10 Port L2 Managed Gigabit Ethernet Switch with 2 Open SFP Slots - Rack Mountable

IES101002SFP

DE: Bedienungsanleitung - de.startech.com
FR: Guide de l'utilisateur - fr.startech.com
ES: Guía del usuario - es.startech.com
IT: Guida per l'uso - it.startech.com
NL: Gebruiksaanwijzing - nl.startech.com
PT: Guia do usuário - pt.startech.com

For the latest information, technical specifications, and support for this product, please visit www.startech.com/IES101002SFP.

ABOUT THIS MANUAL

Purpose This manual gives specific information on how to configure and manage the IES10100S2FP using the terminal console and telnet utility.

Audience This manual is intended for use by network administrators who are responsible for operating and maintaining network equipment; consequently, it assumes a basic network network knowledge of general switch functions, the Internet Protocol (IP), and Standard and Simple Network Management Protocol (SNMP).

CONTENTS

Content

Chapter 1 GENERAL

1.GENERAL

1.1General Commands

General Commands	Description
Help/?	Get help on a group or a specific command
Up	Move one command level up
Logout	Exit CLI
Command Prompt	
>	You can issue supported command here after login successfully.

1.2Command Groups

Command Groups	Description
System	System settings and reset options
IP	IP configuration and Ping
Port	Port management
MAC	MAC address table
VLAN	Virtual LAN
PVLAN	Private VLAN
Security	Security management
STP	Spanning Tree Protocol
Aggr	Link Aggregation
LACP	Link Aggregation Control Protocol
LLDP	Link Layer Discovery Protocol
LLDPMED	Link Layer Discovery Protocol Media
EEE	Energy Efficient Ethernet
Thermal	Thermal Protection
Led_power	LED power reduction
QoS	Quality of Service
Mirror	Port mirroring
Config	Load/Save of configuration via TFTP
Firmware	Download of firmware via TFTP

```
UPnP                    Universal Plug and Play
MVR                     Multicast VLAN Registration
Voice VLAN              Specific VLAN for voice traffic
Loop Protect            Loop Protection
IPMC                    MLD/IGMP Snooping
sFlow                   sFlow Agent
VCL                     VLAN Control List
Type '<group>' to enter command group, e.g. 'port'.
Type '<group> ?' to get list of group commands, e.g. 'port ?'.
Type '<command> ?' to get help on a command, e.g. 'port mode ?'.
Commands may be abbreviated, e.g. 'por co' instead of 'port configuration'.
```

Chapter 2 SYSTEM

2. SYSTEM

Available Commands:

System Configuration [all | (port <port_list>)]
System Log Configuration
System Timezone Configuration
System Version
System Log Server Mode [enable|disable]
System Name [<name>]
System Timezone Offset [<offset>]
System Contact [<contact>]
System Log Server Address [<ip_addr_string>]
System Timezone Acronym [<acronym>]
System DST Configuration
System Location [<location>]
System Log Level [info|warning|error]
System DST Mode [disable|recurring|non-recurring]
System DST start <week> <day> <month> <date> <year> <hour> <minute>
System Log Lookup [<log_id>] [all|info|warning|error]
System DST end <week> <day> <month> <date> <year> <hour> <minute>
System Log Clear [all|info|warning|error]
System Reboot
System DST Offset [<dst_offset>]
System Restore Default [keep_ip]
System Load

2.1 Configuration

System>configuration ?

Description:

Show system configuration.

Syntax:

System Configuration [all | (port <port_list>)]

Parameters:

all	Show all switch configuration, default: Show system configuration
port	Show switch port configuration
<port_list>	Port list or 'all', default: All ports

2.2 Log Configuration

System> log configuration ?

Description:

Show system log configuration.

Syntax:

System Log Configuration

2.3 Timezone Configuration

System/Timezone>configuration ?

Description:

Show System Timezone configuration.

Syntax:

System Timezone Configuration

2.4 Version

System>version ?

Description:

Show system version information.

Syntax:

System Version

2.5 Log Server Mode

System>log server mode ?

Description:

Show or set the system log server mode.

Syntax:

System Log Server Mode [enable|disable]

Parameters:

enable	Enable system log server mode
disable	Disable system log server mode
(default	Show system Log server mode)

2.6 Name

System>name ?

Description:

Set or show the system name.

Syntax:

System Name [<name>]

Parameters:

<name>: System name string. (1-255)

Use "" to clear the string

System name is a text string drawn from the alphabet (A-Za-z), digits (0-9), minus sign (-).

No blank or space characters are permitted as part of a name.

The first character must be an alpha character, and the first or last character must not be a minus sign.

2.7 Timezone offset

System>timezone offset ?

Description:

Set or show the system timezone offset.

Syntax:

System Timezone Offset [<offset>]

Parameters:

<offset> Time zone offset in minutes (-7200 to 7201) relative to UTC

2.8 Contact

System>contact ?

Description:

Set or show the system contact.

Syntax:

System Contact [<contact>]

Parameters:

<contact>	System contact string. (1-255) Use "" to clear the string In CLI, No blank or space characters are permitted as part of a contact.

2.9 Log Server Address

System>log server address ?

Description:

Show or set the system log server address.

Syntax:

System Log Server Address [<ip_addr_string>]

Parameters:

<ip_addr_string>	IP host address (a.b.c.d) or a host name string

2.10 Timezone Acronym

System>timezone acronym ?

Description:

Set or show the system timezone acronym.

Syntax:

System Timezone Acronym [<acronym>]

Parameters:

<acronym>	Time zone acronym (0 - 16 characters)

2.11 DST Configuration

System>dst configuration ?

Description:

Show Daylight Saving Time configuration.

Syntax:

System DST Configuration

2.12 Location

System>location ?

Description:

Set or show the system location.

Syntax:

System Location [<location>]

Parameters:

<location> System location string. (1-255)
Use "" to clear the string
In CLI, no blank or space characters are permitted as part of a location.

2.13 Log Level

System>log level ?

Description:

Show or set the system log level.

It uses to determine what kind of message will send to syslog server.

Syntax:

System Log Level [info|warning|error]

Parameters:

info	Send informations, warnings and errors
warning	Send warnings and errors
error	Send errors

2.14 DST Mode

System>dst mode ?

Description:

Set or show the daylight saving time mode.

Syntax:

System DST Mode [disable|recurring|non-recurring]

Parameters:

Disable	Disable Daylight Saving Time
recurring	Enable Daylight Saving Time as recurring mode
non-recurring	Enable Daylight Saving Time as non-recurring mode

2.15 DST Start

System>DST start ?

Description:

start: Set or show the daylight saving time start time settings

Syntax:

System DST start <week> <day> <month> <date> <year> <hour> <minute>

Parameters:

<week> : Week (1-5), 0: ignored
<day> : Day (1-7), 0: ignored
<month> : Month (1-12), 0: ignored
<date> : Date (1-31), 0: ignored
<year> : Year (2000-2097)

<hour> : Hour (0-23)
<minute>: Minutes (0-59)

2.16 Log Lookup

System>log lookup ?
Description:
Show the system log.

Syntax:

System Log Lookup [<log_id>] [all|info|warning|error]

Parameters:
<log_id>: System log ID or range (default: All entries)
all   : Show all levels (default)
info   : Show informations
warning : Show warnings
error   : Show errors

2.17 DST end

System>DST end ?
Description:
end: Set or show the daylight saving time end time settings

Syntax:

System DST end <week> <day> <month> <date> <year> <hour> <minute>

Parameters:
<week> : Week (1-5), 0: ignored
<day>   : Day (1-7), 0: ignored
<month> : Month (1-12), 0: ignored

<date> : Date (1-31), 0: ignored
<year> : Year (2000-2097)
<hour> : Hour (0-23)
<minute>: Minutes (0-59)

2.18 Log Clear

System>log clear ?
Description:
Clear the system log.

Syntax:

System Log Clear [all|info|warning|error]

Parameters:
all : Show all levels (default)
info : Show informations
warning : Show warnings
error : Show errors

2.19 Reboot

System>reboot ?
Description:
Reboot the system.

Syntax:

System Reboot

2.20 Dst offset

System>Dst offset ?

Description:

Set or show the daylight saving time offset.

Syntax:

System DST Offset [<dst_offset>]

Parameters:

<dst_offset>: DST offset in minutes (1 to 1440)

2.21 Restore Default

System>Restore Default ?

Description:

Restore factory default configuration.

Syntax:

System Restore Default [keep_ip]

Parameters:

keep_ip: Keep IP configuration, default: Restore full configuration

2.22 Load

System>Load ?

Description:

Show current CPU load: 100ms, 1s and 10s running average (in percent, zero is idle).

Syntax:

System Load

Chapter 3 IP

3. IP

Available Commands:

IP Configuration
IP DHCP [enable|disable]
IP Setup [<ip_addr>] [<ip_mask>] [<ip_router>] [<vid>]
IP Ping <ip_addr_string> [(Length <ping_length>)] [(Count <ping_count>)] [(Interval <ping_interval>)]
IP DNS [<ip_addr>]
IP DNS_Proxy [enable|disable]
IP IPv6 AUTOCONFIG [enable|disable]
IP IPv6 Setup [<ipv6_addr>] [<ipv6_prefix>] [<ipv6_router>]
IP IPv6 State <ipv6_addr> [enable|disable]
IP IPv6 Ping6 <ipv6_addr> [(Length <ping_length>)] [(Count <ping_count>)] [(Interval <ping_interval>)]
IP NTP Configuration
IP NTP Mode [enable|disable]
IP NTP Server Add <server_index> <ip_addr_string>
IP NTP Server Ipv6 Add <server_index> <server_ipv6>
IP NTP Server Delete <server_index>

3.1 Configuration

IP>Configuration ?
Description:
Show IP configuration.

Syntax:

IP Configuration

3.2 DHCP

IP>DHCP ?
Description:
Set or show the DHCP client mode.

Syntax:

IP DHCP [enable|disable]

Parameters:

enable	Enable or renew DHCP client
disable	Disable DHCP client

3.3 Setup

IP>setup ?
Description:
Set or show the IP setup.

Syntax:

IP Setup [<ip_addr>] [<ip_mask>] [<ip_router>] [<vid>]

Parameters:
<ip_addr> : IP address (a.b.c.d), default: Show IP address
<ip_mask> : IPv4 subnet mask (a.b.c.d), default: Show IPv4 mask
<ip_router>: IPv4 router (a.b.c.d), default: Show IPv4 router
<vid> : VLAN ID (1-4095), default: Show VLAN ID

3.4 Ping

IP>Ping ?
Description:
Ping IP address (ICMP echo).

Syntax:

IP Ping <ip_addr_string> [(Length <ping_length>)] [(Count <ping_count>)] [(Interval <ping_interval>)]

Parameters:

<ip_addr_string>	IPv4 host address (a.b.c.d) or a host name string
length	PING Length keyword
<ping_length>	Ping ICMP data length (2-1452; Default is 56), excluding MAC, IP and ICMP headers
count	PING Count keyword
<ping_count>	Transmit ECHO_REQUEST packet count (1-60; Default is 5)

interval PING Interval keyword
<ping_interval> Ping interval (0-30; Default is 0)

3.5 DNS

IP>DNS ?

Description:

Set or show the DNS server address.

Syntax:

IP DNS [<ip_addr>]

Parameters:

<ip_addr>: IP address (a.b.c.d), default: Show IP address

3.6 DNS_Proxy

IP>DNS_Proxy ?

Description:

Set or show the IP DNS Proxy mode.

Syntax:

IP DNS_Proxy [enable|disable]

Parameters:

enable : Enable DNS Proxy

disable: Disable DNS Proxy

3.7 IPv6 AUTOCONFIG

IP>IPv6 AUTOCONFIG ?

Description:

Set or show the IPv6 AUTOCONFIG mode.

Syntax:

IP IPv6 AUTOCONFIG [enable|disable]

Parameters:

enable	Enable IPv6 AUTOCONFIG mode
disable	Disable IPv6 AUTOCONFIG mode

3.8 IPv6 Setup

IP>IPv6 Setup ?

Description:

Set or show the IPv6 setup.

Syntax:

IP IPv6 Setup [<ipv6_addr>] [<ipv6_prefix>] [<ipv6_router>]

Parameters:

<ipv6_addr>	IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separates each field (:). For example, four hexadecimal digits with a colon separates each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can only appear once. It also used a following legally IPv4 address. For example,'::192.1.2.34'.
<ipv6_prefix>	IPv6 subnet mask , default: Show IPv6 prefix
<ipv6_router>	IPv6 router , default: Show IPv6 router. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separates each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can only appear once. It also used a following legally IPv4 address. For example,'::192.1.2.34'.

3.9 IPv6 State

IP>IPv6 State ?

Description:

Set or show the IPv6 Interface operational state.

Syntax:

IP IPv6 State <ipv6_addr> [enable|disable]

Parameters:

<ipv6_addr>	IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separates each field (:). For example, four hexadecimal digits with a colon separates each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can only appear once. It also used a following legally IPv4 address. For example,'::192.1.2.34'.
enable	Enable the designated IPv6 Interface
disable	Disable the designated IPv6 Interface

3.10 NTP Configuration

IP>NTP Configuration ?

Description:

Show NTP configuration.

Syntax:

IP NTP Configuration

3.11 NTP Mode

IP>NTP Mode ?
Description:
Set or show the NTP mode.

Syntax:

IP NTP Mode [enable|disable]

Parameters:

enable	Enable NTP mode
disable	Disable NTP mode

(default: Show NTP mode)

3.12 NTP Mode

IP>NTP Server Add ?
Description:
Add NTP server entry.

Syntax:

IP NTP Server Add <server_index> <ip_addr_string>

Parameters:
<server_index> : The server index (1-5)
<ip_addr_string>: IP host address (a.b.c.d) or a host name string

3.13 NTP Server IPv6 Add

IP>NTP Server IPv6 Add ?

Description:

Add NTP server IPv6 entry.

Syntax:

IP NTP Server Ipv6 Add <server_index> <server_ipv6>

Parameters:

<server_index> The server index (1-5)

<server_ipv6> IPv6 server address.
IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separates each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can only appear once. It also used a following legally IPv4 address. For example,'::192.1.2.34'.

3.14 NTP Server IPv6 Add

IP>NTP Server Delete ?

Description:

Delete NTP server entry.

Syntax:

IP NTP Server Delete <server_index>

Parameters:

<server_index>: The server index (1-5)

3.15 NTP Server Delete

IP>NTP Server Delete ?

Description:

Delete NTP server entry.

Syntax:

IP NTP Server Delete <server_index>

Parameters:

<server_index>: The server index (1-5)

Chapter 4 PORT

4. PORT

Available Commands:

Port Configuration [<port_list>] [up|down]
Port Mode [<port_list>] [auto|10hdx|10fdx|100hdx|100fdx|1000fdx|sfp_auto_ams]
Port Flow Control [<port_list>] [enable|disable]
Port State [<port_list>] [enable|disable]
Port MaxFrame [<port_list>] [<max_frame>]
Port Power [<port_list>] [enable|disable|actiphy|dynamic]
Port Excessive [<port_list>] [discard|restart]
Port Statistics [<port_list>] [<command>] [up|down]
Port VeriPHY [<port_list>]
Port SFP [<port_list>]

4.1 Configuration

Port>Configuration ?
Description:
Show port configuration.

Syntax:

Port Configuration [<port_list>] [up|down]

Parameters:
<port_list>: Port list or 'all', default: All ports
up : Show ports, which are up
down : Show ports, which are down

4.2 Mode

Port>Mode ?
Description:
Set or show the port speed and duplex mode.

Syntax:

Port Mode [<port_list>] [auto|10hdx|10fdx|100hdx|100fdx|1000fdx|sfp_auto_ams]

Parameters:
<port_list> Port list or 'all', default: All ports
auto Auto negotiation of speed and duplex
10hdx 10 Mbps, half duplex
10fdx 10 Mbps, full duplex
100hdx 100 Mbps, half duplex

100fdx 100 Mbps, full duplex
1000fdx 1 Gbps, full duplex
sfp_auto_ams Auto detection of SFP
(default: Show configured and current mode)

4.3 Flow Control

Port>Flow Control ?

Description:

Set or show the port flow control mode.

Syntax:

Port Flow Control [<port_list>] [enable|disable]

Parameters:

<port_list> Port list or 'all', default: All ports
enable Enable flow control
disable Disable flow control
(default: Show flow control mode)

4.4 State

Port>State ?

Description:

Set or show the port administrative state.

Syntax:

Port State [<port_list>] [enable|disable]

Parameters:

<port_list> Port list or 'all', default: All ports
enable Enable port

disable Disable port
(default: Show administrative mode)

4.5 MaxFrame

Port>MaxFrame ?
Description:
Set or show the port maximum frame size.

Syntax:

Port MaxFrame [<port_list>] [<max_frame>]

Parameters:
<port_list> Port list or 'all', default: All ports
<max_frame> Port maximum frame size (1518-9600), default: Show maximum frame size

4.6 Power

Port>Power ?
Description:
Set or show the port PHY power mode.

Syntax:

Port Power [<port_list>] [enable|disable|actiphy|dynamic]

Parameters:
<port_list> Port list or 'all', default: All ports
enable Enable all power control
disable Disable all power control
actiphy Enable ActiPHY power control
dynamic Enable Dynamic power control

4.7 Excessive

Port>Excessive ?

Description:

Set or show the port excessive collision mode.

Syntax:

Port Excessive [<port_list>] [discard|restart]

Parameters:

<port_list> Port list or 'all', default: All ports

discard Discard frame after 16 collisions

restart Restart backoff algorithm after 16 collisions

(default: Show mode)

4.8 Statistics

Port>Statistics ?
Description:
Show port statistics.

Syntax:

Port Statistics [<port_list>] [<command>] [up|down]

Parameters:

<port_list>	Port list or 'all', default: All ports
<command>	The command parameter takes the following values:
clear	Clear port statistics
packets	Show packet statistics
bytes	Show byte statistics
errors	Show error statistics
discards	Show discard statistics
filtered	Show filtered statistics
0..7	Show priority statistics
(default: Show all port statistics)	
up	Show ports, which are up
down	Show ports, which are down

4.9 VeriPHY

Port>VeriPHY ?
Description:
Run cable diagnostics.

