifications.

Table 22. Hardware ACL

Function	Privilege	Description	Example
`show macacl [entry-id WORD<1-7>]`	User EXEC	Display MAC ACL information.	switch# show macacl entry-id 4-5
`show ipacl [entry-id WORD<1-7>]`	User EXEC	Display IP ACL information.	switch# show ipacl entry-id 4-5
`macacl entry-id <1-250>`	Admin EXEC	Add entries to the mac acl table.	switch(config)# macacl entry-id 1
`no macacl entry-id WORD<1-7>`	Admin EXEC	Delete entries from the mac acl table.	switch(config)# no macacl entry-id 1-2

Table 22. Hardware ACL (Continued)

Function	Privilege	Description	Example
`ipacl entry-id <1-250>`	Admin EXEC	Add entries to the ip acl table.	switch(config)# ipacl entry-id 1
`no ipacl entry-id WORD<1-7>`	Admin EXEC	Delete entries from the ip acl table.	switch(config)# no ipacl entry-id 1-2
`dst-mac A:B:C:D:E:F mask A:B:C:D:E:F`	Admin EXEC	Set the rule "dst mac" to the entry.	switch(config-macacl)# dst-mac 00:11:22:33:44:55 mask FF:FF:FF:FF:FF:FF
`no dst-mac`	Admin EXEC	Clear the rule "dst mac" from the entry	switch(config-macacl)# no dst-mac
`src-mac A:B:C:D:E:F mask A:B:C:D:E:F`	Admin EXEC	Set the rule "src mac" to the entry.	switch(config-macacl)# src-mac 00:11:22:33:44:55 mask FF:FF:FF:FF:FF:FF
`no src-mac`	Admin EXEC	Clear the rule "src mac" from the entry	switch(config-macacl)# no src-mac
`ethertype <0-65535>`	Admin EXEC	Set the rule "ether type" to the entry.	switch(config-macacl)# ether-type 5555
`no ethertype`	Admin EXEC	Clear the rule "ether type" from the entry	switch(config-macacl)# no eth-ertype
`vlanid <1-4094>`	Admin EXEC	Set the rule "VLAN ID" to the entry.	switch(config-macacl)# vlanid 200
`no vlanid`	Admin EXEC	Clear the rule "VLAN ID" from the entry.	switch(config-macacl)# no vlanid
`dst-ip A.B.C.D mask A.B.C.D`	Admin EXEC	Set the rule "dst ip" to the entry.	switch(config-ipacl)# dst-ip 192.168.1.20 mask 255.255.255.255
`no dst-ip`	Admin EXEC	Clear the rule "dst ip" from the entry	switch(config-ipacl)# no dst-ip
`src-ip A.B.C.D mask A.B.C.D`	Admin EXEC	Set the rule "src ip" to the entry.	switch(config-ipacl)# src-ip 192.168.1.20 mask 255.255.255.255
`no src-ip`	Admin EXEC	Clear the rule "src ip" from the entry	switch(config-ipacl)# no src-ip
`no protocol`	Admin EXEC	Clear the rule "ip protocol" from the entry	switch(config-ipacl)# no protocol
`protocol icmp`	Admin EXEC	Set the rule "ip protocol icmp" to the entry.	switch(config-ipacl)# protocol icmp
`protocol tcp [dst-port <0-65535>] [srcport <0-65535>]`	Admin EXEC	Set the rule "tcp src port" and "tcp dst port" to the entry.	switch(config-ipacl)# protocol tcp switch(config-ipacl)# protocol tcp dstport 1000 srcport 2000
`protocol udp [dst-port <0-65535>] [srcport <0-65535>]`	Admin EXEC	Set the rule "udp src port" and "udp dst port" to the entry.	switch(config-ipacl)# protocol udp switch(config-ipacl)# protocol udp dstport 1000 srcport 2000

Table 22. Hardware ACL (Continued)

Function	Privilege	Description	Example
`action permit`	Admin EXEC	Set the antry action to "permit"	switch(config-ipacl)# action permit switch(config-macacl)# action permit
`action drop`	Admin EXEC	Set the antry action to "drop"	switch(config-ipacl)# action drop switch(config-macacl)# action drop
`action assign-queue <1-8>`	Admin EXEC	Set the antry action to redirect "ingress queue".	switch(config-ipacl)# assign-queue 6 switch(config-macacl)# assign-queue 6
`incoming-interface IF_NMLPORTS`	Admin EXEC	Set the rule "incoming interface" to the entry.	switch(config-ipacl)# incoming-interface GigabitEthernet 1 switch(config-macacl)# incoming-interface GigabitEthernet 1
`[no] active`	Admin EXEC	Active the ACL entry. Use no form to inactive the ACL entry.	switch(config-ipacl)# active switch(config-ipacl)# no active switch(config-macacl)# active switch(config-macacl)# no active

Security Login

Terminal Access Controller Access Control System (TACACS) and Remote Access Dial-In User Service (RADIUS) are security protocols that provide validation of users who are attempting to gain access to a router or NAS.

Table 23. Security Login

Function	Privilege	Description	Example
`show security-login`	User EXEC	Display Security Login information.	switch# show security-login
`[no] security-login`	Admin EXEC	Enable or Disable Security Login.	switch(config)# security-login switch(config)# no security-login
`[no] security-login access-contrl (all | http | ssh | telnet)`	Admin EXEC	Add the access control mode. Use no form to remove the access control mode.	switch(config)# security-login access-contrl all switch(config)# no security-login access-contrl all
`security-login login-type (all | both | radius | tacacs)`	Admin EXEC	Set the login type.	switch(config)# security-login login-type all
`no security-login login-type`	Admin EXEC	Clear the login type	switch(config)# no security-login login-type

Table 23. Security Login (Continued)

Function	Privilege	Description	Example
`security-login radius-config ip A.B.C.D port <1-65535> secret WORD<0-128>`	Admin EXEC	Set the radius server configuration.	switch(config)# security-login radius-config ip 192.168.1.20 port 80 secret 12345678
`security-login tacacs-config ip A.B.C.D port <1-65535> secret WORD<0-128>`	Admin EXEC	Set the tacacs server configuration.	switch(config)# security-login tacacs-config ip 192.168.1.20 port 80 secret 12345678

GMRP

Generic Attribute Registration Protocol (GARP) Multicast Registration Protocol (GMRP) allows network devices to register endstations with multicast groups and provides multicast filtering similar to IGMP snooping.

Table 24. GMRP

`show gmrp`	User EXEC	Display GMRP information.	switch# show gmrp
`[no] gmrp`	Admin EXEC	Enable or Disable GMRP Protocol.	switch(config)# gmrp switch(config)# no gmrp

Chapter 3
Security

The following feature commands are included in this chapter:

- ”Storm Control”
- “Port Security” on page 56
- “802.1X” on page 57
- “Remote Authentication” on page 58
- “Account Manager” on page 59
- “DoS Attack Prevention” on page 59
- “IP Security” on page 61

Storm Control

The Storm Control page allows you to setup the units and Preamble/IFG to manage the occurrence of packet flooding on the LAN and consequent traffic to prevent the degrading of network performance.