Syntax:

Port VeriPHY [<port_list>]

Parameters:

<port_list> Port list or 'all', default: All ports

4.10 SFP

Port>SFP ?

Description:

Show the detected sfp type.

Syntax:

Port SFP [<port_list>]

Parameters:

<port_list> Port list or 'all', default: All ports

Chapter 5 MAC

5.MAC

Available Commands:

MAC Configuration [<port_list>]
MAC Add <mac_addr> <port_list> [<vid>]
MAC Delete <mac_addr> [<vid>]
MAC Lookup <mac_addr> [<vid>]
MAC Agetime [<age_time>]
MAC Learning [<port_list>] [auto|disable|secure]
MAC Dump [<mac_max>] [<mac_addr>] [<vid>]
MAC Statistics [<port_list>]
MAC Flush

5.1 Configuration

MAC>configuration ?
Description:
Show MAC address table configuration.

Syntax:

MAC Configuration [<port_list>]

Parameters:
<port_list>: Port list or 'all', default: All ports

5.2 Add

MAC>Add ?
Description:
Add MAC address table entry.

Syntax:

MAC Add <mac_addr> <port_list> [<vid>]

Parameters:

<mac_addr>	MAC address ('xx-xx-xx-xx-xx-xx' or 'xx.xx.xx.xx.xx.xx' or 'xxxxxxxxxxxx', x is a hexadecimal digit)
<port_list>	Port list or 'all' or 'none'
<vid>	VLAN ID (1-4095), default: 1

5.3 Delete

MAC>delete ?
Description:
Delete MAC address entry.

Syntax:

MAC Delete <mac_addr> [<vid>]

Parameters:

<mac_addr>	MAC address ('xx-xx-xx-xx-xx-xx' or 'xx.xx.xx.xx.xx.xx' or 'xxxxxxxxxxxx', x is a hexadecimal digit)
<vid>	VLAN ID (1-4095), default: 1

5.4 Lookup

MAC>Lookup ?
Description:
Lookup MAC address entry.

Syntax:

MAC Lookup <mac_addr> [<vid>]

Parameters:

<mac_addr>	MAC address ('xx-xx-xx-xx-xx-xx' or 'xx.xx.xx.xx.xx.xx' or 'xxxxxxxxxxxx', x is a hexadecimal digit)
<vid>	VLAN ID (1-4095), default: 1

5.5 Agetime

MAC>Agetime ?

Description:

Set or show the MAC address age timer.

Syntax:

MAC Agetime [<age_time>]

Parameters:

<age_time>: MAC address age time (0,10-1000000) 0=disable, default: Show age time

5.6 Learning

MAC>Learning ?

Description:

Set or show the port learn mode.

Syntax:

MAC Learning [<port_list>] [auto|disable|secure]

Parameters:

<port_list>	Port list or 'all', default: All ports
auto	Automatic learning
disable	Disable learning
secure	Secure learning

(default: Show learn mode)

5.7 Dump

MAC>Dump ?

Description:

Show sorted list of MAC address entries.

Syntax:

MAC Dump [<mac_max>] [<mac_addr>] [<vid>]

Parameters:

<mac_max>	Maximum number of MAC addresses, default: Show all addresses
<mac_addr>	First MAC address ('xx-xx-xx-xx-xx-xx' or 'xx.xx.xx.xx.xx.xx' or 'xxxxxxxxxxxx', x is a hexadecimal digit), default: MAC address zero
<vid>	First VLAN ID (1-4095), default: 1

5.8 Statistics

MAC>Statistics ?

Description:

Show MAC address table statistics.

Syntax:

MAC Statistics [<port_list>]

Parameters:

<port_list>: Port list or 'all', default: All ports

5.9 Flush

MAC>flush ?

Description:

Flush all learned entries.

Syntax:

MAC Flush

Chapter 6 VLAN

6.VLAN

Available Commands:

VLAN Configuration [<port_list>]
VLAN PVID [<port_list>] [<vid>|none]
VLAN FrameType [<port_list>] [all|tagged|untagged]
VLAN IngressFilter [<port_list>] [enable|disable]
VLAN tx_tag [<port_list>] [untag_pvid|untag_all|tag_all]
VLAN PortType [<port_list>] [unaware|c-port|s-port|s-custom-port]
VLAN EtypeCustomSport [<etype>]
VLAN Add <vid>|<name> [<ports_list>]
VLAN Forbidden Add <vid>|<name> [<port_list>]
VLAN Delete <vid>|<name>
VLAN Forbidden Delete <vid>|<name>
VLAN Forbidden Lookup [<vid>] [(name <name>)]
VLAN Lookup [<vid>] [(name <name>)] [combined|static|nas|mvr|voice_vlan|all]
VLAN Name Add <name> <vid>
VLAN Name Delete <name>
VLAN Name Lookup [<name>]
VLAN Status [<port_list>] [combined|static|nas|mvr|voice_vlan|mstp|vcl|all|conflicts]

6.1 Configuration

VLAN>Configuration ?
Description:
Show VLAN configuration.

Syntax:

VLAN Configuration [<port_list>]

Parameters:
<port_list> Port list or 'all', default: All ports

6.2 PVID

VLAN>PVID ?
Description:
Set or show the port VLAN ID.

Syntax:

VLAN PVID [<port_list>] [<vid>|none]

Parameters:
<port_list> Port list or 'all', default: All ports
<vid>|none Port VLAN ID (1-4095) or 'none', default: Show port VLAN ID

6.4 FrameType

VLAN>FrameType ?
Description:
Set or show the port VLAN frame type.

Syntax:

VLAN FrameType [<port_list>] [all|tagged|untagged]

Parameters:
<port_list>: Port list or 'all', default: All ports
all : Allow tagged and untagged frames
tagged : Allow tagged frames only
untagged : Allow untagged frames only
(default: Show accepted frame types)

6.5 IngressFilter

VLAN>IngressFilter ?
Description:
Set or show the port VLAN ingress filter.

Syntax:

VLAN IngressFilter [<port_list>] [enable|disable]

Parameters:

<port_list>	Port list or 'all', default: All ports
enable	Enable VLAN ingress filtering
disable	Disable VLAN ingress filtering

(default: Show VLAN ingress filtering)

6.6 TX_tag

VLAN>tx_tag ?
Description:
Set or show the port egress tagging.

Syntax:

VLAN tx_tag [<port_list>] [untag_pvid|untag_all|tag_all]

Parameters:

<port_list>	Port list or 'all', default: All ports
Tx tag	(Egress tagging)
untag_pvid	All VLANs except pvid will be tagged
untag_all	All VLANs will be untagged
tag_all	All VLANs will be tagged

6.7 PortType

VLAN>PortType ?
Description:
Set or show the VLAN port Type.

Syntax:

VLAN PortType [<port_list>] [unaware|c-port|s-port|s-custom-port]

Parameters:

<port_list>	Port list or 'all', default: All ports
Port Type	

6.8 EtypeCustomSport

VLAN>EtypeCustomSport ?

Description:

Set or show the Custom S-port EtherType.

Syntax:

VLAN EtypeCustomSport [<etype>]

Parameters:

Ether Type (0x0600-0xFFFF)

6.9 Add

VLAN>Add ?

Description:

Add or modify VLAN entry.

Syntax:

VLAN Add <vid>|<name> [<ports_list>]

Parameters:

<vid>|<name>	VLAN ID (1-4095) or VLAN Name
<ports_list>	Ports list. By default none of the ports are selected. To select all ports, use 'all' keyword

6.9 Forbidden Add

VLAN>Forbidden Add ?

Description:

Add or modify VLAN entry in forbidden table.

Syntax:

VLAN Forbidden Add <vid>|<name> [<port_list>]

Parameters:

<vid>|<name>	VLAN ID (1-4095) or VLAN Name
<port_list>	Port list or 'all', default: All ports

6.10 Delete

VLAN>Delete ?

Description:

Delete VLAN entry.

Syntax:

VLAN Delete <vid>|<name>

Parameters:

<vid>|<name>	VLAN ID (1-4095) or VLAN Name

6.11 Forbbiden Delete

VLAN>Forbidden Delete ?
Description:
Delete VLAN entry.

Syntax:

VLAN Forbidden Delete <vid>|<name>

Parameters:

<vid>|<name>	VLAN ID (1-4095) or VLAN Name

6.12 Forbbiden Lookup

VLAN>Forbidden Lookup ?
Description:
Lookup VLAN Forbidden port entry.

Syntax:

VLAN Forbidden Lookup [<vid>] [(name <name>)]

Parameters:

<vid>	VLAN ID (1-4095), default: Show all VLANs
name	VLAN name string
<name>	VLAN name - Maximum of 32 characters. VLAN Name can only contain alphabets or numbers.

VLAN name should contain at least one alphabet.

6.13 Lookup

VLAN>Lookup ?

Description:

Lookup VLAN entry.

Syntax:

VLAN Lookup [<vid>] [(name <name>)] [combined|static|nas|mvr|voice_vlan|all]

Parameters:

<vid>	VLAN ID (1-4095), default: Show all VLANs
name	VLAN name string
<name>	VLAN name - Maximum of 32 characters. VLAN Name can only contain alphabets or numbers.

VLAN name should contain at least one alphabet.

combined	Shows All the Combined VLAN database
static	Shows the VLAN entries configured by the administrator
nas	Shows the VLANs configured by NAS
mvr	Shows the VLANs configured by MVR
voice_vlan	Shows the VLANs configured by Voice VLAN
all	Shows all VLANs configuration

(default: combined VLAN Users configuration)

6.14 Name Add

VLAN>Name Add ?

Description:

Add VLAN Name to a VLAN ID Mapping.

Syntax:

VLAN Name Add <name> <vid>

Parameters:

<name>	VLAN name - Maximum of 32 characters. VLAN Name can only contain alphabets or numbers.

VLAN name should contain at least one alphabet.

<vid>	VLAN ID (1-4095)

6.15 Name Add

VLAN>Name Delete ?

Description:

Delete VLAN Name to VLAN ID Mapping.

Syntax:

VLAN Name Delete <name>

Parameters:

<name>	VLAN name - Maximum of 32 characters. VLAN Name can only contain alphabets or numbers.

VLAN name should contain at least one alphabet.

6.16 Name Lookup

VLAN>Name Lookup ?
Description:
Show VLAN Name table.

Syntax:

VLAN Name Lookup [<name>]

Parameters:
<name>: VLAN name - Maximum of 32 characters. VLAN Name can only contain alphabets or numbers.
VLAN name should contain at least one alphabet.

6.17 Status

VLAN>Status ?
Description:
VLAN Port Configuration Status.

Syntax:

VLAN Status [<port_list>] [combined|static|nas|mvr|voice_vlan|mstp|vcl|all|conflicts]

Parameters:

<port_list>	Port list or 'all', default: All ports
combined	combined VLAN Users configuration
static	static port configuration
nas	NAS port configuration
mvr	MVR port configuration
voice_vlan	Voice VLAN port configuration

mstp MSTP port configuration
vcl VCL port configuration
all All VLAN Users configuration
(default: all VLAN Users configuration)

Chapter 7 PVLAN

7.PVLAN

Available Commands:

PVLAN Configuration [<port_list>]
PVLAN Add <pvlan_id> [<port_list>]
PVLAN Delete <pvlan_id>
PVLAN Lookup [<pvlan_id>]
PVLAN Isolate [<port_list>] [enable|disable]

7.1 Configuration

PVLAN>Configuration ?

Description:

Show Private VLAN configuration.

Syntax:

PVLAN Configuration [<port_list>]

Parameters:

<port_list>	Port list or 'all', default: All ports

7.2 Add

PVLAN>Add ?

Description:

Add or modify Private VLAN entry.

Syntax:

PVLAN Add <pvlan_id> [<port_list>]

Parameters:

<pvlan_id>	Private VLAN ID. The allowed range for a Private VLAN ID is the same as the switch port number range.
<port_list>	Port list or 'all', default: All ports

7.3 Delete

PVLAN>Delete ?
Description:
Delete Private VLAN entry.

Syntax:

PVLAN Delete <pvlan_id>

Parameters:
<pvlan_id> Private VLAN ID. The allowed range for a Private VLAN ID is the same as the switch port number range.

7.4 Lookup

PVLAN>Lookup ?
Description:
Lookup Private VLAN entry.

Syntax:

PVLAN Lookup [<pvlan_id>]

Parameters:
<pvlan_id> Private VLAN ID, default: Show all PVLANs. The allowed range for a Private
VLAN ID is the same as the switch port number range.

7.5 Isolate

PVLAN>Isolate ?

Description:

Set or show the port isolation mode.

Syntax:

PVLAN Isolate [<port_list>] [enable|disable]

Parameters:

<port_list>	Port list or 'all', default: All ports
enable	Enable port isolation
disable	Disable port isolation

(default: Show port isolation port list)

Chapter 8 SECURITY

8.SECURITY

Command Groups:

Switch : Switch security
Network : Network security
AAA : Authentication, Authorization and Accounting

8.1 Switch

Command Groups:

Security Switch Users	User management
Security Switch Privilege	Privilege level
Security Switch Auth	Authentication
Security Switch SSH	Secure Shell
Security Switch HTTPS	Hypertext Transfer Protocol over Secure Socket Layer
Security Switch Access	Access management
Security Switch SNMP	Simple Network Management Protocol
Security Switch RMON	Remote Network Monitoring

8.1.1 Switch Users

Available Commands:

Security Switch Users Configuration
Security Switch Users Add <user_name> <password> <privilege_level>
Security Switch Users Delete <user_name>

8.1.1.1 Configuration

Security/Switch/Users>Configuration ?
Description:
Show users configuration.

Syntax:

Security Switch Users Configuration

8.1.1.2 Add

Security/Switch/Users>Add ?

Description:

Add or modify users entry.

Syntax:

Security Switch Users Add <user_name> <password> <privilege_level>

Parameters:

<user_name>	A string identifying the user name that this entry should belong to. The allowed string length is (1-31). The valid user name is a combination of letters, numbers and underscores
<password>	The password for this user name. The allowed string length is (0-31). Use 'clear' or "" as null string
<privilege_level>	User privilege level (1-15)

8.1.1.3 Delete

Security/Switch/Users>Delete ?

Description:

Delete users entry.

Syntax:

Security Switch Users Delete <user_name>

Parameters:

<user_name>	A string identifying the user name that this entry should belong to. The allowed string length is (1-31). The valid

user name is a combination of letters, numbers and underscores

8.1.2 Switch Privilege

Available Commands:

Security Switch Privilege Level Configuration
Security Switch Privilege Level Group <group_name> [<cro>] [<crw>] [<sro>] [<srw>]
Security Switch Privilege Level Current

8.1.2.1 Level Configuration

Security/Switch/Privilege>Level Configuration ?
Description:
Show privilege configuration.

Syntax:

Security Switch Privilege Level Configuration

8.1.2.2 Level Group

Security/Switch/Privilege>Level Group ?

Description:

Configure a privilege level group.

Syntax:

Security Switch Privilege Level Group <group_name>
[<cro>] [<crw>] [<sro>] [<srw>]

Parameters:

<group_name>	Privilege group name
<cro>	Configuration read-only privilege level (1-15)
<crw>	Configuration/Execute read-write privilege level (1-15)
<sro>	Status/Statistics read-only privilege level (1-15)
<srw>	Status/Statistics read-write privilege level (1-15)

8.1.2.3 Level Current

Security/Switch/Privilege>Level Current ?

Description:

Show the current privilege level.

Syntax:

Security Switch Privilege Level Current

8.1.3 Switch Auth

Available Commands:

Security Switch Auth Configuration	
Security Switch Auth Method	[console|telnet|ssh|web] [none|local|radius|tacacs+] [enable|disable]

8.1.3.1 Configuration

Security/Switch/Auth>Configuration ?

Description:

Show Auth configuration.

Syntax:

Security Switch Auth Configuration

8.1.3.2 Method

Security/Switch/Auth>Method ?

Description:

Set or show Auth method. (default: Show Auth method).

Syntax:

Security Switch Auth Method	[console|telnet|ssh|web] [none|local|radius|tacacs+] [enable|disable]

Parameters:

console	Settings for console
telnet	Settings for telnet
ssh	Settings for ssh
web	Settings for web
	(default: Set or show the specific client authentication method)
none	Authentication disabled
local	Use local authentication
radius	Use remote RADIUS authentication
tacacs+	Use remote TACACS+ authentication
	(default: Show client authentication method)
enable	Enable local authentication if remote authentication fails
disable	Disable local authentication if remote authentication fails
	(The parameter is effective when it is typed)

8.1.4 Switch SSH

Available Commands:

Security Switch SSH Configuration
Security Switch SSH Mode [enable|disable]

8.1.4.1 Configuration

Security/Switch/SSH>Configuration ?
Description:
Show SSH configuration.

Syntax:

Security Switch SSH Configuration

8.1.4.2 Mode

Security/Switch/SSH>Mode ?
Description:
Set or show the SSH mode.

Syntax:

Security Switch SSH Mode [enable|disable]

Parameters:
enable : Enable SSH
disable: Disable SSH

(default: Show SSH mode)

8.1.5 Switch HTTPS

Available Commands:

Security Switch HTTPS Configuration
Security Switch HTTPS Mode [enable|disable]
Security Switch HTTPS Redirect [enable|disable]

8.1.5.1 Configuration

Security/Switch/HTTPS>Configuration ?
Description:
Show HTTPS configuration.

Syntax:

Security Switch HTTPS Configuration

8.1.5.2 Mode

Security/Switch/HTTPS>Mode ?
Description:
Set or show the HTTPS mode.

Syntax:

Security Switch HTTPS Mode [enable|disable]

Parameters:
enable : Enable HTTPS

disable: Disable HTTPS
(default: Show HTTPS mode)

8.1.5.3 Redirect

Security/Switch/HTTPS>Redirect ?
Description:
Set or show the HTTPS redirect mode.
Automatic redirect web browser to HTTPS during HTTPS mode enabled.

Syntax:

Security Switch HTTPS Redirect [enable|disable]

Parameters:
enable Enable HTTPS redirect
disable Disable HTTPS redirect
(default: Show HTTPS redirect mode)

8.1.6 Switch Access

Available Commands:

Security Switch Access Configuration
Security Switch Access Mode [enable|disable]
Security Switch Access Add <access_id> <start_ip_addr> <end_ip_addr>
[web] [snmp] [telnet]
Security Switch Access Ipv6 Add <access_id> <start_ipv6_addr> <end_ipv6_addr>
[web] [snmp] [telnet]
Security Switch Access Delete <access_id>
Security Switch Access Lookup [<access_id>]

Security Switch Access Clear
Security Switch Access Statistics [clear]

8.1.6.1 Configuration

Security/Switch/Access>Configuration ?
Description:
Show access management configuration.

Syntax:

Security Switch Access Configuration

8.1.6.2 Mode

Security/Switch/Access>Mode ?
Description:
Set or show the access management mode.

Syntax:

Security Switch Access Mode [enable|disable]

Parameters:
enable Enable access management
disable Disable access management
(default: Show access management mode)

8.1.6.3 Add

Security/Switch/Access>Add ?

Description:

Add access management entry, default: Add all supported protocols.

Syntax:

Security Switch Access Add <access_id> <start_ip_addr> <end_ip_addr>
[web] [snmp] [telnet]

Parameters:

<access_id>	entry index (1-16)
<start_ip_addr>	Start IP address (a.b.c.d)
<end_ip_addr>	End IP address (a.b.c.d)
web	Indicates that the host can access the switch from HTTP/HTTPS
snmp	Indicates that the host can access the switch from SNMP
telnet	Indicates that the host can access the switch from TELNET/SSH

8.1.6.4 IPv6 Add

Security/Switch/Access>IPv6 Add ?

Description:

Add access management IPv6 entry, default: Add all supported protocols.

Syntax:

Security Switch Access Ipv6 Add <access_id> <start_ipv6_addr> <end_ipv6_addr> [web] [snmp] [telnet]

Parameters:

<access_id>	entry index (1-16)
<start_ipv6_addr>	Start IPv6 address. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separates each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can only appear once. It also used a following legally IPv4 address. For example,'::192.1.2.34'.
<end_ipv6_addr>	End IPv6 address. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separates each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can only appear once. It also used a following legally IPv4 address. For example,'::192.1.2.34'.
web	Indicates that the host can access the switch from HTTP/HTTPS
snmp	Indicates that the host can access the switch from SNMP
telnet	Indicates that the host can access the switch from TELNET/SSH

8.1.6.5 Delete

Security/Switch/Access>Delete ?

Description:

Delete access management entry.

Syntax:

Security Switch Access Delete <access_id>

Parameters:

<access_id>: entry index (1-16)

8.1.6.6 Lookup

Security/Switch/Access>Lookup ?

Description:

Lookup access management entry.

Syntax:

Security Switch Access Lookup [<access_id>]

Parameters:

<access_id>: entry index (1-16)

8.1.6.7 Clear

Security/Switch/Access>Clear ?

Description:

Clear access management entry.

Syntax:

Security Switch Access Clear

8.1.6.8 Statistics

Security/Switch/Access>Statistics ?

Description:

Show or clear access management statistics.

Syntax:

Security Switch Access Statistics [clear]

Parameters:

clear	Clear access management statistics

8.1.7 Switch SNMP

Available Commands:

Security Switch SNMP Configuration
Security Switch SNMP Mode [enable|disable]
Security Switch SNMP Version [1|2c|3]
Security Switch SNMP Read Community [<community>]
Security Switch SNMP Write Community [<community>]
Security Switch SNMP Trap Mode [enable|disable]
Security Switch SNMP Trap Version [1|2c|3]
Security Switch SNMP Trap Community [<community>]
Security Switch SNMP Trap Destination [<ip_addr_string>]
Security Switch SNMP Trap IPv6 Destination [<ipv6_addr>]
Security Switch SNMP Trap Authentication Failure [enable|disable]
Security Switch SNMP Trap Link-up [enable|disable]
Security Switch SNMP Trap Inform Mode [enable|disable]
Security Switch SNMP Trap Inform Timeout [<timeout>]
Security Switch SNMP Trap Inform Retry Times [<retries>]
Security Switch SNMP Trap Probe Security Engine ID [enable|disable]
Security Switch SNMP Trap Security Engine ID [<engineid>]
Security Switch SNMP Trap Security Name [<security_name>]
Security Switch SNMP Engine ID [<engineid>]
Security Switch SNMP Community Add <community> [<ip_addr>] [<ip_mask>]
Security Switch SNMP Community Delete <index>
Security Switch SNMP Community Lookup [<index>]
Security Switch SNMP User Add <engineid> <user_name> [MD5|SHA]
[<auth_password>] [DES] [<priv_password>]
Security Switch SNMP User Delete <index>
Security Switch SNMP User Changekey <engineid> <user_name>
<auth_password> [<priv_password>]
Security Switch SNMP User Lookup [<index>]
Security Switch SNMP Group Add <security_model> <security_name> <group_name>
Security Switch SNMP Group Delete <index>

Security Switch SNMP Group Lookup [<index>]
Security Switch SNMP View Add <view_name> [included|excluded] <oid_subtree>
Security Switch SNMP View Delete <index>
Security Switch SNMP View Lookup [<index>]

Security Switch SNMP Access Add <group_name> <security_model> <security_level>
[<read_view_name>] [<write_view_name>]
Security Switch SNMP Access Delete <index>
Security Switch SNMP Access Lookup [<index>]

8.1.7.1 Configuration

Security/Switch/SNMP>Configuration ?
Description:
Show SNMP configuration.

Syntax:

Security Switch SNMP Configuration

8.1.7.2 Mode

Security/Switch/SNMP>Mode ?
Description:
Set or show the SNMP mode.

Syntax:

Security Switch SNMP Mode [enable|disable]

Parameters:

enable	Enable SNMP
disable	Disable SNMP

(default: Show SNMP mode)

8.1.7.3 Version

Security/Switch/SNMP>Version ?

Description:

Set or show the SNMP protocol version.

Syntax:

Security Switch SNMP Version [1|2c|3]

Parameters:

1 SNMP version 1

2c SNMP version 2c

3 SNMP version 3

(default: Show SNMP version)

8.1.7.4 Read Community

Security/Switch/SNMP>Read Community ?

Description:

Set or show the community string for SNMP read access.

Syntax:

Security Switch SNMP Read Community [<community>]

Parameters:

<community>: Community string. Use 'clear' or "" to clear the string

Maximum length allowed is upto 256 characters.

(default: Show SNMP read community)

8.1.7.5 Write Community

Security/Switch/SNMP>Write Community ?
Description:
Set or show the community string for SNMP write access.

Syntax:

Security Switch SNMP Write Community [<community>]

Parameters:
<community>: Community string. Use 'clear' or "" to clear the string
Maximum length allowed is upto 256 characters.
(default: Show SNMP write community)

8.1.7.6 Trap Mode

Security/Switch/SNMP>Trap Mode ?
Description:
Set or show the SNMP trap mode.

Syntax:

Security Switch SNMP Trap Mode [enable|disable]

Parameters:
enable : Enable SNMP traps
disable: Disable SNMP traps
(default: Show SNMP trap mode)

8.1.7.7 Trap Version

Security/Switch/SNMP>Trap Version ?

Description:

Set or show the SNMP trap protocol version.

Syntax:

Security Switch SNMP Trap Version [1|2c|3]

Parameters:

1 SNMP version 1

2c SNMP version 2c

3 SNMP version 3

(default: Show SNMP trap version)

8.1.7.8 Trap Community

Security/Switch/SNMP>Trap community ?

Description:

Set or show the community string for SNMP traps.

Syntax:

Security Switch SNMP Trap Community [<community>]

Parameters:

<community> Community string. Use 'clear' or "" to clear the string
Maximum length allowed is upto 256 characters.

(default: Show SNMP trap community)

8.1.7.9 Trap Destination

Security/Switch/SNMP>Trap Destination ?

Description:

Set or Show the SNMP trap destination address.

Syntax:

Security Switch SNMP Trap Destination [<ip_addr_string>]

Parameters:

<ip_addr_string>: IP host address (a.b.c.d) or a host name string

8.1.7.10 Trap IPv6 Destination

Security/Switch/SNMP>Trap IPv6 Destination ?

Description:

Set or Show the SNMP trap destination IPv6 address.

Syntax:

Security Switch SNMP Trap IPv6 Destination [<ipv6_addr>]

Parameters:

<ipv6_addr> IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separates each field (:). For example, four hexadecimal digits with a colon separates each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can only

appear once. It also used a following legally IPv4 address.
For example,'::192.1.2.34'.

8.1.7.11 Trap Authentication Failure

Security/Switch/SNMP>Trap Authentication Failure ?

Description:

Set or show the SNMP authentication failure trap mode.

Syntax:

Security Switch SNMP Trap Authentication Failure [enable|disable]

Parameters:

enable Enable SNMP trap authentication failure
disable Disable SNMP trap authentication failure
(default: Show SNMP trap authentication failure mode)

8.1.7.12 Trap Link-up

Security/Switch/SNMP>Trap Link-up ?

Description:

Set or show the port link-up and link-down trap mode.

Syntax:

Security Switch SNMP Trap Link-up [enable|disable]

Parameters:

Enable Enable SNMP trap link-up and link-down
Disable Disable SNMP trap link-up and link-down
(default: Show SNMP trap link-up and link-down mode)

8.1.7.13 Trap Inform Mode

Security/Switch/SNMP>Trap Inform Mode ?

Description:

Set or show the SNMP trap inform mode.

Syntax:

Security Switch SNMP Trap Inform Mode [enable|disable]

Parameters:

Enable Enable SNMP trap inform

Disable Disable SNMP trap inform

(default: Show SNMP inform mode)

8.1.7.14 Trap Inform Timeout

Security/Switch/SNMP>Trap Inform Timeout ?

Description:

Set or show the SNMP trap inform timeout (usecs).

Syntax:

Security Switch SNMP Trap Inform Timeout [<timeout>]

Parameters:

<timeout> SNMP trap inform timeout (0-2147 seconds)

(default: Show SNMP trap inform timeout)

8.1.7.15 Trap Inform Retry Times

Security/Switch/SNMP>Trap inform Retry Times ?

Description:

Set or show the SNMP trap inform retry times.

Syntax:

Security Switch SNMP Trap Inform Retry Times [<retries>]

Parameters:

<retries> SNMP trap inform retransmited times (0-255)

(default: Show SNMP trap inform retry times)

8.1.7.16 Trap Probe Security Engine ID

Security/Switch/SNMP>Trap Probe Security Engine ID ?

Description:

Show SNMP trap security engine ID probe mode.

Syntax:

Security Switch SNMP Trap Probe Security Engine ID [enable|disable]

Parameters:

Enable Enable SNMP trap security engine ID probe

Disable Disable SNMP trap security engine ID probe

(default: Show SNMP trap security engine ID probe mode)

8.1.7.17 Trap Security Engine ID

Security/Switch/SNMP>Trap Security Engine ID ?

Description:

Set or show SNMP trap security engine ID.

Syntax:

Security Switch SNMP Trap Security Engine ID [<engineid>]

Parameters:

<engineid>: Engine ID, the format may not be all zeros or all 'ff'H
and is restricted to 5 - 32 octet string

8.1.7.18 Trap Security Name

Security/Switch/SNMP>Trap Security Name ?

Description:

Set or show SNMP trap security name.

Syntax:

Security Switch SNMP Trap Security Name [<security_name>]

Parameters:

<security_name> A string representing the security name for a principal
(default: Show SNMP trap security name).
The allowed string length is (1-32),
and the allowed content is ASCII characters from 33 to 126

8.1.7.19 Engine ID

Security/Switch/SNMP>Engine ID ?

Description:

Set or show SNMPv3 local engine ID.

Syntax:

Security Switch SNMP Engine ID [<engineid>]

Parameters:

<engineid>	Engine ID, the format may not be all zeros or all 'ff'H and is restricted to 5 - 32 octet string

8.1.7.20 Community Add

Security/Switch/SNMP>Community Add ?

Description:

Add or modify SNMPv3 community entry.
The entry index key is <community>.

Syntax:

Security Switch SNMP Community Add <community> [<ip_addr>] [<ip_mask>]

Parameters:

<community>	Community string
<ip_addr>	IP address (a.b.c.d), default: Show IP address
<ip_mask>	IPv4 subnet mask (a.b.c.d), default: Show IP mask

8.1.7.21 Community Delete

Security/Switch/SNMP>Community Delete ?

Description:

Delete SNMPv3 community entry.

Syntax:

Security Switch SNMP Community Delete <index>

Parameters:

<index> entry index (1-64)

8.1.7.22 Community Lookup

Security/Switch/SNMP>Community Lookup ?

Description:

Lookup SNMPv3 community entry.

Syntax:

Security Switch SNMP Community Lookup [<index>]

Parameters:

<index> entry index (1-64)

8.1.7.23 User Add

Security/Switch/SNMP>User Add ?

Description:

Add SNMPv3 user entry.

The entry index key are <engineid> and <user_name> and it doesn't allow modify.

Syntax:

Security Switch SNMP User Add <engineid> <user_name> [MD5|SHA]
[<auth_password>] [DES] [<priv_password>]

Parameters:

<engineid>	Engine ID, the format may not be all zeros or all 'ff'H and is restricted to 5 - 32 octet string
<user_name>	A string identifying the user name that this entry should belong to. The name of "None" is reserved. The allowed string length is (1-32), and the allowed content is ASCII characters from 33 to 126
md5	An optional flag to indicate that this user using MD5 authentication protocol. The allowed length is (8-32), and the allowed content is ASCII characters from 33 to 126
sha	An optional flag to indicate that this user using SHA authentication protocol. The allowed length is (8-40), and the allowed content is ASCII characters from 33 to 126
<auth_password>	A string identifying the authentication pass phrase
des	An optional flag to indicate that this user using DES privacy protocol privacy protocol should belong to. The allowed string length is (8-32), and the allowed content is ASCII characters from 33 to 126
<priv_password>	A string identifying the privacy pass phrase. The allowed string length is (8-40), and the allowed content is ASCII characters from 33 to 126

8.1.7.24 User Delete

Security/Switch/SNMP>User Delete ?

Description:

Delete SNMPv3 user entry.

Syntax:

Security Switch SNMP User Delete <index>

Parameters:

<index> entry index (1-64)

8.1.7.25 User Changekey

Security/Switch/SNMP>User Changekey ?

Description:

Change SNMPv3 user password.

Syntax:

Security Switch SNMP User Changekey <engineid> <user_name>
<auth_password> [<priv_password>]

Parameters:

<engineid>	Engine ID, the format may not be all zeros or all 'ff'H and is restricted to 5 - 32 octet string
<user_name>	A string identifying the user name that this entry should belong to. The name of "None" is reserved. The allowed string length is (1-32), and the allowed content is ASCII characters from 33 to 126

<auth_password> A string identifying the authentication pass phrase
<priv_password> A string identifying the privacy pass phrase.
The allowed string length is (8-40), and the allowed content is ASCII characters from 33 to 126

8.1.7.26 User Lookup

Security/Switch/SNMP>User Lookup ?

Description:

Lookup SNMPv3 user entry.

Syntax:

Security Switch SNMP User Lookup [<index>]

Parameters:

<index> entry index (1-64)

8.1.7.27 Group Add

Security/Switch/SNMP>Group Add ?

Description:

Add or modify SNMPv3 group entry.
The entry index key are <security_model> and <security_name>.

Syntax:

Security Switch SNMP Group Add <security_model> <security_name> <group_name>

Parameters:

<security_model> v1 - Reserved for SNMPv1
v2c - Reserved for SNMPv2c
usm - User-based Security Model (USM)
<security_name> A string identifying the security name that this entry should belong to. The allowed string length is (1-32), and the allowed content is ASCII characters from 33 to 126

<group_name> A string identifying the group name that this entry should belong to. The allowed string length is (1-32), and the allowed content is ASCII characters from 33 to 126

8.1.7.28 Group Delete

Security/Switch/SNMP>Group Delete ?

Description:

Delete SNMPv3 group entry.

Syntax:

Security Switch SNMP Group Delete <index>

Parameters:

<index> entry index (1-64)

8.1.7.29 Group Lookup

Security/Switch/SNMP>Group Lookup ?

Description:

Lookup SNMPv3 group entry.

Syntax:

Security Switch SNMP Group Lookup [<index>]

Parameters:

<index> entry index (1-64)

8.1.7.30 View Add

Security/Switch/SNMP>View Add ?

Description:

Add or modify SNMPv3 view entry.

The entry index key are <view_name> and <oid_subtree>.

Syntax:

Security Switch SNMP View Add <view_name> [included|excluded] <oid_subtree>

Parameters:

<view_name>	A string identifying the view name that this entry should belong to. The allowed string length is (1-32), and the allowed content is ASCII characters from 33 to 126
included	An optional flag to indicate that this view subtree should included
excluded	An optional flag to indicate that this view subtree should excluded
<oid_subtree>	The OID defining the root of the subtree to add to the named view

8.1.7.31 View Delete

Security/Switch/SNMP>View Delete ?

Description:

Delete SNMPv3 view entry.

Syntax:

Security Switch SNMP View Delete <index>

Parameters:

<index> entry index (1-64)

8.1.7.32 View Lookup

Security/Switch/SNMP>View Lookup ?

Description:

Lookup SNMPv3 view entry.

Syntax:

Security Switch SNMP View Lookup [<index>]

Parameters:

<index> entry index (1-64)

8.1.7.33 Access Add

Security/Switch/SNMP>Access Add ?

Description:

Add or modify SNMPv3 access entry.

The entry index key are <group_name>, <security_model> and <security_level>.