Table 25. Storm Control

Function	Privilege	Description	Example
show storm-control	User EXEC	Display storm-control information.	switch# show storm-control
show storm-control interfaces IF_NMLPORTS	User EXEC	Display storm-control information in specified interface.	switch# show storm-control interfaces fa5
storm-control ifg (include|exclude)	Admin EXEC	Decide whether to include/ exclude the preamble and inter frame gap into the calculation or not.	switch(config)# storm-control ifg include
storm-control unit (bps|pps)	Admin EXEC	Set the unit of calculation method.	switch(config)# storm-control unit bps
[no] storm-control	Admin EXEC	Disable or enable storm-control.	switch(config)# storm-control
[no] storm-control (broadcast|unknown-unicast|unknown-multicast)	Admin EXEC	Disable or enable storm-control type.	switch(config-if)# storm-control broadcast

Table 25. Storm Control (Continued)

Function	Privilege	Description	Example
`storm-control (broadcast|unknown-unicast|unknown-multicast) level <1-1000000>`	Admin EXEC	Set control rate of storm-control type.	switch(config-if)# storm-control broadcast level 1000
`no storm-control (broadcast|unknown-unicast|unknown-multicast) level`	Admin EXEC	No control rate of storm-control type.	switch(config-if)# no storm-control broadcast level
`storm-control action (drop|shutdown)`	Admin EXEC	The storm control mechanism drops packets which exceed storm control rate or just shuts down the port.	switch(config-if)# storm-control action shutdown
`no storm-control action`	Admin EXEC	Set action to drop.	switch(config-if)# no storm-control action

Port Security

This feature lets you control access to all or specific ports on the switch based on the source MAC addresses of the network devices. You specify the maximum number of source MAC addresses that ports can learn. Ports that learn their maximum number of addresses discard packets that have new, unknown addresses, preventing access to the switch by any further devices.

Table 26. Port Security

Function	Privilege	Description	Example
`show port-security`	User EXEC	Display port-security status.	switch# show port-security
`[no] port-security [learning-limit <0-64>]`	Admin EXEC	Enable port security of a port and specify a maximum FDB learning number of that port. Disable port security.	switch(config-if)# port-security learning-limit 5 switch(config-if)# port-security switch(config-if)# no port-security
`[no] mac-violation-notify`	Admin EXEC	When a port reaches its maximum FDB learning number, the system will send to SNMP trap for a new MAC.	switch(config-if)# mac-violation-notify switch(config-if)# no mac-violation-notify

802.1X

The 802.1x function provides port-based authentication to prevent unauthorized devices (clients) from gaining access to the network.

Table 27. 802.1X

Function	Privilege	Description	Example
`show dot1x status`	User EXEC	Show Dot1x configuration.	switch# show dot1x
`[no] dot1x`	Admin EXEC	Configure radius server enable/disable. The "dot1x" command globally enables 802.1x ability. The "no dot1x run" command disables the 802.1x ability.	switch#show dot1x switch(config)# no dot1x
`dot1x authentication-based (port | mac)`	Admin EXEC	Configure radius server authentication mode.	switch(config)# dot1x authentication-based port switch(config)# dot1x authentication-based mac
`dot1x authentication-port IF_PORTS sectype (authorize | disable)`	Admin EXEC	Configure radius server authentication port.	switch(config)# dot1x authentication-port FastEthernet 1 sectype authorize switch(config)# dot1x authentication-port FastEthernet 1 sectype disable
`dot1x sys-configuration ip X.X.X.X radius-port <1-65535> accounting-port <1-65535> secret WORD<0-128>`	Admin EXEC	Configure radius server IP & port and secret key.	switch(config)# dot1x sys-configuration ip 192.168.1.100 radius-port 1812 accounting-port 1813 secret 12345678
`dot1x misc-configuration reauth-period <1-65535>`	Admin EXEC	Configure radius server reauth period.	switch(config)# dot1x misc-configuration reauth-period 3600

Remote Authentication

Remote Authentication is used to authenticate a reply from the server, and is used in encrypting passwords; its length is 16 bytes.

Table 28. Remote Authentication

Function	Privilege	Description	Example
`show security-login`	User EXEC	Show security login configuration.	switch# show security-login
`[no] security-login`	Admin EXEC	Use "security-login" command to enable security-login services. Use no form to disable service.	switch(config)# security-login switch(config)# no security-login
`security-login radius-config ip X.X.X.X port <1-65535> secret WORD<0-128>`	Admin EXEC	Configure radius login access control.	switch(config)# security-login radius-config ip 192.168.1.100 port 1812 secret 12345678
`security-login tacacs-config ip X.X.X.X port <1-65535> secret WORD<0-128>`	Admin EXEC	Configure security login access control.	switch(config)# security-login rtacacs-config ip 192.168.1.100 port 1812 secret 12345678
`security-login access-contrl (http | telnet | ssh | all)`	Admin EXEC	Configure security login access control.	switch(config)# security-login access-contrl http
`no security-login access-contrl (http | telnet | ssh | all)`	Admin EXEC	Reset security login access control.	switch(config)# no security-login access-contrl
`login-type (radius | tacacs | both | all)`	Admin EXEC	Configure security login type.	switch(config)# security-login login-type radius
`no security-login login-type`	Admin EXEC	Reset security login type.	switch(config)# no security-login login-type

Account Manager

The account manager commands are used to change the default password and create additional passwords for access to the management software.

Table 29. Account Manager

Function	Privilege	Description	Example
`show username`	User EXEC	Show all user accounts in local database.	switch# show username
`show privilege`	User EXEC	Show current privilege level.	switch# show privilege
`username WORD<0-32> [privilege (admin|user)] (password WORD<0-32>) | (secret [encrypted] WORD<0-32>) | nopassword`	Admin EXEC	Use "username" command to add a new user account or edit an existing user account.	switch(config)# username test privilege admin secret 1234
`no username WORD<0-32>`	Admin EXEC	Delete an existing user account.	switch(config)# no username test
`enable (password | (secret [encrypted])) PASSWORD`	Admin EXEC	Edit password for each privilege level to enable authentication.	switch(config)# enable secret 1234
`no enable`	Admin EXEC	Restore enable password to default empty value.	switch(config)# no enable

DoS Attack Prevention

The Denial of Service (DoS) commands allow you to enable and disable the DoS Attack Prevention feature.

Table 30. DoS Attack Prevention

Function	Privilege	Description	Example
`show dos`	User EXEC	Show current dos global state.	switch# show dos

Table 30. DoS Attack Prevention (Continued)

Function	Privilege	Description	Example

`[no] dos VALUE`
`tcphdr-min-length 10`
`smurf-netmask <0-32>`
`icmp-ping-max-length 1024`
`ipv6-min-frag-size-length <0-65535>`
	User EXEC	After select "Configure DUT to enable/disable support types of attacks tcphdr-min-check | smurf-deny | icmpv6-ping-max-check | icmpv4-ping-max-check | ipv6-min-frag-size-check", Size/Length need to be set.	switch(config)# dos
			daeqsa-deny Destination MAC equals to source MAC
			icmp-frag-pkts-deny Fragmented ICMP packets
			icmp-ping-max-length DoS information
			icmpv4-ping-max-check Check ICMPv4 ping maximum packets size
			icmpv6-ping-max-check Check ICMPv6 ping maximum packets size
			ipv6-min-frag-size-check Check minimum size of IPv6 fragments
			ipv6-min-frag-size-length DoS information
			land-deny Source IP equals to destination IP
			nullscan-deny NULL Scan Attacks
			pod-deny Ping of Death Attacks
			smurf-deny Smurf Attacks
			smurf-netmask DoS information
			syn-sportl1024-deny SYN packets with sport less than 1024
			synfin-deny SYN and FIN bits set in the packet
			synrst-deny SYNC and RST bits set in the packet
			tcp-frag-off-min-check TCP fragment packet with offset equals to one
			tcpblat-deny Source TCP port equals to destination TCP port
			tcphdr-min-check Check minimum TCP header
			tcphdr-min-length DoS information
			udpblat-deny Source UDP port equals to destination UDP port
			xma-deny Xmascan: sequence number is zero and the FIN, URG and PSH bits are set

`show dos interfaces IF_PORTS`	User EXEC	Show dos configuration on selected ports.	switch# show dos interfaces GigabitEthernet 1

Table 30. DoS Attack Prevention (Continued)

Function	Privilege	Description	Example
`[no] dos (tcp-frag-off-min-check|synrst-deny|synfin-deny|xma-deny|nullscan-deny|syn-sportl1024-deny|tcphdr-min-check|smurf-deny|icmpv6-ping-max-check|icmpv4-ping-max-check|icmp-frag-pkts-deny|ipv6-min-frag-size-check|pod-deny|tcpblat-deny|udpblat-deny|land-deny|daeqsa-deny)`	Admin EXEC	Configure DUT to enable/ disable support types of attacks.	switch(config)# no dos land-deny switch(config)# dos land-deny

IP Security

The IP Security commands allow you to enable and disable the IP Security feature.