Syntax:

Security Switch SNMP Access Add <group_name> <security_model> <security_level>
[<read_view_name>] [<write_view_name>]

Parameters:

<group_name>	A string identifying the group name that this entry should belong to. The allowed string length is (1-32), and the allowed content is ASCII characters from 33 to 126
<security_model>	any - Accepted any security model (v1|v2c|usm) v1 - Reserved for SNMPv1 v2c - Reserved for SNMPv2c usm - User-based Security Model (USM)
<security_level>	noAuthNoPriv - None authentication and none privacy AuthNoPriv - Authentication and none privacy AuthPriv - Authentication and privacy
<read_view_name>	The name of the MIB view defining the MIB objects for which this request may request the current values. The name of "None" is reserved. The allowed string length is (1-32), and the allowed content is ASCII characters from 33 to 126
<write_view_name>	The name of the MIB view defining the MIB objects for which this request may potentially SET new values. The name of "None" is reserved. The allowed string length is (1-32), and the allowed content is ASCII characters from 33 to 126

8.1.7.34 Access Delete

Security/Switch/SNMP>Access Delete ?

Description:

Delete SNMPv3 access entry.

Syntax:

Security Switch SNMP Access Delete <index>

Parameters:

<index> entry index (1-64)

8.1.7.35 Access Lookup

Security/Switch/SNMP>Access Lookup ?

Description:

Lookup SNMPv3 access entry.

Syntax:

Security Switch SNMP Access Lookup [<index>]

Parameters:

<index> entry index (1-64)

8.1.8 Switch RMON

Available Commands:

Security Switch RMON Statistics Add <stats_id> <data_source>
Security Switch RMON Statistics Delete <stats_id>
Security Switch RMON Statistics Lookup [<stats_id>]
Security Switch RMON History Add <history_id> <data_source> [<interval>] [<buckets>]
Security Switch RMON History Delete <history_id>
Security Switch RMON History Lookup [<history_id>]
Security Switch RMON Alarm Add <alarm_id> <interval> <alarm_variable> [absolute|delta]
<rising_threshold> <rising_event_index> <falling_threshold>
<falling_event_index> [rising|falling|both]
Security Switch RMON Alarm Delete <alarm_id>
Security Switch RMON Alarm Lookup [<alarm_id>]
Security Switch RMON Event Add <event_id> [none|log|trap|log_trap] [<community>]
[<description>]
Security Switch RMON Event Delete <event_id>
Security Switch RMON Event Lookup [<event_id>]

8.1.8.1 Statistics Add

Security/Switch/RMON>Statistics Add ?

Description:

Add or modify RMON Statistics entry.

The entry index key is <stats_id>.

Syntax:

Security Switch RMON Statistics Add <stats_id> <data_source>

Parameters:

<stats_id> Statistics ID (1-65535).

<data_source> The OID that indicates that the ifIndex in ifEntry.

The value should be like .1.3.6.1.2.1.2.2.1.1.xxx.

8.1.8.2 Statistics Delete

Security/Switch/RMON>Statistics Delete ?

Description:

Delete RMON Statistics entry.

The entry index key is <stats_id>.

Syntax:

Security Switch RMON Statistics Delete <stats_id>

Parameters:

<stats_id> Statistics ID (1-65535).

8.1.8.3 Statistics Lookup

Security/Switch/RMON>Statistics Lookup ?

Description:

Show RMON Statistics entries.

Syntax:

Security Switch RMON Statistics Lookup [<stats_id>]

Parameters:

<stats_id> Statistics ID (1-65535).

8.1.8.4 History Add

Security/Switch/RMON>History Add ?

Description:

Add or modify RMON Hisotry entry.

The entry index key is <history_id>.

Syntax:

Security Switch RMON History Add <history_id> <data_source> [<interval>] [<buckets>]

Parameters:

<history_id> History ID (1-65535).

<data_source> The OID that indicates that the ifIndex in ifEntry.

The value should be like .1.3.6.1.2.1.2.2.1.1.xxx.

<interval> Sampling interval (1-3600) (default: 1800).

<buckets> The maximum data entries associated this History control entry stored in RMON(1-65535) (default: 50).

8.1.8.5 History Delete

Security/Switch/RMON>History Delete ?

Description:

Delete RMON Hisotry entry.

The entry index key is <history_id>.

Syntax:

Security Switch RMON History Delete <history_id>

Parameters:

<history_id>: History ID (1-65535).

8.1.8.6 History Lookup

Security/Switch/RMON>History Lookup ?

Description:

Show RMON History entries.

Syntax:

Security Switch RMON History Lookup [<history_id>]

Parameters:

<history_id> History ID (1-65535).

8.1.8.7 Alarm Add

Security/Switch/RMON>Alarm Add ?

Description:

Add or modify RMON Alarm entry.

The entry index key is <alarm_id>.

Syntax:

Security Switch RMON Alarm Add <alarm_id> <interval> <alarm_variable> [absolute|delta]
<rising_threshold> <rising_event_index> <falling_threshold>
<falling_event_index> [rising|falling|both]

Parameters:

<alarm_id> Alarm ID (1-65535).

<interval> Sampling interval (1-2147483647) (default: 30).

<alarm_variable> The MIB OID that need to be referenced.

.1.3.6.1.2.1.2.2.1.10.xxx – ifInOctets

.1.3.6.1.2.1.2.2.1.11.xxx – ifInUcastPkts

.1.3.6.1.2.1.2.2.1.12.xxx – ifInNUcastPkts

.1.3.6.1.2.1.2.2.1.13.xxx – ifInDiscards

.1.3.6.1.2.1.2.2.1.14.xxx – ifInErrors

.1.3.6.1.2.1.2.2.1.15.xxx – ifInUnkownProtos

.1.3.6.1.2.1.2.2.1.16.xxx – ifOutOctets

.1.3.6.1.2.1.2.2.1.17.xxx – ifOutUcastPkts

.1.3.6.1.2.1.2.2.1.18.xxx – ifOutNUcastPkts

.1.3.6.1.2.1.2.2.1.19.xxx – ifOutDiscards

.1.3.6.1.2.1.2.2.1.20.xxx – ifOutErrors

.1.3.6.1.2.1.2.2.1.21.xxx – ifOutQLen

"xxx" means the interface identified by a particular value of this index is the same interface as identified by the same value of OID 'ifIndex'.

absolute Get the sample directly.

delta Calculate the difference between samples (default).

<rising_threshold> Rising threshold value (-2147483648–2147483647).

<rising_event_index> Rising event index (1-65535).

<falling_threshold>	Falling threshold value (-2147483648–2147483647).
<falling_event_index>	Falling event index (1-65535).
rising	Trigger alarm when the first value is larger than the rising threshold.
falling	Trigger alarm when the first value is less than the falling threshold.
both	Trigger alarm when the first value is larger than the rising threshold or less than the falling threshold (default)

8.1.8.8 Alarm Delete

Security/Switch/RMON>Alarm Delete ?

Description:

Delete RMON Alarm entry.

The entry index key is <alarm_id>.

Syntax:

Security Switch RMON Alarm Delete <alarm_id>

Parameters:

<alarm_id>: Alarm ID (1-65535).

8.1.8.9 Alarm Lookup

Security/Switch/RMON>Alarm Lookup ?

Description:

Show RMON Alarm entries.

Syntax:

Security Switch RMON Alarm Lookup [<alarm_id>]

Parameters:

<alarm_id> Alarm ID (1-65535).

8.1.8.10 Event Add

Security/Switch/RMON>Event Add ?
Description:
Add or modify RMON Event entry.
The entry index key is <event_id>.

Syntax:

Security Switch RMON Event Add <event_id> [none|log|trap|log_trap] [<community>] [<description>]

Parameters:

<event_id>	Event ID (1-65535).
none	Get the sample directly.
log	Get the sample directly.
trap	Get the sample directly.
log_trap	Calculate the difference between samples (default).
<community>	Specify the community when trap is sent (the string length is 0~127) (default: public).
<description>	The string for describing this event (the string length is 0~127) (default: null string).

8.1.8.11 Event Delete

Security/Switch/RMON>Event Delete ?
Description:
Delete RMON Event entry.
The entry index key is <event_id>.

Syntax:

Security Switch RMON Event Delete <event_id>

Parameters:
<event_id>: Event ID (1-65535).

8.1.8.12 Event Lookup

Security/Switch/RMON>Event Lookup ?
Description:
Show RMON Event entries.

Syntax:

Security Switch RMON Event Lookup [<event_id>]

Parameters:
<event_id>: Event ID (1-65535).

8.2 NETWORK

Command Groups:

Security Network Psec : Port Security Status
Security Network Limit : Port Security Limit Control
Security Network NAS : Network Access Server (IEEE 802.1X)
Security Network ACL : Access Control List
Security Network DHCP : Dynamic Host Configuration Protocol
Security Network IP : IP Source Guard
Security Network ARP : Address Resolution Protocol

8.2.1 Network Psec

Available Commands:

Security Network Psec Switch [<port_list>]
Security Network Psec Port [<port_list>]

8.2.1.1 Switch

Security/Network/Psec>Switch ?
Description:
Show Port Security status.

Syntax:

Security Network Psec Switch [<port_list>]

Parameters:

<port_list> Port list or 'all', default: All ports

8.2.1.2 Port

Security/Network/Psec>Port ?

Description:

Show MAC Addresses learned by Port Security.

Syntax:

Security Network Psec Port [<port_list>]

Parameters:

<port_list> Port list or 'all', default: All ports

8.2.2 Network Limit

Available Commands:

Security Network Limit Configuration [<port_list>]
Security Network Limit Mode [enable|disable]
Security Network Limit Aging [enable|disable]
Security Network Limit Agetime [<age_time>]
Security Network Limit Port [<port_list>] [enable|disable]
Security Network Limit Limit [<port_list>] [<limit>]
Security Network Limit Action [<port_list>] [none|trap|shut|trap_shut]
Security Network Limit Reopen [<port_list>]

8.2.2.1 Configuration

Security/Network/Limit>configuration ?
Description:
Show Limit Control configuration.

Syntax:

Security Network Limit Configuration [<port_list>]

Parameters:
<port_list> Port list or 'all', default: All ports

8.2.2.2 Mode

Security/Network/Limit>Mode ?
Description:
Set or show global state.

Syntax:

Security Network Limit Mode [enable|disable]

Parameters:
enable Globally enable port security
disable Globally disable port security
(default: Show current global state of port security limit control)

8.2.2.3 Aging

Security/Network/Limit>Aging ?
Description:
Set or show aging state.

Syntax:

Security Network Limit Aging [enable|disable]

Parameters:
enable Enable aging
disable Disable aging
(default: Show current state of aging)

8.2.2.4 Agetime

Security/Network/Limit>agetime ?
Description:
Time in seconds between check for activity on learned MAC addresses.

Syntax:

Security Network Limit Agetime [<age_time>]

Parameters:
<age_time>: Time in seconds between checks for activity on a MAC address (10-10000000 seconds)
(default: Show current age time)

8.2.2.5 Port

Security/Network/Limit>Port ?

Description:

Set or show per-port state.

Syntax:

Security Network Limit Port [<port_list>] [enable|disable]

Parameters:

<port_list> Port list or 'all', default: All ports

enable Enable port security on this port

disable Disable port security on this port

(default: Show current port state of port security limit control)

8.2.2.6 Port

Security/Network/Limit>Limit ?

Description:

Set or show the max. number of MAC addresses that can be learned on this set of ports.

Syntax:

Security Network Limit Limit [<port_list>] [<limit>]

Parameters:

<port_list> Port list or 'all', default: All ports

<limit> Max. number of MAC addresses on this port

(default: Show current limit)

8.2.2.7 Action

Security/Network/Limit>Action ?

Description:

Set or show the action involved with exceeding the limit.

Syntax:

Security Network Limit Action [<port_list>] [none|trap|shut|trap_shut]

Parameters:

<port_list>	Port list or 'all', default: All ports
	none|trap|shut|trap_shut: Action to be taken in case the number of MAC addresses exceeds the limit
none	Don't do anything
trap	Send an SNMP trap
shut	Shutdown the port
trap_shut	Send an SNMP trap and shutdown the port

(default: Show current action)

8.2.2.8 Reopen

Security/Network/Limit>Reopen ?

Description:

Reopen one or more ports whose limit is exceeded and shut down.

Syntax:

Security Network Limit Reopen [<port_list>]

Parameters:

<port_list>	Port list or 'all', default: All ports

8.2.3 Network NAS

Available Commands:

Security Network NAS Configuration [<port_list>]
Security Network NAS Mode [enable|disable]
Security Network NAS State [<port_list>]
[auto|authorized|unauthorized|single|multi|macbased]
Security Network NAS Reauthentication [enable|disable]
Security Network NAS ReauthPeriod [<reauth_period>]
Security Network NAS EapolTimeout [<eapol_timeout>]
Security Network NAS Agetime [<age_time>]
Security Network NAS Holdtime [<hold_time>]
Security Network NAS RADIUS_QoS [global|<port_list>] [enable|disable]
Security Network NAS RADIUS_VLAN [global|<port_list>] [enable|disable]
Security Network NAS Guest_VLAN [global|<port_list>] [enable|disable] [<vid>]
[<reauth_max>] [<allow_if_eapol_seen>]
Security Network NAS Authenticate [<port_list>] [now]
Security Network NAS Statistics [<port_list>] [clear|eapol|radius]

8.2.3.1 Configuration

Security/Network/NAS>Configuration ?

Description:

Show 802.1X configuration.

Syntax:

Security Network NAS Configuration [<port_list>]

Parameters:

<port_list> Port list or 'all', default: All ports

8.2.3.2 Mode

Security/Network/NAS>Mode ?

Description:

Set or show the global NAS state.

Syntax:

Security Network NAS Mode [enable|disable]

Parameters:

enable Globally enable 802.1X

disable Globally disable 802.1X

(default: Show current 802.1X global state)

8.2.3.3 State

Security/Network/NAS>State ?

Description:

Set or show the port security state.

Syntax:

Security Network NAS State [<port_list>]
[auto|authorized|unauthorized|single|multi|macbased]

Parameters:

<port_list>	Port list or 'all', default: All ports
auto	Port-based 802.1X Authentication
authorized	Port access is allowed
unauthorized	Port access is not allowed
single	Single Host 802.1X Authentication
multi	Multiple Host 802.1X Authentication
macbased	Switch authenticates on behalf of the client

(default: Show 802.1X state)

8.2.3.4 Reauthentication

Security/Network/NAS>Reauthentication ?

Description:

Set or show Reauthentication state.

Syntax:

Security Network NAS Reauthentication [enable|disable]

Parameters:

enable	Enable reauthentication
disable	Disable reauthentication

(default: Show current reauthentication mode)

8.2.3.5 ReauthPeriod

Security/Network/NAS>ReauthPeriod ?

Description:

Set or show the period between reauthentication attempts.

Syntax:

Security Network NAS ReauthPeriod [<reauth_period>]

Parameters:

<reauth_period>	Period between reauthentication attempts (1-3600 seconds)

(default: Show current reauthentication period)

8.2.3.6 EapolTimeout

Security/Network/NAS>EapolTimeout ?

Description:

Set or show the time between EAPOL retransmissions.

Syntax:

Security Network NAS EapolTimeout [<eapol_timeout>]

Parameters:

<eapol_timeout>	Time between EAPOL retransmissions (1-65535 seconds)

(default: Show current EAPOL retransmission timeout)

8.2.3.7 Agetime

Security/Network/NAS>Agetime ?

Description:

Time in seconds between check for activity on successfully authenticated MAC addresses.

Syntax:

Security Network NAS Agetime [<age_time>]

Parameters:

<age_time> Time between checks (10-1000000 seconds)
(default: Show current age time)

8.2.3.8 Holdtime

Security/Network/NAS>Holdtime ?

Description:

Time in seconds before a MAC-address that failed authentication gets a new authentication chance.

Syntax:

Security Network NAS Holdtime [<hold_time>]

Parameters:

<hold_time> Time on hold (10-1000000 seconds)
(default: Show current hold time)

8.2.3.9 RADIUS_QoS

Security/Network/NAS>RADIUS_QoS ?

Description:

Set or show either global state (use the global keyword) or per-port state of RADIUS-assigned QoS.

Syntax:

Security Network NAS RADIUS_QoS [global|<port_list>] [enable|disable]

Parameters:

global	Select the global RADIUS-assigned QoS setting
<port_list>	Select the per-port RADIUS-assigned QoS setting

(default: Show current per-port RADIUS-assigned QoS state)

enable	Enable RADIUS-assigned QoS either globally or on one or more ports
disable	Disable RADIUS-assigned QoS either globally or on one or more ports

(default: Show current RADIUS-assigned QoS state)

8.2.3.10 RADIUS_VLAN

Security/Network/NAS>RADIUS_VLAN ?

Description:

Set or show either global state (use the global keyword) or per-port state of RADIUS-assigned VLAN.

Syntax:

Security Network NAS RADIUS_VLAN [global|<port_list>] [enable|disable]

Parameters:

global : Select the global RADIUS-assigned VLAN setting
<port_list>: Select the per-port RADIUS-assigned VLAN setting
(default: Show current per-port RADIUS-assigned VLAN state)
enable : Enable RADIUS-assigned VLAN either globally or on one or more ports
disable: Disable RADIUS-assigned VLAN either globally or on one or more ports
(default: Show current RADIUS-assigned VLAN state)

8.2.3.11 Guest_VLAN

Security/Network/NAS>Guest_VLAN ?

Description:

Set or show either global state and parameters (use the global keyword) or per-port state of Guest VLAN

Unless the 'global' keyword is used, the <reauth_max> and <allow_if_eapol_seen> parameters will not be unused..