Table 31. IP Security

Function	Privilege	Description	Example
`show ip-security`	User EXEC	Display IP security information.	switch# show ip-security
`[no] ip-security`	Admin EXEC	Disable or enable IP security.	switch(config)# ip-security
`ip-security ip A.B.C.D mask A.B.C.D [service (ping | http | https | telnet | ssh | snmp) state (enable | disable)]`	Admin EXEC	Add a specified IP (and service) entry for IP security usage.	switch(config)# ip-security ip 192.168.1.1 mask 255.255.0.0 service ping state enable
`no ip-security ip A.B.C.D mask A.B.C.D`	Admin EXEC	Remove specified IP security entry.	switch(config)# no ip-security ip 192.168.1.1 mask 255.255.0.0

Chapter 4

Quality of Service

The Quality of Service function allows the switch to implement congestion-management and congestion-avoidance of the Ethernet traffic based on the prioritization values in Layer 2 frames. Implementing QoS in the network makes performance predictable and bandwidth utilization much more effective.

The following feature commands are included in this chapter:

- ”QoS”
- “Rate Limit” on page 66

QoS

The switch supports eight CoS queues for each egress port. For each of the eight queues, two types of scheduling can be configured: Strict Priority and non-Strict Priority (Weighted Round Robin). Mapping for CoS, DSCP and IP precedence is available on a port by port basis.

Table 32. QoS

Function	Privilege	Description	Example
`show qos`	User EXEC	Display QoS state.	switch# show qos
`show qos queueing`	User EXEC	Display QoS queueing state.	switch# show qos queueing
`show qos interfaces IF_PORTS`	User EXEC	Display QoS state by interface.	switch# show qos interface gi1
`show qos map [(cos-queue|dscp-queue|precedence-queue|queue-cos|queue-dscp|queue-precedence)]`	User EXEC	Display QoS map detail.	switch# show qos map
`[no] qos`	Admin EXEC	Enabled or disabled the device to QoS mode.	switch# configure switch(config)# qos switch(config)# exit

Table 32. QoS (Continued)

Function	Privilege	Description	Example
`qos queue strict-priority-num <0-8>`	Admin EXEC	Specify the strict priority queue number.	switch# configure switch(config)# qos queue strict-priority-num 1 switch(config)# exit
`qos queue weight SEQUENCE`	Admin EXEC	Specify the non-strict priority queue weight value. The valid queue weight value is from 1 to 127.	switch# configure switch(config)# qos queue weight 3 switch(config)# exit
`qos map cos-queue SEQUENCE to <1-8>`	Admin EXEC	Configure or show CoS to queue map	switch# configure switch(config)# qos map cos-queue 6 7 to 1 switch(config)# exit
`qos map dscp-queue SEQUENCE to <1-8>`	Admin EXEC	Configure or show DSCP to queue map.	switch# configure switch(config)# qos map dscp-queue 6 7 to 1 switch(config)# exit
`qos map precedence-queue SEQUENCE to <1-8>`	Admin EXEC	Configure or show IP Precedence to queue map.	switch# configure switch(config)# qos map precedence-queue 6 7 to 1 switch(config)# exit
`qos trust (cos|cos-dscp|dscp|precedence)`	Admin EXEC	Specify the device to trust CoS. Specify the device to trust DSCP for IP packets, and trust CoS for non-IP packets. Specify the device to trust DSCP. Specify the device to trust IP Precedence	switch# configure switch(config)# qos trust cos switch(config)# qos trust dscp switch(config)# exit
`no qos trust`	Admin EXEC	Clear qos trust configure.	switch# configure switch(config)# no qos trust switch(config)# exit
`qos cos <0-7>`	Admin EXEC	Specify the CoS value for the interface.	switch# configure switch(config)# interface gi1 switch(config-if)# qos cos 1 switch(config-if)# exit switch(config)# exit

Table 32. QoS (Continued)

Function	Privilege	Description	Example
`[no] qos trust`	Admin EXEC	Enabled or disabled the QoS mode per port.	switch# configure switch(config)# interface gi1 switch(config-if)# qos switch(config-if)# exit switch(config)# exit
`qos map queue-cos SEQUENCE to <0-7>`	Admin EXEC	Configure or show CoS to queue map.	switch# configure switch(config)# interface gi1 switch(config-if)# qos map cos-queue 6 7 to 1 switch(config-if)# exit switch(config)# exit
`qos map queue-dscp SEQUENCE to <0-63>`	Admin EXEC	Configure or show DSCP to queue map.	switch# configure switch(config)# interface gi1 switch(config-if)# qos map dscp-queue 6 7 to 1 switch(config-if)# exit switch(config)# exit
`qos map queue-precedence SEQUENCE to <0-7>`	Admin EXEC	Configure or show IP Precedence to queue map.	switch# configure switch(config)# interface gi1 switch(config-if)# qos map precedence-queue 6 7 to 1 switch(config-if)# exit switch(config)# exit
`[no] qos remark (cos|dscp|precedence)`	Admin EXEC		

Rate Limit

Rate Limit features traffic bandwidth control on a per port basis. Bandwidth control is supported for t

- ❐ Ingress Bandwidth Control
- ❐ Egress Bandwidth Control
- ❐ Egress Queue.

Table 33. Rate Limit

Function	Privilege	Description	Example
`show rate-limit`	User EXEC	Display rate-limit information.	switch# show rate-limit
`show rate-limit interfaces IF_NMLPORTS`	User EXEC	Display rate-limit information in specified interface.	switch# show rate-limit interfaces fa 5
`rate-limit ingress <16-1000000>`	Admin EXEC	Set ingress rate-limit.	switch(config-if)# rate-limit ingress 10000
`no rate-limit ingress`	Admin EXEC	No ingress rate-limit.	switch(config-if)# no rate-limit ingress
`rate-limit egress <16-1000000>`	Admin EXEC	Set egress rate-limit.	switch(config-if)# rate-limit egress 10000
`no rate-limit egress`	Admin EXEC	No egress rate-limit.	switch(config-if)# no rate-limit egress
`rate-limit egress queue <1-8> <16-1000000>`	Admin EXEC	Set egress rate-limit in queue.	switch(config-if)# rate-limit egress queue 3 10000
`no rate-limit egress queue <1-8>`	Admin EXEC	No egress rate-limit in queue.	switch(config-if)# no rate-limit egress queue 3

Chapter 5

Management

The following feature commands are included in this chapter:

IP Management

The IP Settings menu allows you to show or modify a static or DHCP network addresses.

Table 34. IP Management

Function	Privilege	Description	Example
`show ip`	User EXEC	Show system IPv4 address, net mask and default gateway.	switch# show ip
`show ip dhcp`	User EXEC	Show IPv4 DHCP client enable state.	switch# show ip dhcp
`show auto-ip`	User EXEC		

Table 34. IP Management (Continued)

Function	Privilege	Description	Example
`[no] ip dhcp`	Admin EXEC	Use "IP DHCP" command to enable DHCP client to get IP address from remote DHCP server. Use "No IP DHCP" command to disable DHCP client and use static IP address.	switch(config)# ip dhcp switch(config)# no ip dhcp
`ip address A.B.C.D [mask A.B.C.D]`	Admin EXEC	Modify administration IPv4 address.	switch(config)# ip address 192.168.1.200 mask 255.255.255.0
`default-gateway A.B.C.D`	Admin EXEC	Modify default gateway address.	switch(config)# ip default-gateway 192.168.1.100
`no ip default-gateway`	Admin EXEC	use “no ip default-gateway” to restore default gateway address to factory default.	switch(config)# no ip default-gateway
`show ipv6 dhcp`	User EXEC	Show system IPv6 DHCP client enable state.	switch# show ipv6 dhcp
`show ipv6`	User EXEC	Show system IPv6 address, net mask, default gateway and auto config state.	switch# show ipv6
`[no] ipv6 dhcp`	Admin EXEC	Use "IPv6 DHCP" command enable DHCPv6 client to get IP address from remote DHCPv6 server. Use "No IPv6 DHCP" command to disable DHCPv6 client and use static IPv6 address or IPv6 auto config address.	switch(config)# ipv6 dhcp
`[no] ipv6 autoconfig`	Admin EXEC	Use "IPv6 autoconfig" command to enable IPv6 auto configuration feature. Use "No IPv6 autoconfig" command to disable IPv6 auto configuration feature.	switch(config)# no ipv6 autoconfig
`ipv6 address X:X::X:X prefix <0-128>`	Admin EXEC	Use "IPv6 address" command to specify static IPv6 address.	switch(config)# ipv6 address fe80::20e:2eff:fef1:4b3c prefix 128
`ipv6 default-gateway X:X::X:X`	Admin EXEC	Use "IPv6 default-gateway" command to modify default gateway IPv6 address.	switch(config)# ipv6 default-gateway fe80::dcad:beff:feef:103

LLDP

LLDP is a one-way protocol without request/response sequences. Information is advertised by stations implementing the transmit function, and is received and processed by stations implementing the receive function.

Table 35. LLDP

Function	Privilege	Description	Example
`show lldp`	User EXEC	Display LLDP information.	switch# show lldp
`show lldp interfaces IF_NMLPORTS`	User EXEC	Display LLDP information in specified ports.	switch# show lldp interfaces fa5
`show lldp local-device`	User EXEC	Display the local configuration.	switch# show lldp local-device
`show lldp interfaces IF_NMLPORTS local-device`	User EXEC	Display the local configuration in specified ports.	switch# show lldp interfaces fa5,fa6 local-device
`show lldp neighbor`	User EXEC	Display the neighbor's LLDP information.	switch# show lldp neighbor
`show lldp interfaces IF_NMLPORTS neighbor`	User EXEC	Display the neighbor's LLDP information in specified ports.	switch# show lldp interfaces fa5,fa6 neighbor
`show lldp statistics`	User EXEC	Display the LLDP RX/TX statistics.	switch# show lldp statistics
`show lldp interfaces IF_NMLPORTS statistics`	User EXEC	Display the LLDP RX/TX statistics in specified ports.	switch# show lldp interfaces fa5,fa6 statistics
`show lldp interfaces IF_NMLPORTS tlvs-overloading`	User EXEC	Display the length of LLDP TLVs and if the TLVs overload the PDU length in specified ports.	switch# show lldp interfaces fa5,fa6 tlvs-overloading
`clear lldp statistics`	Admin EXEC	Clear statistics of LLDP.	switch# clear lldp statistics
`[no] lldp`	Admin EXEC	Disable or enable LLDP.	switch(config)# lldp
`[no] lldp tx`	Admin EXEC	Per port disable or enable LLDP TX.	switch(config-if)# lldp rx
`[no] lldp rx`	Admin EXEC	Per port disable or enable LLDP RX.	switch(config-if)# lldp tx

Table 35. LLDP (Continued)

Function	Privilege	Description	Example
`lldp holdtime-multiplier <2-10>`	Admin EXEC	Set the LLDP PDU hold multiplier that decides time-to-live (TTL) value sent in LLDP advertisements: TTL = (tx-interval * holdtime-multiplier).	switch(config)# lldp holdtime-multiplier 4
`no lldp holdtime-multiplier`	Admin EXEC		switch(config)# no lldp holdtime-multiplier
`lldp tx-interval <5-32767>`	Admin EXEC	Set the LLDP TX interval.	switch(config)# lldp tx-interval 30
`no lldp tx-interval`	Admin EXEC		switch(config)# no lldp tx-interval
`lldp reinit-delay <1-10>`	Admin EXEC	Set the LLDP re-initial delay. This delay avoids LLDP generating too many PDUs if the port is up and down frequently.	switch(config)# lldp reinit-delay 2
`no lldp reinit-delay`	Admin EXEC		switch(config)# no lldp reinit-delay
`lldp tx-delay <1-8191>`	Admin EXEC	Set the delay in seconds between successive LLDP frame transmissions. The delay starts to count any time that LLDP PDU is sent, such as by LLDP PDU advertise routine, LLDP PDU content change, port link up, etc.	switch(config)# lldp tx-delay 2
`no lldp tx-delay`	Admin EXEC		switch(config)# no lldp tx-delay
`lldp tlv-select pvid (enable|disable)`	Admin EXEC	This command per port configures the 802.1 PVID TLV attach enable status.	switch(config-if)# lldp tlv-select pvid enable
`no lldp tlv-select pvid`	Admin EXEC		switch(config-if)# no lldp tlv-select pvid

Table 35. LLDP (Continued)

Function	Privilege	Description	Example
`lldp tlv-select vlan-name (add|remove) VLAN-LIST`	Admin EXEC	The commands per port add or remove VLAN list for 802.1 VLAN-NAME TLV.	switch(config-if)# lldp tlv-select vlan-name add 1,2,3,4
`lldp tlv-select TLV [TLV] [TLV] [TLV] [TLV] [TLV] [TLV] [TLV]`	Admin EXEC	This command per port configures the selected TLV attaching in PDU.	switch(config-if)# lldp tlv-select port-desc sys-name sys-desc sys-cap mac-phy lag max-frame-size management-addr
`no lldp tlv-select`	Admin EXEC		switch(config-if)# no lldp tlv-select
`lldp lldpdu (filtering|bridging|flooding)`	Admin EXEC	This command globally configures the LLDP PDU handling behavior when LLDP is globally disabled. It should be noted that if LLDP is globally enabled and per port LLDP RX status is configured to disable, the received LLDP PDU is dropped instead of taking the global disable behavior.	switch(config)# lldp lldpdu filtering
`no lldp lldpdu`	Admin EXEC		switch(config)# no lldp lldpdu

SNMP

Simple Network Management Protocol (SNMP) is a protocol to facilitate the monitoring and exchange of management information between network devices. Through SNMP, the health of the network or status of a particular device can be determined.