Syntax:

Security Network NAS Guest_VLAN [global|<port_list>] [enable|disable] [<vid>] [<reauth_max>] [<allow_if_eapol_seen>]

Parameters:

global Select the global Guest VLAN setting

<port_list> Select the per-port Guest VLAN setting

(default: Show current per-port Guest VLAN state)

enable|disable enable : Enable Guest VLAN either globally or on one or more ports

disable: Disable Guest VLAN either globally or on one or more ports

(default: Show current Guest VLAN state)

<vid> Guest VLAN ID used when entering the Guest VLAN. Use the 'global' keyword to change it

(default: Show current Guest VLAN ID)

<reauth_max> The value can only be set if you use the 'global' keyword in the beginning of the command.

The number of times a Request Identity EAPOL frame is sent without response before considering entering the Guest VLAN

(default: Show current Maximum Reauth Count value

<allow_if_eapol_seen> The value can only be set if you use the 'global' keyword in the beginning of the command.

Disable The Guest VLAN can only be entered if no EAPOL frames have been received on a port for the lifetime of the port

enable The Guest VLAN can be entered even if an EAPOL frame has

been received during the lifetime of the port
(default: Show current setting)

8.2.3.12 Authenticate

Security/Network/NAS>Authenticate ?
Description:
Refresh (restart) 802.1X authentication process.

Syntax:

Security Network NAS Authenticate [<port_list>] [now]

Parameters:
<port_list> Port list or 'all', default: All ports
now Force reauthentication immediately
(default: Schedule a reauthentication)

8.2.3.13 Statistics

Security/Network/NAS>Statistics ?
Description:
Show or clear 802.1X statistics.

Syntax:

Security Network NAS Statistics [<port_list>] [clear|eapol|radius]

Parameters:
<port_list> Port list or 'all', default: All ports
clear Clear statistics
eapol Show EAPOL statistics
radius Show Backend Server statistics
(default: Show all statistics)

8.2.4 Network ACL

Available Commands:

Security Network ACL Configuration [<port_list>]
Security Network ACL Action [<port_list>] [permit|deny] [<rate_limiter>]
[<port_redirect>] [<mirror>] [<logging>] [<shutdown>]
Security Network ACL Policy [<port_list>] [<policy>]
Security Network ACL Rate [<rate_limiter_list>] [<rate_unit>] [<rate>]
Security Network ACL Add [<ace_id>] [<ace_id_next>]
[(port <port_list>)] [(policy <policy> <policy_bitmask>)]
[<tagged>] [<vid>] [<tag_prio>] [<dmac_type>]
[(etype [<etype>] [<smac>] [<dmac>]) |
(arp [<sip>] [<dip>] [<smac>] [<arp_opcode>] [<arp_flags>]) |
(ip [<sip>] [<dip>] [<protocol>] [<ip_flags>]) |
(icmp [<sip>] [<dip>] [<icmp_type>] [<icmp_code>] [<ip_flags>]) |
(udp [<sip>] [<dip>] [<sport>] [<dport>] [<ip_flags>]) |
(tcp [<sip>] [<dip>] [<sport>] [<dport>] [<ip_flags>] [<tcp_flags>])]
[permit|deny] [<rate_limiter>] [<port_redirect>] [<mirror>]
[<logging>] [<shutdown>]
Security Network ACL Delete <ace_id>
Security Network ACL Lookup [<ace_id>]
Security Network ACL Clear
Security Network ACL Status
[combined|static|loop_protect|dhcp|upnp|arp_inspection|ipmc|ip_source_guard|conflicts]
Security Network ACL Port State [<port_list>] [enable|disable]

8.2.4.1 Configuration

Security/Network/ACL>Configuration ?

Description:

Show ACL Configuration.

Syntax:

Security Network ACL Configuration [<port_list>]

Parameters:

<port_list>	Port list or 'all', default: All ports

8.2.4.2 Action

Security/Network/ACL>Action ?

Description:

Set or show the ACL port default action.

Syntax:

Security Network ACL Action [<port_list>] [permit|deny] [<rate_limiter>]
[<port_redirect>] [<mirror>] [<logging>] [<shutdown>]

Parameters:

<port_list>	Port list or 'all', default: All ports
permit	Permit forwarding (default)
deny	Deny forwarding
<rate_limiter>	Rate limiter number (1-15) or 'disable'
<port_redirect>	Port list for copy of frames or 'disable'
<mirror>	Mirror of frames: enable|disable

<logging> System logging of frames: log|log_disable
<shutdown> Shut down ingress port: shut|shut_disable

8.2.4.3 Policy

Security/Network/ACL>Policy ?
Description:
Set or show the ACL port policy.

Syntax:

Security Network ACL Policy [<port_list>] [<policy>]

Parameters:
<port_list> Port list or 'all', default: All ports
<policy> Policy number (0-255)

8.2.4.4 Rate

Security/Network/ACL>Rate ?
Description:
Set or show the ACL rate limiter.

Syntax:

Security Network ACL Rate [<rate_limiter_list>] [<rate_unit>] [<rate>]

Parameters:
<rate_limiter_list>: Rate limiter list (1-16), default: All rate limiters
<rate_unit> : IP flags: pps|kbps, default: pss
<rate> : Rate in pps (0-100) or kbps (0, 100, 2*100, 3*100, ..., 1000000)

8.2.4.5 Add

Security/Network/ACL>Add ?

Description:

Add or modify Access Control Entry (ACE).

If the ACE ID parameter <ace_id> is specified and an entry with this ACE ID already exists, the ACE will be modified. Otherwise, a new ACE will be added. If the ACE ID is not specified, the next available ACE ID will be used.

If the next ACE ID parameter <ace_id_next> is specified, the ACE will be placed before this ACE in the list. If the next ACE ID is not specified, the ACE will be placed last in the list.

If the Switch keyword is used, the rule applies to all ports.
If the Port keyword is used, the rule applies to the specified port only.
If the Policy keyword is used, the rule applies to all ports configured with the specified policy. The default is that the rule applies to all ports.

Syntax:

Security Network ACL Add [<ace_id>] [<ace_id_next>]
[(port <port_list>)] [(policy <policy> <policy_bitmask>)]
[<tagged>] [<vid>] [<tag_prio>] [<dmac_type>]
[(etype [<etype>] [<smac>] [<dmac>]) |
(arp [<sip>] [<dip>] [<smac>] [<arp_opcode>] [<arp_flags>]) |
(ip [<sip>] [<dip>] [<protocol>] [<ip_flags>]) |
(icmp [<sip>] [<dip>] [<icmp_type>] [<icmp_code>] [<ip_flags>]) |
(udp [<sip>] [<dip>] [<sport>] [<dport>] [<ip_flags>]) |
(tcp [<sip>] [<dip>] [<sport>] [<dport>] [<ip_flags>] [<tcp_flags>])]
[permit|deny] [<rate_limiter>] [<port_redirect>] [<mirror>] [<logging>]
[<shutdown>]

Parameters:

<ace_id>	ACE ID (1-256), default: Next available ID
<ace_id_next>	Next ACE ID (1-256), default: Add ACE last
port	Port ACE keyword
<port_list>	Port list or 'all', default: All ports
policy	Policy ACE keyword
<policy>	Policy number (0-255)
<policy_bitmask>	Policy number bitmask (0x0-0xFF)
<tagged>	Tagged of frames: any|enable|disable
<vid>	VLAN ID (1-4095) or 'any'
<tag_prio>	VLAN tag priority (0-7) or 'any'
<dmac_type>	DMAC type: any|unicast|multicast|broadcast
etype	Ethernet Type keyword
<etype>	Ethernet Type: 0x600 - 0xFFFF or 'any' but excluding 0x800(IPv4) 0x806(ARP) and 0x86DD(IPv6)
<smac>	Source MAC address ('xx-xx-xx-xx-xx-xx' or 'xx.xx.xx.xx.xx.xx' or 'xxxxxxxxxxxx', x is a hexadecimal digit) or 'any'
<dmac>	Destination MAC address ('xx-xx-xx-xx-xx-xx' or 'xx.xx.xx.xx.xx.xx' or 'xxxxxxxxxxxx', x is a hexadecimal digit) or 'any'
arp	ARP keyword
<sip>	Source IP address (a.b.c.d/n) or 'any'
<dip>	Destination IP address (a.b.c.d/n) or 'any'
<arp_opcode>	ARP operation code: any|arp|rarp|other
<arp_flags>	ARP flags: request|smac|tmac|len|ip|ether [0|1|any]
ip	IP keyword
<protocol>	IP protocol number (0-255) or 'any'
<ip_flags>	IP flags: ttl|options|fragment [0|1|any]
icmp	ICMP keyword
<icmp_type>	ICMP type number (0-255) or 'any'
<icmp_code>	ICMP code number (0-255) or 'any'
udp	UDP keyword
<sport>	Source UDP/TCP port range (0-65535) or 'any'
<dport>	Destination UDP/TCP port range (0-65535) or 'any'
tcp	TCP keyword
<tcp_flags>	TCP flags: fin|syn|rst|psh|ack|urg [0|1|any]
permit	Permit forwarding (default)

deny	Deny forwarding
<rate_limiter>	Rate limiter number (1-15) or 'disable'
<port_redirect>	Port list for copy of frames or 'disable'
<mirror>	Mirror of frames: enable|disable
<logging>	System logging of frames: log|log_disable
<shutdown>	Shut down ingress port: shut|shut_disable

8.2.4.6 Delete

Security/Network/ACL>Delete ?

Description:

Delete ACE.

Syntax:

Security Network ACL Delete <ace_id>

Parameters:

<ace_id>: ACE ID (1-256)

8.2.4.7 Lookup

Security/Network/ACL>Lookup ?

Description:

Show ACE, default: All ACEs.

Syntax:

Security Network ACL Lookup [<ace_id>]

Parameters:

<ace_id>	ACE ID (1-256)

8.2.4.8 Clear

Security/Network/ACL>Clear ?

Description:

Clear all ACL counters.

Syntax:

Security Network ACL Clear

8.2.4.9 Status

Security/Network/ACL>Status ?

Description:

Show ACL status.

Syntax:

Security Network ACL Status
[combined|static|loop_protect|dhcp|upnp|arp_inspection|ipmc|ip_source_guard|conflicts]

Parameters:

combined	Show combined status
static	Show static user configured status
loop_protect	Shows the status by Loop Protect
dhcp	Show DHCP status
upnp	Show UPnP status
arp_inspection	Show ARP Inspection status
ipmc	Show IPMC status

ip_source_guard Show IP Source Guard status
conflicts Show conflict status
(default : Show combined status)

8.2.4.10 Port State

Security/Network/ACL>Port State ?

Description:

Set or show the ACL port state.

Syntax:

Security Network ACL Port State [<port_list>] [enable|disable]

Parameters:

<port_list> Port list or 'all', default: All ports
enable|disable: ACL port state

8.2.5 Network ACL

Available Commands:

Security Network DHCP Relay Configuration
Security Network DHCP Relay Mode [enable|disable]
Security Network DHCP Relay Server [<ip_addr>]
Security Network DHCP Relay Information Mode [enable|disable]
Security Network DHCP Relay Information Policy [replace|keep|drop]
Security Network DHCP Relay Statistics [clear]
Security Network DHCP Snooping Configuration
Security Network DHCP Snooping Mode [enable|disable]
Security Network DHCP Snooping Port Mode [<port_list>] [trusted|untrusted]
Security Network DHCP Snooping Statistics [<port_list>] [clear]

8.2.5.1 Relay Configuration

Security/Network/DHCP>Relay Configuration ?

Description:

Show DHCP relay configuration.

Syntax:

Security Network DHCP Relay Configuration

8.2.5.2 Relay Mode

Security/Network/DHCP>Relay Mode ?

Description:

Set or show the DHCP relay mode.

Syntax:

Security Network DHCP Relay Mode [enable|disable]

Parameters:

enable	Enable DHCP relaly mode. When enable DHCP relay mode operation, the agent forward and to transfer DHCP messages between the clients and the server when they are not on the same subnet domain. And the DHCP broadcast message won't flood for security considered.
Disable	Disable DHCP relaly mode

(default: Show flow DHCP relaly mode)

8.2.5.3 Relay Server

Security/Network/DHCP>Relay Server ?

Description:

Show or set DHCP relay server.

Syntax:

Security Network DHCP Relay Server [<ip_addr>]

Parameters:

<ip_addr>	IP address (a.b.c.d), default: Show IP address

8.2.5.4 Relay Information Mode

Security/Network/DHCP>Relay Information Mode ?

Description:

Set or show DHCP relay agent information option mode.
When enable DHCP relay information mode operation, the agent insert specific information (option 82) into a DHCP message when forwarding to DHCP server and remote it from a DHCP message when transferring to DHCP client. It only works under DHCP relay operation mode enabled.

Syntax:

Security Network DHCP Relay Information Mode [enable|disable]

Parameters:

Enable	Enable DHCP relay agent information option mode
Disable	Disable DHCP relay agent information option mode

(default: Show DHCP relay agent information option mode)

8.2.5.5 Relay Information Policy

Security/Network/DHCP>Relay Information Policy ?

Description:

Set or show the DHCP relay mode.
When enable DHCP relay information mode operation, if agent receive a DHCP message that already contains relay agent information. It will enforce the policy.

Syntax:

Security Network DHCP Relay Information Policy [replace|keep|drop]

Parameters:

replace	Replace the original relay information when receive a DHCP message that already contains it
keep	Keep the original relay information when receive a DHCP message that already contains it
drop	Drop the package when receive a DHCP message that already contains relay information

(default: Show DHCP relay information policy)

8.2.5.6 Relay Statistics

Security/Network/DHCP>Relay Statistics ?

Description:

Show or clear DHCP relay statistics.

Syntax:

Security Network DHCP Relay Statistics [clear]

Parameters:

clear Clear DHCP relay statistics

8.2.5.7 Snooping Configuration

Security/Network/DHCP>Snooping Configuration ?

Description:

Show DHCP snooping configuration.

Syntax:

Security Network DHCP Snooping Configuration

8.2.5.8 Snooping Mode

Security/Network/DHCP>Snooping Mode ?

Description:

Set or show the DHCP snooping mode.

Syntax:

Security Network DHCP Snooping Mode [enable|disable]

Parameters:

Enable Enable DHCP snooping mode.
When enable DHCP snooping mode operation, the request DHCP messages will be forwarded to trusted ports and only allowed reply packets from trusted ports.

Disable Disable DHCP snooping mode

(default: Show flow DHCP snooping mode)

8.2.5.9 Snooping Port Mode

Security/Network/DHCP>Snooping Port Mode ?

Description:

Set or show the DHCP snooping port mode.

Syntax:

Security Network DHCP Snooping Port Mode [<port_list>] [trusted|untrusted]

Parameters:

<port_list>	Port list or 'all', default: All ports
Trusted	Configures the port as trusted sources of the DHCP message
untrusted	Configures the port as untrusted sources of the DHCP message

(default: Show flow DHCP snooping port mode)

8.2.5.10 Snooping Statistics

Security/Network/DHCP>Snooping Statistics ?

Description:

Show or clear DHCP snooping statistics.

The statistics doesn't count the DHCP packets for system DHCP client or DHCP relay mode is enabled.

Syntax:

Security Network DHCP Snooping Statistics [<port_list>] [clear]

Parameters:

<port_list>	Port list or 'all', default: All ports
clear	Clear DHCP snooping statistics

8.2.6 Network IP

Available Commands:

Security Network IP Source Guard Configuration
Security Network IP Source Guard Mode [enable|disable]
Security Network IP Source Guard Port Mode [<port_list>] [enable|disable]
Security Network IP Source Guard limit [<port_list>]
[<dynamic_entry_limit>|unlimited]
Security Network IP Source Guard Entry [<port_list>] add|delete
<vid> <allowed_ip> <allowed_mac>
Security Network IP Source Guard Status [<port_list>]
Security Network IP Source Guard Translation

8.2.6.1 Source Guard Configuration

Security/Network/IP>Source Guard Configuration ?

Description:

Show IP source guard configuration.

Syntax:

Security Network IP Source Guard Configuration

8.2.6.2 Source Guard Mode

Security/Network/IP>Source Guard Mode ?

Description:

Set or show IP source guard mode.

Syntax:

Security Network IP Source Guard Mode [enable|disable]

Parameters:

Enable	Enable IP Source Guard
disable	Disable IP Source Guard

8.2.6.3 Source Guard Port Mode

Security/Network/IP>Source Guard Port Mode ?

Description:

Set or show the IP Source Guard port mode.

Syntax:

Security Network IP Source Guard Port Mode [<port_list>] [enable|disable]

Parameters:

<port_list>	Port list or 'all', default: All ports
enable	Enable IP Source Guard port
disable	Disable IP Source Guard port

(default: Show IP Source Guard port mode)

8.2.6.4 Source Guard Limit

Security/Network/IP>Source Guard Limit ?

Description:

Set or show the IP Source Guard port limitation for dynamic entries.

Syntax:

Security Network IP Source Guard limit [<port_list>]
[<dynamic_entry_limit>|unlimited]

Parameters:

<port_list>	Port list or 'all', default: All ports
<dynamic_entry_limit>|unlimited	dynamic entry limit (0-2) or unlimited

8.2.6.5 Source Guard Entry

Security/Network/IP>Source Guard Entry ?

Description:

Add or delete IP source guard static entry.

Syntax:

Security Network IP Source Guard Entry [<port_list>] add|delete
<vid> <allowed_ip> <allowed_mac>

Parameters:

<port_list>	Port list or 'all', default: All ports
add	Add new port IP source guard static entry
delete	Delete existing port IP source guard static entry
<vid>	VLAN ID (1-4095)

<allowed_ip> IPv4 address (a.b.c.d), IP address allowed for doing IP source guard
<allowed_mac> MAC address ('xx-xx-xx-xx-xx-xx' or 'xx.xx.xx.xx.xx.xx' or 'xxxxxxxxxxxx', x is a hexadecimal digit), MAC address allowed for doing IP source guard

8.2.6.6 Source Guard Status

Security/Network/IP>Source Guard Status ?

Description:

Show IP source guard static and dynamic entries.

Syntax:

Security Network IP Source Guard Status [<port_list>]

Parameters:

<port_list> Port list or 'all', default: All ports

8.2.6.7 Source Translation

Security/Network/IP>Source Guard Translation ?