Table 36. SNMP

Function	Privilege	Description	Example
`show snmp`	User EXEC	Display SNMP state.	switch# show snmp
`show snmpv3`	User EXEC	Display SNMPv3 configure state.	switch# show snmpv3
`show snmp trap`	User EXEC	Display SNMP trap setting.	switch# show snmp trap

Table 36. SNMP (Continued)

Function	Privilege	Description	Example
`[no] snmp`	Admin EXEC	Enable or disabled SNMP engine.	switch# configure switch(config)# snmp switch(config)# exit
`[no] snmp trap (auth|linkUp-Down|warm-start|cold-start|port-security)`	Admin EXEC	Specify SNMP trap setting.	switch# configure switch(config)# snmp trap auth switch(config)# exit
`snmp community NAME (ro|rw)`	Admin EXEC	SNMP v1/v2 community name. SNMP community read or readwrite attribute for basic mode.	switch# configure switch(config)# snmp community user rw switch(config)# exit
`no snmp community NAME`	Admin EXEC	Delete SNMP community name.	switch# configure switch(config)# no snmp community user switch(config)# exit
`snmp host (A.B.C.D|X:X::X:X|HOSTNAME) [version (1|2c)] NAME`	Admin EXEC	SNMP trap host IPv4/IPv6 address or host name. v1/v2c/v3 traps. SNMP community name or user name.	switch# configure switch(config)# snmp host 192.168.1.100 version 2c private switch(config)# exit
`no snmp host (A.B.C.D|X:X::X:X|HOSTNAME) [version (1|2c)]`	Admin EXEC	Delete SNMP host.	switch# configure switch(config)# no snmp host 192.168.1.100 version 2c switch(config)# exit
`snmpv3 user NAME (ro|rw) auth (md5|sha) password WORD<8-32> priv password WORD<8-32>`	Admin EXEC	SNMPv3 user name. SNMPv3 user read or readwrite attribute for basic mode. SNMPv3 user security level, auth-protocol, prvi-protocol.	switch# configure switch(config)# snmpv3 user root rw auth md5 password 12345678 switch(config)# exit
`no snmpv3 user NAME`	Admin EXEC	Delete SNMPv3 user name.	switch# configure switch(config)# no snmp user root switch(config)# exit

Power Over Ethernet

Power Over Ethernet is the function supplying power to Powered Devices (PD) through the switch in the event that AC power is not readily available.

Table 37. Power Over Ethernet

Function	Privilege	Description	Example
`show poe (system|port)`	User EXEC	Use "show PoE (system|port)" command to show current PoE setting value and status.	This example shows current PoE status per port. switch# show poe port
`poe`	Admin EXEC	Use PoE command to enter PoE's control level.	This example shows how to enter PoE control level. switch# configure switch(config)# poe switch(config-poe)#
`system powerlimit <0-800>`	Admin EXEC	Use "system powerlimit" command to configure how much power can be used in entire system.	This example shows how to configure whole system available power to 720W. switch(config-poe)# system power-limit 120
`system ac-disconnect (enable|disable)`	Admin EXEC	Use ac-disconnect command to determine which disconnect type will be selected.	This example shows how to configure disconnect type to DC typeswitch(config-poe)#. system ac-disconnect disable
`system overload-disconnect (port-priority|overload-port-first)`	Admin EXEC	Use system overload-disconnect command to determine which PoE port will supply power when the total power is at full load. There are two algorithms supported, and this command allows selection of the algorithm.	This example shows how to select overload-port-first to be the overload-disconnect's algorithm. switch(config-poe)# system overload-disconnect overload-port-first
`interfaces IF_NMLPORT legacy-mode (enable|disable)`	Admin EXEC	Use "legacy-mode (enable|disable)" command to configure supply power mechanism to legacy mode in PoE port.	This example shows how to configure fa1's PoE power to legacy mode. switch(config-poe)# interfaces FastEthernet 1 legacy-mode enable
`interfaces IF_NMLPORT state (enable|disable)`	Admin EXEC	Use "state (enable|disable)" command to configure whether PoE port will supply power or not.	This example shows how to stop PoE port supply power via fa1. switch(config-poe)# interfaces FastEthernet 1 state disable

Table 37. Power Over Ethernet

Function	Privilege	Description	Example
`interfaces IF_NMLPORT plfc (enable|disable)`	Admin EXEC	Use "plfc (enable|disable)" command to configure how much power PoE port will supply based on PD's class level.	This example shows how to configure fa1's PoE supply power mode to plfc(power-limit from class). switch(config-poe)# interfaces FastEthernet 1 plfc enable
`interfaces IF_NMLPORT priority (low|medium|high|critical)`	Admin EXEC	Use "priority (low|medium|high|critical)" command to configure PoE port's priority of power supply sequence.	This example shows how to configure fa1 as the most high priority level in power supply sequence. switch(config-poe)# interfaces FastEthernet 1 priority critical
`interfaces IF_NMLPORT power-limit <0-30000>`	Admin EXEC	Use "power-limit <0-30000>" command to configure how much power can be used via PoE port.	This example shows how to configure fa1's power of PoE to 15W. switch(config-poe)# interfaces FastEthernet 1 power-limit 15000

Configuration Management

The commands in Table 38 manage the startup and configuration files.

Table 38. Configuration Management

Function	Privilege	Description	Example
`show (startup-config|running-config)`	Admin EXEC	Show startup/running configuration.	switch# show startup-config switch# show running-config
`show running-config interfaces IF_PORTS`	Admin EXEC	Show running configuration on selected ports.	switch# show running-config interfaces GigabitEthernet 1
`copy running-config (startup-config|)`	Admin EXEC	Copy running configuration to startup configuration.	switch# copy running-config startupst-config
`copy (running-config|startup-config) tftp://`	Admin EXEC	Copy running/startup configuration to remote tftp server.	switch# copy running-config startupst-config tftp://192.168.1.111/test1.cfg
`copy tftp:// (running-config|startup-config)`	Admin EXEC	Upgrade running/startup configuration from remote tftp server.	switch# copy tftp://192.168.1.111/test2.cfg startup-config
`copy (startup-config) running-config`	Admin EXEC	Copy startup configuration to running configuration.	switch# copy startupst-config running-config

Table 38. Configuration Management (Continued)

Function	Privilege	Description	Example
`delete (startup-config|flash://)`	Admin EXEC	Restore factory defaults, equal to command "restore-defaults".	switch# delete backup-config
`reset`	Admin EXEC	Restore system to all factory defaults.	switch# reset
`reset except for [ip-address] [vlan] [user-account]`	Admin EXEC	Restore system to all factory defaults except for specified settings.	switch# reset except for ip-address
`save`	Admin EXEC		

Firmware Management

The commands in Table 39 manage and upgrade the firmware image files.

Table 39. Firmware Management

Function	Privilege	Description	Example
`boot system (image0|image1)`	Admin EXEC	Dual image stores a backup image in the flash partition. Use "boot system" command to select the active firmware image. The other firmware image will become a backup.	switch(config)# boot system image1
`delete system (image0|image1)`	Admin EXEC	Delete firmware image stored in flash.	switch# delete system image1
`copy (flash:// |tftp://) (flash:/ /|tftp://)`	Admin EXEC	Upgrade/backup firmware image from/to remote tftp server.	switch# copy tftp:// 192.168.1.100/vmlinux.bix flash://image0

DHCP Server

The Dynamic Host Configuration Protocol (DHCP) is a network protocol enabling a server to automatically assign an IP address to a computer from a defined range of numbers configured for a given network.