Description:

Translate IP source guard dynamic entries into static entries.

Syntax:

Security Network IP Source Guard Translation

8.2.7 Network ARP

Available Commands:

Security Network ARP Inspection Configuration
Security Network ARP Inspection Mode [enable|disable]
Security Network ARP Inspection Port Mode [<port_list>] [enable|disable]
Security Network ARP Inspection Entry [<port_list>] add|delete
<vid> <allowed_mac> <allowed_ip>
Security Network ARP Inspection Status [<port_list>]
Security Network ARP Inspection Translation

8.2.7.1 Inspection Configuration

Security/Network/ARP>Inspection Configuration ?

Description:

Show ARP inspection configuration.

Syntax:

8.2.7.2 Inspection Mode

Security/Network/ARP>Inspection Mode ?

Description:

Set or show ARP inspection mode.

Syntax:

Security Network ARP Inspection Mode [enable|disable]

Parameters:

enable	Enable ARP Inspection
disable	Disable ARP Inspection

8.2.7.3 Inspection Port Mode

Security/Network/ARP>Inspection Port Mode ?

Description:

Set or show the ARP Inspection port mode.

Syntax:

Security Network ARP Inspection Port Mode [<port_list>] [enable|disable]

Parameters:

<port_list>	Port list or 'all', default: All ports
enable	Enable ARP Inspection port
disable	Disable ARP Inspection port

(default: Show ARP Inspection port mode)

8.2.7.4 Inspection Entry

Security/Network/ARP>Inspection Entry ?

Description:

Add or delete ARP inspection static entry.

Syntax:

Security Network ARP Inspection Entry [<port_list>] add|delete
<vid> <allowed_mac> <allowed_ip>

Parameters:

<port_list>	Port list or 'all', default: All ports
add	Add new port ARP inspection static entry
delete	Delete existing port ARP inspection static entry
<vid>	VLAN ID (1-4095)
<allowed_mac>	MAC address ('xx-xx-xx-xx-xx-xx' or 'xx.xx.xx.xx.xx.xx' or 'xxxxxxxxxxxx', x is a hexadecimal digit), MAC address allowed for doing ARP request
<allowed_ip>	IPv4 address (a.b.c.d), IP address allowed for doing ARP request

8.2.7.5 Inspection Status

Security/Network/ARP>Inspection Status ?

Description:

Show ARP inspection static and dynamic entries.

Syntax:

Security Network ARP Inspection Status [<port_list>]

Parameters:
<port_list>: Port list or 'all', default: All ports

8.2.7.6 Inspection Translation

Security/Network/ARP>Inspection Translation ?
Description:
Translate ARP inspection dynamic entries into static entries.

Syntax:

Security Network ARP Inspection Translation

8.3 AAA

Available Commands:

Security AAA Configuration
Security AAA Timeout [<timeout>]
Security AAA Deadtime [<dead_time>]
Security AAA RADIUS [<server_index>] [enable|disable] [<ip_addr_string>] [<secret>] [<server_port>]
Security AAA ACCT_RADIUS [<server_index>] [enable|disable] [<ip_addr_string>] [<secret>] [<server_port>]

Security AAA TACACS+ [<server_index>] [enable|disable] [<ip_addr_string>] [<secret>] [<server_port>]
Security AAA Statistics [<server_index>]

8.3.1 Configuration

Security/AAA>Configuration ?
Description:
Show Auth configuration.

Syntax:

Security AAA Configuration

8.3.2 Timeout

Security/AAA>Timeout ?
Description:
Set or show server timeout.

Syntax:

Security AAA Timeout [<timeout>]

Parameters:
<timeout> Server response timeout (3-3600 seconds)
(default: Show server timeout configuration)

8.3.3 Deadtime

Security/AAA>Deadtime ?

Description:

Set or show server dead time.

Syntax:

Security AAA Deadtime [<dead_time>]

Parameters:

<dead_time> Time that a server is considered dead if it doesn't answer a request (0-3600 seconds)

(default: Show server dead time configuration)

8.3.4 RADIUS

Security/AAA>RADIUS ?

Description:

Set or show RADIUS authentication server setup.

Syntax:

Security AAA RADIUS [<server_index>] [enable|disable] [<ip_addr_string>] [<secret>] [<server_port>]

Parameters:

The server index (1-5)

(default: Show RADIUS authentication server configuration)

enable Enable RADIUS authentication server

disable Disable RADIUS authentication server

(default: Show RADIUS server mode)

<ip_addr_string> IP host address (a.b.c.d) or a host name string

<secret>	Secret shared with external authentication server. To use spaces in secret, enquote the secret. Quotes in the secret are not allowed.
<server_port>	Server UDP port. Use 0 to use the default RADIUS port (1812)

8.3.5 ACCT_RADIUS

Security/AAA>ACCT_RADIUS ?

Description:

Set or show RADIUS accounting server setup.

Syntax:

Security AAA ACCT_RADIUS [<server_index>] [enable|disable] [<ip_addr_string>] [<secret>] [<server_port>]

Parameters:

The server index (1-5)

(default: Show RADIUS accounting server configuration)

enable	Enable RADIUS accounting server
disable	Disable RADIUS accounting server

(default: Show RADIUS server mode)

<ip_addr_string>	IP host address (a.b.c.d) or a host name string
<secret>	Secret shared with external accounting server. To use spaces in secret, enquote the secret. Quotes in the secret are not allowed.
<server_port>	Server UDP port. Use 0 to use the default RADIUS port (1813)

8.3.6 TACACS+

Security/AAA>TACACS+ ?

Description:

Set or show TACACS+ authentication server setup.

Syntax:

Security AAA TACACS+ [<server_index>] [enable|disable] [<ip_addr_string>] [<secret>] [<server_port>]

Parameters:

The server index (1-5)

(default: Show TACACS+ authentication server configuration)

enable	Enable TACACS+ authentication server
disable	Disable TACACS+ authentication server

(default: Show TACACS+ server mode)

<ip_addr_string>	IP host address (a.b.c.d) or a host name string
<secret>	Secret shared with external authentication server. To use spaces in secret, enquote the secret. Quotes in the secret are not allowed.
<server_port>	Server TCP port. Use 0 to use the default TACACS+ port (49)

8.3.7 Statistics

Security/AAA>Statistics ?

Description:

Show RADIUS statistics.

Syntax:

Security AAA Statistics [<server_index>]

Parameters:
The server index (1-5)
(default: Show statistics for all servers)

Chapter 9 STP

9.STP

Available Commands:

STP Configuration
STP Version [<stp_version>]
STP Txhold [<holdcount>]
STP MaxHops [<maxhops>]
STP MaxAge [<max_age>]
STP FwdDelay [<delay>]
STP CName [<config-name>] [<integer>]
STP bpduFilter [enable|disable]
STP bpduGuard [enable|disable]
STP recovery [<timeout>]
STP Status [<msti>] [<stp_port_list>]
STP Msti Priority [<msti>] [<priority>]
STP Msti Map [<msti>] [clear]
STP Msti Add <msti> <vid-range>
STP Port Configuration [<stp_port_list>]
STP Port Mode [<stp_port_list>] [enable|disable]
STP Port Edge [<stp_port_list>] [enable|disable]
STP Port AutoEdge [<stp_port_list>] [enable|disable]
STP Port P2P [<stp_port_list>] [enable|disable|auto]
STP Port RestrictedRole [<stp_port_list>] [enable|disable]

STP Port RestrictedTcn [<stp_port_list>] [enable|disable]
STP Port bpduGuard [<stp_port_list>] [enable|disable]
STP Port Statistics [<stp_port_list>] [clear]
STP Port Mcheck [<stp_port_list>]
STP Msti Port Configuration [<msti>] [<stp_port_list>]
STP Msti Port Cost [<msti>] [<stp_port_list>] [<path_cost>]
STP Msti Port Priority [<msti>] [<stp_port_list>] [<priority>]

9.1 Configuration

STP>Configuration ?
Description:
Show STP Bridge configuration.

Syntax:

STP Configuration

9.2 Version

STP>Version ?
Description:
Set or show the STP Bridge protocol version.

Syntax:

STP Version [<stp_version>]

Parameters:
<stp_version> mstp|rstp|stp

9.3 Txhold

STP>Txhold ?

Description:
Set or show the STP Bridge Transmit Hold Count parameter.

Syntax:

STP Txhold [<holdcount>]

Parameters:
<holdcount>: STP Transmit Hold Count (1-10)

9.4 MaxHops

STP>MaxHops ?
Description:
Set or show the MSTP Bridge Max Hop Count parameter.

Syntax:

STP MaxHops [<maxhops>]

Parameters:
<maxhops> STP BPDU MaxHops (6-40))

9.5 MaxAge

STP>MaxAge ?
Description:
Set or show the bridge instance maximum age.

Syntax:

STP MaxAge [<max_age>]

Parameters:

<max_age>: STP maximum age time (6-40, and max_age <= (forward_delay-1)*2)

9.6 FwdDelay

STP>FwdDelay ?

Description:

Set or show the bridge instance forward delay.

Syntax:

STP FwdDelay [<delay>]

Parameters:

<delay>	MSTP forward delay (4-30, and max_age <= (forward_delay-1)*2))

9.7 CName

STP>CName ?

Description:

Set or Show MSTP configuration name and revision.

Syntax:

STP CName [<config-name>] [<integer>]

Parameters:

<config-name>	MSTP Configuration name. A text string up to 32 characters long. Use quotes (") to embed spaces in name.
<integer>	Integer value

9.8 bpduFilter

STP>bpduFilter ?

Description:

Set or show edge port BPDU Filtering.

Syntax:

STP bpduFilter [enable|disable]

Parameters:

enable|disable	enable or disable BPDU Filtering for Edge ports

9.9 bpduGuard

STP>bpduGuard ?

Description:

Set or show edge port BPDU Guard.

Syntax:

STP bpduGuard [enable|disable]

Parameters:

enable|disable	enable or disable BPDU Guard for Edge ports

9.10 recovery

STP>recovery ?

Description:

Set or show edge port error recovery timeout.

Syntax:

STP recovery [<timeout>]

Parameters:

<timeout>: Time before error-disabled ports are reenabled (30-86400 seconds, 0 disables) (default: Show recovery timeout)

9.11 Status

STP>Status ?

Description:

Show STP Bridge status.

Syntax:

STP Status [<msti>] [<stp_port_list>]

Parameters:

<msti>	STP bridge instance no (0-7, CIST=0, MSTI1=1, ...)
<stp_port_list>	Port list or 'all'. Port zero means aggregations.

9.12 Msti Priority

STP>Msti Priority ?

Description:

Set or show the bridge instance priority.

Syntax:

STP Msti Priority [<msti>] [<priority>]

Parameters:

<msti>	STP bridge instance no (0-7, CIST=0, MSTI1=1, ...)
<priority>	STP bridge priority (0/4096/8192/12288/.../53248/57344/61440)

9.13 Msti Map

STP>MSti Map ?

Description:

Show or clear MSTP MSTI VLAN mapping configuration.

Syntax:

STP Msti Map [<msti>] [clear]

Parameters:

<msti>	STP bridge instance no (0-7, CIST=0, MSTI1=1, ...)
clear	Clear VID to MSTI mapping

9.14 Msti Add

STP>Msti Add ?

Description:

Add a VLAN (single or range) to a MSTI.

Syntax:

STP Msti Add <msti> <vid-range>

Parameters:

<msti>	STP bridge instance no (0-7, CIST=0, MSTI1=1, ...)
<vid-range>	Single VLAN ID (1-4094) or 'xx-yy' VLAN ID range

9.15 Port Configuration

STP>Port Configuration ?

Description:

Show STP Port configuration.

Syntax:

STP Port Configuration [<stp_port_list>]

Parameters:

<stp_port_list>	Port list or 'all'. Port zero means aggregations.

9.16 Port Mode

STP>Port Mode ?

Description:

Set or show the STP enabling for a port.

Syntax:

STP Port Mode [<stp_port_list>] [enable|disable]

Parameters:

<stp_port_list>	Port list or 'all'. Port zero means aggregations.
enable	Enable MSTP protocol
disable	Disable MSTP protocol

9.17 Port Edge

STP>Port Edge ?

Description:

Set or show the STP adminEdge port parameter.

Syntax:

STP Port Edge [<stp_port_list>] [enable|disable]

Parameters:

<stp_port_list>	Port list or 'all'. Port zero means aggregations.
enable	Configure MSTP adminEdge to Edge
disable	Configure MSTP adminEdge to Non-edge

9.18 Port AutoEdge

STP>Port AutoEdge ?

Description:

Set or show the STP autoEdge port parameter.

Syntax:

STP Port AutoEdge [<stp_port_list>] [enable|disable]

Parameters:

<stp_port_list>	Port list or 'all'. Port zero means aggregations.
enable	Enable MSTP autoEdge
disable	Disable MSTP autoEdge

9.19 Port P2P

STP>Port P2P ?

Description:

Set or show the STP point2point port parameter.

Syntax:

STP Port P2P [<stp_port_list>] [enable|disable|auto]

Parameters:

<stp_port_list>	Port list or 'all'. Port zero means aggregations.
enable	Enable MSTP point2point
disable	Disable MSTP point2point
auto	Automatic MSTP point2point detection

9.20 Port RestrictedRole

STP>Port RestrictedRole ?

Description:

Set or show the MSTP restrictedRole port parameter.

Syntax:

STP Port RestrictedRole [<stp_port_list>] [enable|disable]

Parameters:

<stp_port_list>	Port list or 'all'. Port zero means aggregations.
enable	Enable MSTP restricted role
disable	Disable MSTP restricted role

9.21 Port RestrictedTcn

STP>Port RestrictedTcn ?

Description:

Set or show the MSTP restrictedTcn port parameter.

Syntax:

STP Port RestrictedTcn [<stp_port_list>] [enable|disable]

Parameters:

<stp_port_list>	Port list or 'all'. Port zero means aggregations.
enable	Enable MSTP restricted TCN
disable	Disable MSTP restricted TCN

9.22 bpduGuard

STP>bpduGuard ?
Description:
Set or show edge port BPDU Guard.

Syntax:

STP bpduGuard [enable|disable]

Parameters:

enable|disable	enable or disable BPDU Guard for Edge ports

9.23 Port Statistics

STP>Port Statistics ?
Description:
Show STP port statistics.

Syntax:

STP Port Statistics [<stp_port_list>] [clear]

Parameters:

<stp_port_list>	Port list or 'all'. Port zero means aggregations.
clear	Clear the selected port statistics

9.24 Port Mcheck

STP>Port Mcheck ?

Description:

Set the STP mCheck (Migration Check) variable for ports.

Syntax:

STP Port Mcheck [<stp_port_list>]

Parameters:

<stp_port_list>: Port list or 'all'. Port zero means aggregations.

9.25 Msti Port Configuration

STP>Msti Port Configuration ?

Description:

Show the STP port instance configuration.

Syntax:

STP Msti Port Configuration [<msti>] [<stp_port_list>]

Parameters:

<msti>	STP bridge instance no (0-7, CIST=0, MSTI1=1, ...)
<stp_port_list>	Port list or 'all'. Port zero means aggregations.

9.26 Msti Port Cost

STP>Msti Port Cost ?

Description:

Set or show the STP port instance path cost.

Syntax:

STP Msti Port Cost [<msti>] [<stp_port_list>] [<path_cost>]

Parameters:

<msti>	STP bridge instance no (0-7, CIST=0, MSTI1=1, ...)
<stp_port_list>	Port list or 'all'. Port zero means aggregations.
<path_cost>	STP port path cost (1-200000000) or 'auto'

9.27 Msti Port Priority

STP>Msti Port Priority ?

Description:

Set or show the STP port instance priority.

Syntax:

STP Msti Port Priority [<msti>] [<stp_port_list>] [<priority>]

Parameters:

<msti>	STP bridge instance no (0-7, CIST=0, MSTI1=1, ...)
<stp_port_list>	Port list or 'all'. Port zero means aggregations.
<priority>	STP port priority (0/16/32/48/.../224/240)

Chapter 10 AGGREGATION

10.AGGREGATION

Available Commands:

Aggr Configuration
Aggr Add <port_list> [<aggr_id>]
Aggr Delete <aggr_id>
Aggr Lookup [<aggr_id>]
Aggr Mode [smac|dmac|ip|port] [enable|disable]

10.1 Configuration

Aggr>Configuration ?
Description:
Show link aggregation configuration.

Syntax:

Aggr Configuration

10.2 Add

Aggr>Add ?
Description:
Add or modify link aggregation.

Syntax:

Aggr Add <port_list> [<aggr_id>]

Parameters:

<port_list>	Port list or 'all', default: All ports
<aggr_id>	Aggregation ID: 1-5

10.3 Delete

Aggr>Delete ?

Description:

Delete link aggregation.

Syntax:

Aggr Delete <aggr_id>

Parameters:

<aggr_id>: Aggregation ID: 1-5

10.4 Lookup

Aggr>Lookup ?

Description:

Lookup link aggregation.

Syntax:

Aggr Lookup [<aggr_id>]

Parameters:

<aggr_id>: Aggregation ID: 1-5

10.5 Mode

Aggr>Mode ?

Description:

Set or show the link aggregation traffic distribution mode.

Syntax:

Aggr Mode [smac|dmac|ip|port] [enable|disable]

Parameters:

smac	Source MAC address
dmac	Destination MAC address
ip	Source and destination IP address
port	Source and destination UDP/TCP port
enable	Enable field in traffic distribution
disable	Disable field in traffic distribution

Chapter 11 LACP

11.LACP

Available Commands:

LACP Configuration [<port_list>]
LACP Mode [<port_list>] [enable|disable]
LACP Key [<port_list>] [<key>]
LACP Prio [<port_list>] [<prio>]
LACP System Prio [<sysprio>]
LACP Role [<port_list>] [active|passive]
LACP Status [<port_list>]
LACP Statistics [<port_list>] [clear]
LACP Timeout [<port_list>] [fast|slow]

11.1 Configuration

LACP>Configuration ?
Description:
Show LACP configuration.