Table 40. DHCP Server

Function	Privilege	Description	Example
`show dhcp-server [lease]`	User EXEC	Show DHCP server information. Show leased client information.	switch# show dhcp-server switch# show dhcp-server lease
`[no] dhcp-server`	Admin EXEC	Enable or disable DHCP server.	switch(config)# dhcp-server
`dhcp-server lease-time <60-86400>`	Admin EXEC	Set the lease-time of DHCP server.	switch(config)# dhcp-server lease-time 16888
`dhcp-server global low-ip-address A.B.C.D high-ip-address A.B.C.D subnet-mask A.B.C.D gateway A.B.C.D dns A.B.C.D`	Admin EXEC	Set allocate IP range, subnet mask, gateway, DNS in global settings of DHCP server.	switch(config)# dhcp-server global low-ip-address 10.1.1.1 high-ip-address 10.1.2.1 subnet-mask 255.255.0.0 gateway 10.1.1.254 dns 10.1.1.100
`no dhcp-server global`	Admin EXEC	Remove global settings of DHCP server	switch(config)# no dhcp-server global
`dhcp-server interface IF_NMLPORT low-ip-address A.B.C.D high-ip-address A.B.C.D subnet-mask A.B.C.D gateway A.B.C.D dns A.B.C.D`	Admin EXEC	Set allocate IP range, subnet mask, gateway, DNS in specified port settings of DHCP server.	switch(config)# dhcp-server interface GigabitEthernet1 low-ip-address 11.1.1.1 high-ip-address 11.1.2.1 subnet-mask 255.255.0.0 gateway 11.1.1.254 dns 11.1.1.100
`no dhcp-server interfaces IF_NMLPORT`	Admin EXEC	Remove specific port settings of DHCP server.	switch(config)# no dhcp-server interfaces GigabitEthernet1
`dhcp-server vlan entry <1-8> vlan <1-4094> low-ip-address A.B.C.D high-ip-address A.B.C.D subnet-mask A.B.C.D gateway A.B.C.D dns A.B.C.D`	Admin EXEC	Set allocate IP range, subnet mask, gateway, DNS in specified VLAN settings of DHCP server.	switch(config)# dhcp-server vlan entry 2 vlan 12 low-ip-address 12.1.1.1 high-ip-address 12.1.2.1 subnet-mask 255.255.0.0 gateway 12.1.1.254 dns 12.1.1.100
`no dhcp-server vlan entry <1-8>`	Admin EXEC	Remove specific VLAN settings of DHCP server.	switch(config)# no dhcp-server vlan entry 2

Table 40. DHCP Server (Continued)

Function	Privilege	Description	Example
`dhcp-server option82 entry <1-2> low-ip-address A.B.C.D high-ip-address A.B.C.D subnet-mask A.B.C.D gateway A.B.C.D dns A.B.C.D`	Admin EXEC	Set allocate IP range, subnet mask, gateway, DNS in specified option 82 settings of DHCP server.	switch(config)# dhcp-server option82 entry 1 low-ip-address 13.1.1.1 high-ip-address 13.1.2.1 subnet-mask 255.255.0.0 gateway 13.1.1.254 dns 13.1.1.100
`dhcp-server option82 entry <1-2> circuit-id format (string | hex) content WORD<0-120>`	Admin EXEC	Set circuit ID in specified option 82 settings of DHCP server.	switch(config)# dhcp-server option82 entry 1 circuit-id format string content Hello
`dhcp-server option82 entry <1-2> remote-id format (string | hex) content WORD<0-120>`	Admin EXEC	Set remote ID in specified option 82 settings of DHCP server.	switch(config)# dhcp-server option82 entry 1 remote-id format string content World
`no dhcp-server option82 entry <1-2>`	Admin EXEC	Remove specific option 82 settings of DHCP server.	switch(config)# no dhcp-server option82 entry 1

DHCP Client Option 82

The DHCP Client Option 82 configurable Circuit ID and Remote ID feature enhances validation security by allowing you to select naming choices suboptions. You can select a switch-configured hostname or specify an ASCII test string for the remote ID. You can also configure an ASCII text string to override the circuit ID.

Table 41. DHCP Client

Function	Privilege	Description	Example
`show dhcp-auto-provision`	User EXEC	View DHCP-auto-provision status.	switch# show dhcp-auto-provision
`[no] dhcp-auto-provision`	Admin EXEC	Enable of disable DHCP-auto-provision.	switch(config)# dhcp-auto-provision
`[no] ip dhcp option82`	Admin EXEC	Enable or disable DHCP option 82 for DHCP client.	switch(config)# ip dhcp option82

Table 41. DHCP Client (Continued)

Function	Privilege	Description	Example
`ip dhcp option82 circuit-id format (string | hex | user-define) [content WORD<0-120>]`	Admin EXEC	Set circuit-id in DHCP option 82 for DHCP client.	switch(config)# ip dhcp option82 circuit-id format string Hello
`ip dhcp option82 remote-id format (string | hex | user-define) [content WORD<0-120>]`	Admin EXEC	Set remote-id in DHCP option 82 for DHCP client.	switch(config)# ip dhcp option82 remote-id format string World

System Log (SYSLOG)

The Logging Service page allows you to setup the logging services feature for the system log.

Table 42. System Log (SYSLOG)

Function	Privilege	Description	Example
`show logging`	User EXEC	Display the global logging status.	switch# show logging
`show logging (buffered|file)`	User EXEC	Display log of buffer or file.	switch# show logging buffered
`clear logging (buffered|file)`	Admin EXEC	Clear logging information.	switch# clear logging buffered
`[no] logging`	Admin EXEC	Disable or enable logging service.	switch(config)# logging
`logging host (A.B.C.D|HOSTNAME) [port <0-65535>] [severity <0-7>] [facility (local0|local1|local2|local3|local4|local5|local6|local7)]`	Admin EXEC	Set remote log server information and specify the minimum severity mask and facility of logging message.	switch(config)# logging host 192.168.1.100 severity 6 facility local0
`logging (buffered|console|file) [severity <0-7>]`	Admin EXEC	Enable logging into buffer or console of file and specify the minimum severity mask of logging message.	switch(config)# logging buffered severity 6
`no logging (buffered|console|file)`	Admin EXEC	Disable logging into buffer or console or file.	switch(config)# no logging buffered
`no logging host (A.B.C.D|HOSTNAME)`	Admin EXEC	Remove remote log server.	switch(config)# no logging host 192.168.1.100

SNTP - Network Time Protocol

SNTP (Simple Network Time Protocol) synchronizes the system time of a client with a Time Server on the network. The commands in Table 43 are used to configure the SNTP client on the switch.

Table 43. SNTP - Simple Network Time Protocol

Function	Privilege	Description	Example
`show clock [detail]`	User EXEC	Display the details of clock status.	switch# show clock detail 15:46:14 PDT(GMT-7) May 30 2018 No time source Time zone: Acronym is PDT Offset is GMT-7
`clock source (local|sntp)`	Admin EXEC	Set the source of time. Use the no form of this command to select the default setting.	switch(config)# clock source sntp switch(config)# show clock detail 08:32:12 test(UTC+5) Sep 21 2012 No time source Time zone: Acronym is DFL Offset is UTC+8
`clock timezone ACRONYM HOUR-OFF-SET [minutes <0-59>]`	Admin EXEC	Use the clock timezone command to set timezone setting.	switch(config)# clock timezone test +5 switch(config)# show clock detail 10:13:27 test(UTC+5) Sep 21 2012 No time source Time zone: Acronym is test Offset is UTC+5
`no clock timezone`	Admin EXEC	Use the no form of this command to timezone default setting.	switch(config)# no clock timezone
`sntp host HOSTNAME [port <1-65535>]`	Admin EXEC	Use the clock set command to set static time. The static time won't save to configuration file.	switch# clock set 11:03:00 sep 21 2012 11:03:00 DFL(UTC+8) Sep 21 2012
`no sntp`	Admin EXEC	Use the no form of this command to restore sntp default setting.	switch(config)# no sntp
`clock set HH:MM:SS (jan|feb|mar|apr|may|jun|jul|aug|sep|oct|nov|dec) <1-31> <2000-2035>`	Admin EXEC	Use the clock set command to set static time. The static time won't save to configuration file.	switch# clock set 11:03:00 sep 21 2012 11:03:00 DFL(UTC+8) Sep 21 2012

Table 43. SNTP - Simple Network Time Protocol

Function	Privilege	Description	Example
`clock summer-time ACRONYM date (jan|feb|mar|apr|may|jun|jul|aug|sep|oct|nov|dec) <1-31> <2000-2037> HH:MM (jan|feb|mar|apr|may|jun|jul|aug|sep|oct|nov|dec) <1-31> <2000-2037> HH:MM [<1-1440>]`	Admin EXEC	Use the clock summer-time command to set daylight saving time for system time.	switch(config)# clock summer-time ACRONYM date jan 1 2017 00:00 apr 30 2017 23:59 60
`clock summer-time ACRONYM recurring (usa|eu) [<1-1440>]`	Admin EXEC	Use the global daylight saving policy defined by an international organization.	switch(config)# clock summer-time DLS recurring usa 60
`clock summer-time ACRONYM recurring (<1-5>|first|last) (sun|mon|tue|wed|thu|fri|sat) (jan|feb|mar|apr|may|jun|jul|aug|sep|oct|nov|dec) HH:MM (<1-5>|first|last) (sun|mon|tue|wed|thu|fri|sat) (jan|feb|mar|apr|may|jun|jul|aug|sep|oct|nov|dec) HH:MM [<1-1440>]`	Admin EXEC	Use the clock summer-time recurring daylight saving time duration. The first part of the command specifies when summer time begins, and the second part specifies when it ends.	clock summer-time ACRONYM recurring 1 sun jan 20:00 last sun jan 22:00 60
`no clock summer-time`	Admin EXEC	Use the no form of this command to clock summer-time default setting.	switch(config)# no clock summer-time

SMTP

Simple Mail Transfer Protocol (SMTP) is a protocol to send e-mail messages from a mail client to a mail server. SMTP by default uses TCP port 25. The commands presented in Table 44 configure the SMTP client.

Table 44. SMTP

Function	Privilege	Description	Example
`show smtp`	User EXEC	View SMTP client information.	
`smtpc profile-id <1-2> server-ip A.B.C.D server-port <25-25>`	Admin EXEC	Set SMTP server's IP and udp port in profile 1 or 2.	switch(config)# smtpc profile-id 1 server-ip 192.168.1.100 server-port 25
`smtpc profile-id <1-2> sender-mail WORD<1-64>`	Admin EXEC	Set sender's mail address in profile 1 or 2.	switch(config)# smtpc profile-id 1 sender-mail sender@example.com
`no smtpc profile-id <1-2> sender-mail`	Admin EXEC	Remove sender's mail address in profile 1 or 2.	switch(config)# no smtpc profile-id 1 sender-mail sender@example.com
`smtpc profile-id <1-2> target-mail WORD<1-64>`	Admin EXEC	Set target's mail address in profile 1 or 2.	switch(config)# smtpc profile-id 1 sender-mail target@example.com
`no smtpc profile-id <1-2> target-mail (all | WORD<1-64>)`	Admin EXEC	Remove target's mail address in profile 1 or 2.	switch(config)# no smtpc profile-id 1 sender-mail target@example.com
`smtpc active profile-id <1-2>`	Admin EXEC	Select an enabled profile for SMTP client used.	switch(config)# smtpc active profile-id 1
`no smtpc active profile`	Admin EXEC	SMTP client will not use any profile. It means disabled.	switch(config)# no smtpc active profile
`smtpc sendmsg title WORD<1-20> content WORD<1-64>`	Admin EXEC	Send a mail for testing SMTP client.	switch(config)# smtpc sendmsg title hello content world

RMON

Remote monitoring (RMON) uses a client-server model to monitor/ manage remote devices on a network.

Table 45. RMON

Function	Privilege	Description	Example
`show rmon (statistics | history | alarms | events)`	User EXEC	Display RMON setting configuration.	switch# show rmon history
`rmon statistics index <1-65535> interface IF_NMLPORT [owner OWNER<1-32>]`	Admin EXEC	Specify RMON statistics index. Specify statistics interface. Specify owner.	switch# configure switch(config)# rmon statistics index 10 interface gi1 owner ATI switch(config)# exit
`no rmon statistics index <1-65535>`	Admin EXEC	Delete snmp statistics index.	switch# configure switch(config)# no rmon statistics index 10 switch(config)# exit
`rmon history index <1-65535> interface IF_NMLPORT [buckets <1-50>] [interval <1-3600>] [owner OWNER<1-32>]`	Admin EXEC	Specify RMON history index. Specify history interface. Specify history bucket time. Specify history record interval time. Specify owner.	switch# configure switch(config)# rmon history index 10 interface gi1 buckets 20 interval 1000 owner ATI switch(config)# exit
`no rmon history index <1-65535>`	Admin EXEC	Delete SNMP history index.	switch# configure switch(config)# no rmon history index 10 switch(config)# exit
`rmon alarm index <1-65535> oid-variable OID<255> interval <1-2147483647> (absolute|delta) rising-threshold <0-2147483647> rising-event-index <1-65535> falling-threshold <0-2147483647> falling-event-index <1-65535> [owner OWNER<1-32>]`	Admin EXEC	Specify RMON alarm index. Specify alarm OID. Specify alarm check value frequency. How to compare values Specify rasing-threshold. Specify rasing-event-index. Specify falling-threshold. Specify falling-event-index. Specify owner.	switch# configure switch(config)# rmon statistics index 10 interface gi1 owner ATI switch(config)# exit
`no rmon alarm index <1-65535>`	Admin EXEC	Delete SNMP statistics index.	switch# configure switch(config)# no rmon alarm index 10 switch(config)# exit

Table 45. RMON (Continued)

Function	Privilege	Description	Example
`rmon event index <1-65535> description DESC<128> [log] [trap community-name OWNER<1-32>] [owner OWNER<1-32>]`	Admin EXEC	Specify RMON event index. Specify event description. Specify log flag for recording. Specify trap name to send SNMP trap message. Specify owner.	switch# configure switch(config)# rmon event index 10 description Good for us. log trap public owner ATI switch(config)# exit
`no rmon event index <1-65535>`	Admin EXEC	Delete SNMP event index.	switch# configure switch(config)# no rmon event index 10 switch(config)# exit

IP Configuration

The IP Configuration commands in Table 46 allow you to configure a static IPv4 IP address.

Table 46. IP Configuration

Function	Privilege	Description	Example
`ip address A.B.C.D [mask A.B.C.D]`	Admin EXEC	Use "IP address" command to modify administration IPv4 address.	switch(config)# ip address 192.168.1.200 mask 255.255.255.0
`ip default-gateway A.B.C.D`	Admin EXEC	Use "IP default-gateway" command to modify default gateway address.	switch(config)# ip default-gateway 192.168.1.100
`no ip default-gateway`	Admin EXEC	Use "No IP default-gateway" to restore default gateway address to factory default.	switch(config)# no ip default-gateway
`ip dns A.B.C.D [A.B.C.D]`	Admin EXEC	Use "IP DNS" command to modify DNS server address.	switch(config)# ip dns 111.111.111.111
`no ip dns A.B.C.D`	Admin EXEC	Use "No IP DNS" to delete existing DNS server.	switch(config)# no ip dns 111.111.111.111

TELNET

The Telnet service provides local management access via the Console port.

Table 47. TELNET

Function	Privilege	Description	Example
`ip telnet`	Admin EXEC	Use "IP service" command to enable telnet services.	switch(config)# ip telnet
`[no] ip telnet`	Admin EXEC	Use no form to disable service.	switch(config)# no ip telnet

SSH

Secure Shell (SSH) is a protocol providing secure (encrypted) management connection to a remote device.