Syntax:

LACP Configuration [<port_list>]

Parameters:
<port_list> Port list or 'all', default: All ports

11.2 Mode

LACP>Mode ?
Description:
Set or show LACP mode.

Syntax:

LACP Mode [<port_list>] [enable|disable]

Parameters:
<port_list> Port list or 'all', default: All ports
enable Enable LACP protocol
disable Disable LACP protocol
(default: Show LACP mode)

11.3 Key

LACP>Key ?

Description:

Set or show the LACP key.

Syntax:

LACP Key [<port_list>] [<key>]

Parameters:

<port_list>	Port list or 'all', default: All ports
<key>	LACP key (1-65535) or 'auto'

11.4 Prio

LACP>Prio ?

Description:

Set or show the LACP prio.

Syntax:

LACP Prio [<port_list>] [<prio>]

Parameters:

<port_list>	Port list or 'all', default: All ports
<prio>	LACP Prio (0-65535)

11.5 System Prio

LACP>System Prio ?

Description:

Set or show the LACP System prio.

Syntax:

LACP System Prio [<sysprio>]

Parameters:

<sysprio> LACP System Prio (0-65535)

11.6 Role

LACP>Role ?

Description:

Set or show the LACP role.

Syntax:

LACP Role [<port_list>] [active|passive]

Parameters:

<port_list> Port list or 'all', default: All ports
active Initiate LACP negotiation
passive Listen for LACP packets
(default: Show LACP role)

11.7 Status

LACP>Status ?
Description:
Show LACP Status.

Syntax:

LACP Status [<port_list>]

Parameters:
<port_list> Port list or 'all', default: All ports

11.8 Statistics

LACP>Statistics ?
Description:
Show LACP Statistics.

Syntax:

LACP Statistics [<port_list>] [clear]

Parameters:
<port_list> Port list or 'all', default: All ports
clear Clear LACP statistics

11.9 Timeout

LACP>Timeout ?

Description:

Set or show the LACP timeout.

Syntax:

LACP Timeout [<port_list>] [fast|slow]

Parameters:

<port_list>	Port list or 'all', default: All ports
fast	Fast PDU transmissions (fast timeout)
slow	Slow PDU transmissions (slow timeout)

(default: Show LACP timeout)

Chapter 12 LLDP

12.LLDP

Available Commands:

LLDP Configuration [<port_list>]
LLDP Mode [<port_list>] [enable|disable|rx|tx]
LLDP Optional_TLV [<port_list>] [port_descr|sys_name|sys_descr|sys_capa|mgmt_addr] [enable|disable]
LLDP Interval [<interval>]
LLDP Hold [<hold>]
LLDP Delay [<delay>]
LLDP Reinit [<reinit>]
LLDP Statistics [<port_list>] [clear]
LLDP Info [<port_list>]
LLDP cdp_aware [<port_list>] [enable|disable]

12.1 Configuration

LLDP>Configuration ?
Description:
Show LLDP configuration.

Syntax:

LLDP Configuration [<port_list>]

Parameters:
<port_list> Port list or 'all', default: All ports

12.2 Mode

LLDP>Mode ?
Description:
Set or show LLDP mode.

Syntax:

LLDP Mode [<port_list>] [enable|disable|rx|tx]

Parameters:
<port_list> Port list or 'all', default: All ports
enable Enable LLDP reception and transmission
disable Disable LLDP
rx Enable LLDP reception only
tx Enable LLDP transmission only
(default: Show LLDP mode)

12.3 Optional_TLV

LLDP>Optional_TLV ?
Description:
Set or show LLDP Optional TLVs.

Syntax:

LLDP Optional_TLV [<port_list>] [port_descr|sys_name|sys_descr|sys_capa|mgmt_addr] [enable|disable]

Parameters:
<port_list> Port list or 'all', default: All ports
port_descr Description of the port
sysm_name System name
sys_descr Description of the system
sys_capa System capabilities
mgmt_addr Master's IP address
(default: Show optional TLV's configuration)
enable Enables TLV
disable Disable TLV
(default: Show optional TLV's configuration)

12.4 Interval

LLDP>Interval ?
Description:
Set or show LLDP Tx interval.

Syntax:

LLDP Interval [<interval>]

Parameters:

<interval> LLDP transmission interval (5-32768)

12.5 Hold

LLDP>Hold ?

Description:

Set or show LLDP Tx hold value.

Syntax:

LLDP Hold [<hold>]

Parameters:

<hold> LLDP hold value (2-10)

12.6 Delay

LLDP>Delay ?

Description:

Set or show LLDP Tx delay.

Syntax:

LLDP Delay [<delay>]

Parameters:

<delay> LLDP transmission delay (1-8192)

12.7 Reinit

LLDP>Reinit ?

Description:

Set or show LLDP reinit delay.

Syntax:

LLDP Reinit [<reinit>]

Parameters:

<reinit>: LLDP reinit delay (1-10)

12.8 Statistics

LLDP>Statistics ?

Description:

Show LLDP Statistics.

Syntax:

LLDP Statistics [<port_list>] [clear]

Parameters:

<port_list>	Port list or 'all', default: All ports
clear	Clear LLDP statistics

12.9 Info

LLDP>Info ?

Description:

Show LLDP neighbor device information.

Syntax:

LLDP Info [<port_list>]

Parameters:

<port_list> Port list or 'all', default: All ports

12.10 cdp_aware

LLDP>cdp_aware ?

Description:

Set or show if discovery information from received CDP (Cisco Discovery Protocol) frames is added to the LLDP neighbor table.

Syntax:

LLDP cdp_aware [<port_list>] [enable|disable]

Parameters:

<port_list> Port list or 'all', default: All ports

enable Enable CDP awareness (CDP discovery information is added to the LLDP neighbor table)

disable Disable CDP awareness

(default: Show CDP awareness configuration)

Chapter 13 LLDPMED

13.LLDPMED

Available Commands:

LLDPMED Configuration [<port_list>]
LLDPMED Civic
[country|state|county|city|district|block|street|leading_street_direction|trailing_street_suffix|str_suf|house_no|house_no_suffix|landmark|additional_info|name|zip_code|building|apartment|floor|room_number|place_type|postal_com_name|p_o_box|additional_code]
[<civic_value>]
LLDPMED ecs [<ecs_value>]
LLDPMED policy delete <policy_list>
LLDPMED policy add <policy_type> [tagged|untagged] [<vlan_id>] [<l2_priority>] [<dscp>]
LLDPMED port policies [<port_list>] [<policy_list>]
LLDPMED Coordinates [<tude_type>] [<direction>] [coordinate_value]
LLDPMED Datum [<datum_type>]
LLDPMED Fast [<count>]
LLDPMED Info [<port_list>]

13.1 Configuration

LLDPMED>Configuration ?

Description:

Show LLDP-MED configuration.

Syntax:

LLDPMED Configuration [<port_list>]

Parameters:

<port_list>	Port list or 'all', default: All ports

13.2 Civic

LLDPMED>Civic ?

Description:

Set or show LLDP-MED Civic Address Location.

Syntax:

LLDPMED Civic
[country|state|county|city|district|block|street|leading_street_direction|trailing_street_suffix|str_suf|house_no|house_no_suffix|landmark|additional_info|name|zip_code|building|apartment|floor|room_number|place_type|postal_com_name|p_o_box|additional_code]
[<civic_value>]

Parameters:

country	Country
state	National subdivisions (state, caton, region, province, prefecture)
county	County, parish,gun (JP), district(IN)
city	City, townchip, shi (JP)
district	City division,borough, city, district, ward,chou (JP)
block	Neighborhood, block
street	Street
leading_street_direction	Leading street direction
trailing_street_suffix	Trailing street suffix
str_suf	Street Suffix
house_no	House Number
house_no_suffix	House number suffix
landmark	Landmark or vanity address
additional_info	Additional location informationname : Name(residence and office occupant)
zip_code	Postal/zip code
building	Building (structure)
apartment	Unit (apartment, suite)

floor Floor
room_number Room number
place_type Placetype
postal_com_name Postal community name
p_o_box Post office box (P.O. Box)
additional_code Additional code
(default: Show Civic Address Location configuration)
<civic_value> lldpmed The value for the Civic Address Location entry.

13.3 ecs

LLDPMED>ecs ?
Description:
Set or show LLDP-MED Emergency Call Service.

Syntax:

LLDPMED ecs [<ecs_value>]

Parameters:
<ecs_value> lldpmed The value for the Emergency Call Service

13.4 policy delete

LLDPMED>policy delete ?
Description:
Delete the selected policy.

Syntax:

LLDPMED policy delete <policy_list>

Parameters:

<policy_list> List of policies to delete

13.5 policy add

LLDPMED>policy add ?

Description:

Adds a policy to the list of polices.

Syntax:

LLDPMED policy add <policy_type> [tagged|untagged] [<vlan_id>] [<l2_priority>] [<dscp>]

Parameters:

<policy_type>	The policy_type parameter takes the following values:
voice	Voice for use by dedicated IP Telephony handsets and other similar appliances supporting interactive voice services. These devices are typically deployed on a separate VLAN for ease of deployment and enhanced security by isolation from data applications
voice_signaling	Voice Signaling (conditional) for use in network topologies that require a different policy for the voice signaling than for the voice media.
guest_voice	Guest Voice to support a separate limited feature-set voice service for guest users and visitors with their own IP Telephony handsets and other similar appliances supporting interactive voice services.
guest_voice_signaling	Guest Voice Signaling (conditional) for use in network topologies that require a different policy for the guest voice signaling than for the guest voice media.
softphone_voice	Softphone Voice for use by softphone applications on typical data centric devices, such as PCs or laptops. This class of endpoints frequently does not support multiple VLANs, if at all,and are typically configured to use an untagged VLAN or a single tagged data specific VLAN.
video_conferencing	Video Conferencing for use by dedicated Video Conferencing

	equipment and other similar appliances supporting real-time interactive video/audio services.
streaming_video	Streaming Video for use by broadcast or multicast based video content distribution and other similar applications supporting streaming video services that require specific network policy treatment. Video applications relying on TCP with buffering would not be an intended use of this application type.
video_signaling	Video Signaling (conditional) for use in network topologies that require a separate policy for the video signaling than for the video media.
tagged	The device is using tagged framesunragged : The device is using untagged frames
<vlan_id>	VLAN id
<l2_priority>	This field may specify one of eight priority levels (0 through 7), as defined by IEEE 802.1D-2004 [3].
<dscp>	This field shall contain the DSCP value to be used to provide Diffserv node behavior for the specified application type as defined in IETF RFC 2474 [5]. This 6 bit field may contain one of 64 code point values (0 through 63). A value of 0 represents use of the default DSCP value as defined in RFC 2475.

13.6 port policies

LLDPMED>port policies ?

Description:

Set or show LLDP-MED port policies.

Syntax:

LLDPMED port policies [<port_list>] [<policy_list>]

Parameters:

<port_list>	Port list or 'all', default: All ports
<policy_list>	List of policies to delete

13.7 Coordinates

LLDPMED>Coordinates ?

Description:

Set or show LLDP-MED Location.

Syntax:

LLDPMED Coordinates [<tude_type>] [<direction>] [coordinate_value]

Parameters:

<tude_type>	The tude_type parameter takes the following values:
latitude	Latitude, 0 to 90 degrees with max. 4 digits (Positive numbers are north of the equator and negative numbers are south of the equator).
Longitude	Longitude, 0 to 180 degrees with max. 4 digits (Positive values are East of the prime meridian and negative numbers are West of the prime meridian).
altitude	Altitude, -32767 to 32767 Meters or floors with max. 4 digits.
<direction>	The direction parameter takes the following values:
North	North (Valid for latitude)
South	South (Valid for latitude)
West	West (Valid for longitude)
East	East (Valid for longitude)
Meters	Meters (Valid for altitude)
Floor	Floor (Valid for altitude)
coordinate_value	Coordinate value

13.8 Datum

LLDPMED>Datum ?

Description:

Set or show LLDP-MED Coordinates map datum.

Syntax:

LLDPMED Datum [<datum_type>]

Parameters:

<datum_type>	The datum_type parameter takes the following values:
wgs84	WGS84
nad83_navd88	NAD83_NAVD88
nad83_mllw	NAD83_MLLW

13.9 Fast

LLDPMED>Fast ?

Description:

Set or show LLDP-MED Fast Start Repeat Count.

Syntax:

LLDPMED Fast [<count>]

Parameters:

<count>	The number of times the fast start LLDPDU are being sent during the activation of the fast start mechanism defined by LLDP-MED (1-10).

13.10 Info

LLDPMED>Info ?

Description:

Show LLDP-MED neighbor device information.

Syntax:

LLDPMED Info [<port_list>]

Parameters:

<port_list> Port list or 'all', default: All ports

Chapter 14 EEE

14.EEE

Available Commands:

EEE Configuration [<port_list>]
EEE Mode [<port_list>] [enable|disable]
EEE Urgent_queues [<port_list>] [<queue_list>]

14.1 Configuration

EEE>Configuration ?
Description:
Show EEE configuration.

Syntax:

EEE Configuration [<port_list>]

Parameters:
<port_list> Port list or 'all', default: All ports

14.2 Mode

EEE>Mode ?
Description:
Set or show the EEE mode.

Syntax:

EEE Mode [<port_list>] [enable|disable]

Parameters:
<port_list> Port list or 'all', default: All ports
enable Enable EEE

disable Disable EEE
(default: Show eee mode)

14.3 Urgent_queues

EEE>Urgent_queues ?
Description:
Set or show EEE Urgent queues.

Syntax:

EEE Urgent_queues [<port_list>] [<queue_list>]

Parameters:
<port_list> Port list or 'all', default: All ports
<queue_list> List of queues to configure as urgent queues (1-8 or none)

Chapter 15 THERMAL

15.THERMAL

Available Commands:

Thermal prio_temp [<prio_list>] [<shut_down_temp>]
Thermal port_prio [<port_list>] [<prio>]
Thermal status
Thermal configuration

15.1 prio_temp

Thermal>prio_temp ?
Description:
Set or show the temperature at which the ports shall be shut down.

Syntax:

Thermal prio_temp [<prio_list>] [<shut_down_temp>]

Parameters:

<prio_list> List of priorities (0-3)

<shut_down_temp> Temperature at which ports shall be shut down (0-255 degree C)

15.2 port_prio

Thermal>port_prio ?

Description:

Set or show the ports priority.

Syntax:

Thermal port_prio [<port_list>] [<prio>]

Parameters:

<port_list> Port list or 'all', default: All ports

<prio> Priority (0-3)

15.3 Status

Thermal>Status ?

Description:

Shows the chip temperature.

Syntax:

Thermal status

15.4 Configuration

Thermal>configuration ?

Description:
Show thermal_protect configuration.

Syntax:

Thermal configuration

Chapter 16 LED_POWER

16.LED_POWER

Available Commands:

led_power timers [<hour>] [<intensity>]
led_power delete_timer <hour>
led_power maintenance [<maintenance_time>] [on_at_errors|leave_at_errors]
led_power configuration

16.1 timers

led_power>timers ?
Description:

Set or show the time and intensity for the LEDs.

Syntax:

led_power timers [<hour>] [<intensity>]

Parameters:

<hour> The hour (0-23) at which to change LEDs intensity

<intensity> The LED intensity in % (0-100)

16.2 delete_timer

led_power>delete_timer ?

Description:

Deletes a timer.

Syntax:

led_power delete_timer <hour>

Parameters:

<hour> The hour (0-23) at which to change LEDs intensity

16.3 maintenance

led_power>maintenance ?

Description:

Set or show the maintenance settings.

Syntax:

led_power maintenance [<maintenance_time>] [on_at_errors|leave_at_errors]

Parameters:

<maintenance_time>	Time in seconds (0-65535) that the LEDs shall be turned on, when any port changes link state
on_at_errors|leave_at_errors	on_at_error if LEDs shall be turned on if any errors has been detected. leave_at_errors if no LED change shall happen when errors have been detected

16.4 configuration

led_power>configuration ?

Description:

Show Led Power Reduction configuration.

Syntax:

led_power configuration

Chapter 17 QoS

17.QoS

Available Commands:

QoS Configuration [<port_list>]
QoS Port Classification Class [<port_list>] [<class>]
QoS Port Classification DPL [<port_list>] [<dpl>]
QoS Port Classification PCP [<port_list>] [<pcp>]
QoS Port Classification DEI [<port_list>] [<dei>]
QoS Port Classification Tag [<port_list>] [enable|disable]
QoS Port Classification Map [<port_list>] [<pcp_list>] [<dei_list>] [<class>] [<dpl>]
QoS Port Classification DSCP [<port_list>] [enable|disable]
QoS Port Policer Mode [<port_list>] [enable|disable]
QoS Port Policer Rate [<port_list>] [<rate>]
QoS Port Policer Unit [<port_list>] [kbps|fps]
QoS Port Policer FlowControl [<port_list>] [enable|disable]
QoS Port Scheduler Mode [<port_list>] [strict|weighted]
QoS Port Scheduler Weight [<port_list>] [<queue_list>] [<weight>]
QoS Port Shaper Mode [<port_list>] [enable|disable]
QoS Port Shaper Rate [<port_list>] [<bit_rate>]
QoS Port QueueShaper Mode [<port_list>] [<queue_list>] [enable|disable]
QoS Port QueueShaper Rate [<port_list>] [<queue_list>] [<bit_rate>]
QoS Port QueueShaper Excess [<port_list>] [<queue_list>] [enable|disable]
QoS Port TagRemarking Mode [<port_list>] [classified|default|mapped]
QoS Port TagRemarking PCP [<port_list>] [<pcp>]
QoS Port TagRemarking DEI [<port_list>] [<dei>]
QoS Port TagRemarking Map [<port_list>] [<class_list>] [<dpl_list>] [<pcp>] [<dei>]

QoS Port DSCP Translation [<port_list>] [enable|disable]
QoS Port DSCP Classification [<port_list>] [none|zero|selected|all]
QoS Port DSCP EgressRemark [<port_list>]
[disable|enable|remap_dp_unaware|remap_dp_aware]
QoS DSCP Map [<dscp_list>] [<class>] [<dpl>]
QoS DSCP Translation [<dscp_list>] [<trans_dscp>]
QoS DSCP Trust [<dscp_list>] [enable|disable]
QoS DSCP Classification Mode [<dscp_list>] [enable|disable]
QoS DSCP Classification Map [<class_list>] [<dpl_list>] [<dscp>]
QoS DSCP EgressRemap [<dscp_list>] [<dpl_list>] [<dscp>]
QoS Storm Unicast [enable|disable] [<packet_rate>]
QoS Storm Multicast [enable|disable] [<packet_rate>]
QoS Storm Broadcast [enable|disable] [<packet_rate>]
QoS QCL Add [<qce_id>] [<qce_id_next>]
    [<port_list>]
    [<tag>] [<vid>] [<pcp>] [<dei>] [<smac>] [<dmac_type>]
    [(etype [<etype>]) |
    (LLC [<DSAP>] [<SSAP>] [<control>]) |
    (SNAP [<PID>]) |
    (ipv4 [<protocol>] [<sip>] [<dscp>] [<fragment>] [<sport>] [<dport>]) |
    (ipv6 [<protocol>] [<sip_v6>] [<dscp>] [<sport>] [<dport>])]
    [<class>] [<dp>] [<classified_dscp>]
QoS QCL Delete <qce_id>
QoS QCL Lookup [<qce_id>]
QoS QCL Status [combined|static|voice_vlan|conflicts]
QoS QCL Refresh

17.1 Configuration

QoS>Configuration ?