Table 48. SSH

Function	Privilege	Description	Example
`ip ssh`	Admin EXEC	Use "IP service" command to enable ssh services.	switch(config)# ip ssh
`[no] ip ssh`	Admin EXEC	Use no form to disable service.	switch(config)# no ip ssh
`show ip ssh`	User EXEC	Show current ssh service status.	switch# show ip ssh

HTTP

The HTTP page allows you to combine all kinds of AAA lists to the HTTP line. Attempts to access the switch's Web UI from HTTP are first authenticated.

Table 49. HTTP

Function	Privilege	Description	Example
`ip http`	Admin EXEC	Use "IP service" command to enable http services.	switch(config)# ip http
`ip https`	Admin EXEC	Use "IP service" command to enable https services.	switch(config)# ip https
`[no] ip https`	Admin EXEC	Use no form to disable service.	switch(config)# no ip http
`[no] ip http`	Admin EXEC	Use no form to disable service.	switch(config)# no ip http switch(config)# no ip https

Table 49. HTTP (Continued)

Function	Privilege	Description	Example
`show ip (http|https)`	User EXEC	Show current https or http service status.	switch# show ip https
`ip (http|https) session-timeout <0-86400>`	Admin EXEC	Use "IP session-timeout" command to specify the session timeout value for http or https service.	switch(config)# ip http session-timeout 15 switch(config)# ip https session-timeout 20

Chapter 6

Diagnostics

The following feature commands are included in this chapter:

- ”Cable Diagnostic”
- “Device Monitoring Information” on page 88
- “IP-based Diagnostic” on page 89
- “Alarm LEDs” on page 89
- “System Commands” on page 90

Cable Diagnostic

The Cable Diagnostics page allows you to select the port for applying a copper test.

Table 50. Cable Diagnostic

<table>
<tr><th>Function</th><th>Privilege</th><th>Description</th><th>Example</th></tr>
<tr><td>show cable-diag interfaces IF_NML-PORTS</td><td>User EXEC</td><td>Display the estimated length of copper cable attached to the ports.
Show cable-diag interface all.
Display the estimated length of copper cables attached to all ports.
show cable-diag interface
Display the estimated length of copper cable attached to port gi1.</td><td>This example show the cable's information which link in gi1.
switch(config)# show cable-diag interfaces gi1
Port | Speed | Local pair | Pair length | Pair status
------ + ------- + ------------+ ------------- + --------------
gi1 |auto |Pair A |0.88 | Open
Pair B |0.87 | Open
Pair C |0.82 | Open
Pair D |0.82 | Open</td></tr>
</table>

Device Monitoring Information

The Device Monitoring Information (DMI) lists information, such as: System Name, System Location, MAC Address, Firmware version, and more, pertaining to the system. The information is for review only. To modify the device information, see the respective item within the user interface.

Table 51. DMI

Function	Privilege	Description	Example
`show dmi IF_PORTS information`	Admin EXEC	Use this command to display the information of EEPROM and Digital Diagnostic Monitoring Interface in SFP Optical Transceivers.	This example show SFP Optical Transceivers information which plug-in fa10. switch# show dmi FastEthernet 10 information
`[no] dmi (alarm|warning) (temperature|voltag|txbasis|txpower|rxpower) (high|low) state`	Admin EXEC	Use this command to enable/disable the mechanism that monitors SFP Optical Transceiver's Digital Diagnostic Monitoring interface information. Use no form to disable warning/alarm mechanism.	This example shows how to enable temperature's high threshold monitor mechanism with alarm level. (Current sfp plug-in in fa10). switch(config)# interface FastEthernet 10 switch(config-if)# dmi alarm temperature high state
`dmi (alarm|warning) (temperature|voltag|txbasis|txpower|rxpower) (high|low) value INPUT_VALUE`	Admin EXEC	Use this command to configure high/low threshold value used to compare with SFP Optical Transceiver's Digital Diagnostic Monitoring interface's value (temperature, voltage, etc).	This example shows how to configure the temperature high threshold value is 30.5 with alarm level. switch(config-if)# dmi alarm temperature high value 30.5
`[no] dmi alarm-warning message (log|snmp|mail)`	Admin EXEC	Use this command to determine which method to use when notifying of user alarm/warning events.	This example shows how to configure alarm-warning message is system log. switch(config)# dmi alarm-warning message log

IP-based Diagnostic

The IPv4 and IPv6 Ping tests allows you to configure the Ping Test for network connection diagnostics. the ARP commands show and clear entries in the ARP table.

Table 52. IP-based Diagnostic

Function	Privilege	Description	Example
`ping HOSTNAME [count <1-5>] [interval <1-5>] [size <8-5120>]`	User EXEC	Use "ping" command to do network ping diagnostic.	switch# ping 192.168.1.100 count 4 interval 4 size 128
`ping6 HOSTNAME [count <1-5>] [interval <1-5>] [size <8-5120>]`	User EXEC	Use "ping6" command to carry out network ping diagnostic.	switch# ping6 192.168.1.100 count 4 interval 4 size 128
`show arp`	User EXEC	Use "show arp" command to show all arp entries.	Switch# show arp
`clear arp [A.B.C.D]`	Admin EXEC	Use "clear arp" command to clear all arp entries or one specific arp entry.	Switch# clear arp

Alarm LEDs

The System and Alarm LEDs are configurable with the commands outlined in Table 53.

Table 53. Alarm LED

Function	Privilege	Description	Example
`show led`	User EXEC	Use "show LED" command to show current LED event status and error times. NOTE: Only valid after led command is successfully configured in switch(config)# mode.	This example shows current LED event and its own error times. switch# show led (ALARM LED) EVENTS | STATUS | ERROR TIMES ------------------------ + ----------- + ------------- Power Failure | ERROR | 1 ------------------------ + ----------- + -------------

Table 53. Alarm LED (Continued)

Function	Privilege	Description	Example
`[no] led (alarm)`	Admin EXEC	Use "LED (alarm)" command to configure LED indication mechanism. Use no form to disable LED indication mechanism configuration.	This example shows how to configure enable alarm LED indication mechanism. switch(config)# led alarm
`[no] led (alarm) (fiber-down | port-down | power-failure)`	Admin EXEC	Use "(fiber-down | port-down | power-failure)" command to configure which event will be binding with which LED indication mechanism. Use no form to remove event from LED indication mechanism.	- This example shows adding the fiber-down event to alarm LED indication mechanism: switch(config)# led alarm fiber-down - This example shows adding the port-down event to alarm LED indication mechanism: switch(config)# led alarm port-down GigabitEthernet 8

System Commands

Table 54. System

Function	Privilege	Description	Example
`show version`	User EXEC	Use "show version" command to show loader and firmware version and build date.	switch# show version
`show info`	User EXEC	Use "show info" command to show system summary information.	switch# show info
`reboot`	Admin EXEC	Use "reboot" command to make system hot restart.	switch# reboot
`show language`	User EXEC		
`show flash`	User EXEC	Use "show flash" command to show all files" status which stored in flash.	switch# show flash
`clear line telnet`	Admin EXEC		
`terminal length <0-24>`	User EXEC		
`show network-port`	User EXEC	Show network port information.	switch(config)# no network-port type http
`[no] network-port type (http|https|telnet|ssh)`	Admin EXEC	Use no form to restore default value.	

Table 54. System (Continued)

Function	Privilege	Description	Example
`network-port type (http|https|telnet|ssh) port-num <1-65535>`	Admin EXEC	Use the command to change network port.	switch(config)# network-port type http port-num 8080
`system name NAME`	Admin EXEC	Use "system name" command to modify system name information of the switch.	switch(config)# system name myname
`system location LOCATION`	Admin EXEC	Use "system contact" command to modify contact information of the switch.	switch(config)# system contact callme
`system contact CONTACT`	Admin EXEC	Use "system location" command to modify location information of the switch.	switch(config)# system location home