Description:

Show QoS Configuration.

Syntax:

QoS Configuration [<port_list>]

Parameters:

<port_list> Port list or 'all', default: All ports

17.2 Port Classification Class

QoS>Port Classification Class ?

Description:

Set or show the default QoS class.
If the QoS class has been dynamically changed, then the actual
QoS class is shown in parentheses after the configured QoS class.

Syntax:

QoS Port Classification Class [<port_list>] [<class>]

Parameters:

<port_list> Port list or 'all', default: All ports
<class> QoS class (0-7)

17.3 Port Classification DPL

QoS>Port Classification DPL ?

Description:

Set or show the default Drop Precedence Level.

Syntax:

QoS Port Classification DPL [<port_list>] [<dpl>]

Parameters:

<port_list>	Port list or 'all', default: All ports
<dpl>	Drop Precedence Level (0-1)

17.4 Port Classification PCP

QoS>Port Classification PCP ?

Description:

Set or show the default PCP for an untagged frame.

Syntax:

QoS Port Classification PCP [<port_list>] [<pcp>]

Parameters:

<port_list>	Port list or 'all', default: All ports
<pcp>	Priority Code Point (0-7)

17.5 Port Classification DEI

QoS>Port Classification DEI ?

Description:

Set or show the default DEI for an untagged frame.

Syntax:

QoS Port Classification DEI [<port_list>] [<dei>]

Parameters:

<port_list>	Port list or 'all', default: All ports
<dei>	Drop Eligible Indicator (0-1)

17.6 Port Classification Tag

QoS>Port Classification Tag ?

Description:

Set or show if the classification is based on the PCP and DEI values in tagged frames.

Syntax:

QoS Port Classification Tag [<port_list>] [enable|disable]

Parameters:

<port_list>	Port list or 'all', default: All ports
enable	Enable tag classification
disable	Disable tag classification

(default: Show tag classification mode)

17.7 Port Classification Map

QoS>Port Classification Map ?

Description:

Set or show the port classification map.
This map is used when port classification tag is enabled,
and the purpose is to translate the Priority Code Point (PCP) and
Drop Eligible Indicator (DEI) from a tagged frame to QoS class
and DP level.

Syntax:

QoS Port Classification Map [<port_list>] [<pcp_list>] [<dei_list>] [<class>] [<dpl>]

Parameters:

<port_list>	Port list or 'all', default: All ports
<pcp_list>	PCP list or 'all', default: All PCPs (0-7)
<dei_list>	DEI list or 'all', default: All DEIs (0-1)
<class>	QoS class (0-7)
<dpl>	Drop Precedence Level (0-1)

17.8 Port Classification DSCP

QoS>Port Classification DSCP ?

Description:

Set or show if the classification is based on DSCP value in IP frames.

Syntax:

QoS Port Classification DSCP [<port_list>] [enable|disable]

Parameters:

<port_list>	Port list or 'all', default: All ports
enable	Enable DSCP based classification
disable	Disable DSCP based classification

(default: Show DSCP based classification mode)

17.9 Port Policer Mode

QoS>Port Policer Mode ?

Description:

Set or show the port policer mode.

Syntax:

QoS Port Policer Mode [<port_list>] [enable|disable]

Parameters:

<port_list>	Port list or 'all', default: All ports
enable	Enable port policer
disable	Disable port policer

(default: Show port policer mode)

17.10 Port Policer Rate

QoS>Port Policer Rate ?

Description:

Set or show the port policer rate.

Syntax:

QoS Port Policer Rate [<port_list>] [<rate>]

Parameters:

<port_list>	Port list or 'all', default: All ports
<rate>	Rate in kbps or fps (100-3300000)

17.11 Port Policer Unit

QoS>Port Policer Unit ?

Description:

Set or show the port policer unit.

Syntax:

QoS Port Policer Unit [<port_list>] [kbps|fps]

Parameters:

<port_list>	Port list or 'all', default: All ports

kbps Unit is kilo bits per second
fps Unit is frames per second
(default: Show port policer unit)

17.12 Port Policer FlowControl

QoS>Port Policer FlowControl ?
Description:
Set or show the port policer flow control.
If policer flow control is enabled and the port is in flow control mode,
then pause frames are sent instead of discarding frames.

Syntax:

QoS Port Policer FlowControl [<port_list>] [enable|disable]

Parameters:
<port_list> Port list or 'all', default: All ports
enable Enable port policer flow control
disable Disable port policer flow control
(default: Show port policer flow control mode)

17.13 Port Scheduler Mode

QoS>Port Scheduler Mode ?
Description:
Set or show the port scheduler mode.

Syntax:

QoS Port Scheduler Mode [<port_list>] [strict|weighted]

Parameters:
<port_list> Port list or 'all', default: All ports

strict Strict mode
weighted Weighted mode
(default: Show port scheduler mode)

17.14 Port Scheduler Weight

QoS>Port Scheduler Weight ?

Description:

Set or show the port scheduler weight.

Syntax:

QoS Port Scheduler Weight [<port_list>] [<queue_list>] [<weight>]

Parameters:

<port_list> Port list or 'all', default: All ports
<queue_list> Weighted queue list or 'all', default: All weighted queues (0-5)
<weight> Scheduler weight (1-100)

17.15 Port Shaper Mode

QoS>Port Shaper Mode ?

Description:

Set or show the port shaper mode.

Syntax:

QoS Port Shaper Mode [<port_list>] [enable|disable]

Parameters:

<port_list> Port list or 'all', default: All ports
enable Enable port shaper
disable Disable port shaper

(default: Show port shaper mode)

17.16 Port Shaper Rate

QoS>Port Shaper Rate ?

Description:

Set or show the port shaper rate.

Syntax:

QoS Port Shaper Rate [<port_list>] [<bit_rate>]

Parameters:

<port_list>	Port list or 'all', default: All ports
<bit_rate>	Rate in kilo bits per second (100-3300000)

17.17 Port QueueShaper Mode

QoS>Port QueueShaper Mode ?

Description:

Set or show the port queue shaper mode.

Syntax:

QoS Port QueueShaper Mode [<port_list>] [<queue_list>] [enable|disable]

Parameters:

<port_list>	Port list or 'all', default: All ports
<queue_list>	Queue list or 'all', default: All queues (0-7)
enable	Enable port queue shaper
disable	Disable port queue shaper

(default: Show port queue shaper mode)

17.18 Port QueueShaper Rate

QoS>Port QueueShaper Rate ?

Description:

Set or show the port queue shaper rate.

Syntax:

QoS Port QueueShaper Rate [<port_list>] [<queue_list>] [<bit_rate>]

Parameters:

<port_list>	Port list or 'all', default: All ports
<queue_list>	Queue list or 'all', default: All queues (0-7)
<bit_rate>	Rate in kilo bits per second (100-3300000)

17.19 Port QueueShaper Excess

QoS>Port QueueShaper Excess ?

Description:

Set or show the port queue excess bandwidth mode.

Syntax:

QoS Port QueueShaper Excess [<port_list>] [<queue_list>] [enable|disable]

Parameters:

<port_list>	Port list or 'all', default: All ports
<queue_list>	Queue list or 'all', default: All queues (0-7)
enable	Enable use of excess bandwidth
disable	Disable use of excess bandwidth

(default: Show port queue excess bandwidth mode)

17.20 Port TagRemarking Mode

QoS>Port TagRemarking Mode ?

Description:

Set or show the port tag remarking mode.

Syntax:

QoS Port TagRemarking Mode [<port_list>] [classified|default|mapped]

Parameters:

<port_list>	Port list or 'all', default: All ports
classified	Use classified PCP/DEI values
default	Use default PCP/DEI values
mapped	Use mapped versions of QoS class and DP level

(default: Show port tag remarking mode)

17.21 Port TagRemarking PCP

QoS>Port TagRemarking PCP ?

Description:

Set or show the default PCP.

This value is used when port tag remarking mode is set to 'default'.

Syntax:

QoS Port TagRemarking PCP [<port_list>] [<pcp>]

Parameters:

<port_list>	Port list or 'all', default: All ports
<pcp>	Priority Code Point (0-7)

17.22 Port TagRemarking DEI

QoS>Port TagRemarking DEI ?

Description:

Set or show the default DEI.
This value is used when port tag remarking mode is set to 'default'.

Syntax:

QoS Port TagRemarking DEI [<port_list>] [<dei>]

Parameters:

<port_list>	Port list or 'all', default: All ports
<dei>	Drop Eligible Indicator (0-1)

17.23 Port TagRemarking Map

QoS>Port TagRemarking Map ?

Description:

Set or show the port tag remarking map.
This map is used when port tag remarking mode is set to 'mapped',
and the purpose is to translate the classified QoS class (0-7)
and DP level (0-1) to PCP and DEI.

Syntax:

QoS Port TagRemarking Map [<port_list>] [<class_list>] [<dpl_list>] [<pcp>] [<dei>]

Parameters:

<port_list>	Port list or 'all', default: All ports
<class_list>	QoS class list or 'all', default: All QoS classes (0-7)

<dpl_list>	DP level list or 'all', default: All DP levels (0-1)
<pcp>	Priority Code Point (0-7)
<dei>	Drop Eligible Indicator (0-1)

17.24 Port DSCP Translation

QoS>Port DSCP Translation ?

Description:

Set or show DSCP ingress translation mode.
If translation is enabled for a port, incoming frame DSCP value is translated and translated value is used for QoS classification.

Syntax:

QoS Port DSCP Translation [<port_list>] [enable|disable]

Parameters:

<port_list>	Port list or 'all', default: All ports
enable	Enable DSCP ingress translation
disable	Disable DSCP ingress translation

(default: Show DSCP ingress translation mode)

17.25 Port DSCP Classification

QoS>Port DSCP Classification ?

Description:

Set or show DSCP classification based on QoS class and DP level.
This enables per port to map new DSCP value based on QoS class and DP level.

Syntax:

QoS Port DSCP Classification [<port_list>] [none|zero|selected|all]

Parameters:

<port_list>	Port list or 'all', default: All ports
none	No DSCP ingress classification
zero	Classify DSCP if DSCP = 0
selected	Classify DSCP for which class. mode is 'enable'
all	Classify all DSCP

(default: Show port DSCP ingress classification mode)

17.26 Port DSCP EgressRemark

QoS>Port DSCP EgressRemark ?

Description:

Set or show the port DSCP remarking mode.

Syntax:

QoS Port DSCP EgressRemark [<port_list>]
[disable|enable|remap_dp_unaware|remap_dp_aware]

Parameters:

<port_list>	Port list or 'all', default: All ports
disable	Disable DSCP egress rewrite
enable	Enable DSCP egress rewrite with the value received from analyzer
remap_dp_unaware	Rewrite DSCP in egress frame with remapped DSCP where remap is DP unaware or DP = 0
remap_dp_aware	Rewrite DSCP in egress frame with remapped DSCP where remap is DP aware and DP = 1

(default: Show port DSCP egress remarking mode)

17.27 DSCP Map

QoS>DSCP Map ?

Description:

Set or show DSCP mapping table.
This table is used to map QoS class and DP level based on DSCP value.
DSCP value used to map QoS class and DPL is either translated DSCP
value or incoming frame DSCP value.

Syntax:

QoS DSCP Map [<dscp_list>] [<class>] [<dpl>]

Parameters:

<dscp_list> DSCP (0-63 list or 'all'
(default: Show DSCP ingress map table i.e. DSCP->(class, DPL))
<class> QoS class (0-7)
<dpl> Drop Precedence Level (0-1)

17.28 DSCP Translation

QoS>DSCP Translation ?

Description:

Set or show global ingress DSCP translation table.
If port DSCP translation is enabled, translation table is used to
translate incoming frames DSCP value and translated value is used
to map QoS class and DP level.

Syntax:

QoS DSCP Translation [<dscp_list>] [<trans_dscp>]

Parameters:

<dscp_list>	DSCP (0-63) list or 'all'

(default: Show DSCP translation table)

<trans_dscp>	Translated DSCP: 0-63, BE, CS1-CS7, EF or AF11-AF43

17.29 DSCP Trust

QoS>DSCP Trust ?

Description:

Set or show whether a specific DSCP value is trusted.
Only frames with trusted DSCP values are mapped to a specific QoS class and DPL.
Frames with untrusted DSCP values are treated as a non-IP frame.

Syntax:

QoS DSCP Trust [<dscp_list>] [enable|disable]

Parameters:

<dscp_list>	DSCP (0-63) list or 'all'
enable	Set DSCP as trusted DSCP
disable	Set DSCP as un-trusted DSCP

(default: Show DSCP Trust status)

17.30 DSCP Classification Mode

QoS>DSCP Classification Mode ?

Description:

Set or show DSCP ingress classification mode.
If port DSCP classification is 'selected', DSCP will be classified
based on QoS class and DP level only for DSCP value with classification
mode 'enabled'. DSCP may be translated DSCP if translation is enabled
for the port.

Syntax:

QoS DSCP Classification Mode [<dscp_list>] [enable|disable]

Parameters:

<dscp_list>	DSCP (0-63) list or 'all'
enable	Enable DSCP ingress classification
disable	Disable DSCP ingress classification

(default: Show DSCP classification mode)

17.31 DSCP Classification Map

QoS>DSCP Classification Map ?

Description:

Set or show DSCP ingress classification table.
This table is used to map DSCP from QoS class and DP level. The DSCP
which needs to be classified depends on port DSCP classification and
DSCP classification mode. Incoming frame DSCP may be translated beforeusing the value for classification.

Syntax:

QoS DSCP Classification Map [<class_list>] [<dpl_list>] [<dscp>]

Parameters:

<class_list>	QoS class list or 'all', default: All QoS classes (0-7)
<dpl_list>	DP level list or 'all', default: All DP levels (0-1)
<dscp>	Mapped DSCP: 0-63, BE, CS1-CS7, EF or AF11-AF43

17.32 DSCP EgressRemap

QoS>DSCP EgressRemap ?

Description:

Set or show DSCP egress remap table. This table is used if the port
egress remarking mode is 'remap' and the purpose is to map the
DSCP and DP level to a new DSCP value.

Syntax:

QoS DSCP EgressRemap [<dscp_list>] [<dpl_list>] [<dscp>]

Parameters:

<dscp_list>	DSCP (0-63) list or 'all'
<dpl_list>	DP level list or 'all', default: All DP levels (0-1)
<dscp>	Egress remapped DSCP: 0-63, BE, CS1-CS7, EF or AF11-AF43

17.33 Storm Unicast

QoS>Storm Unicast ?

Description:

Set or show the unicast storm rate limiter.
The limiter will only affect flooded frames,
i.e. frames with a (VLAN ID, DMAC) pair not present in the MAC Address table.

Syntax:

QoS Storm Unicast [enable|disable] [<packet_rate>]

Parameters:

enable : Enable unicast storm control
disable : Disable unicast storm control
<packet_rate>: Rate in fps (1, 2, 4, ..., 512, 1k, 2k, 4k, ..., 1024k)

17.34 Storm Multicast

QoS>Storm Multicast ?

Description:

Set or show the multicast storm rate limiter.
The limiter will only affect flooded frames,
i.e. frames with a (VLAN ID, DMAC) pair not present in the MAC Address table.

Syntax:

QoS Storm Multicast [enable|disable] [<packet_rate>]

Parameters:

enable	Enable multicast storm control
disable	Disable multicast storm control
<packet_rate>	Rate in fps (1, 2, 4, ..., 512, 1k, 2k, 4k, ..., 1024k)

17.35 Storm Broadcast

QoS>Storm Broadcast ?

Description:

Set or show the broadcast storm rate limiter.
The limiter will only affect flooded frames,
i.e. frames with a (VLAN ID, DMAC) pair not present in the MAC Address table.

Syntax:

QoS Storm Broadcast [enable|disable] [<packet_rate>]

Parameters:

enable : Enable broadcast storm control
disable : Disable broadcast storm control
<packet_rate>: Rate in fps (1, 2, 4, ..., 512, 1k, 2k, 4k, ..., 1024k)

17.36 QCL Add

QoS>QCL Add ?

Description:

Add or modify QoS Control Entry (QCE).

If the QCE ID parameter <qce_id> is specified and an entry with this QCE ID already exists, the QCE will be modified. Otherwise, a new QCE will be added. If the QCE ID is not specified, the next available QCE ID will be used. If the next QCE ID parameter <qce_id_next> is specified, the QCE will be placed

before this QCE in the list. If the next QCE ID is not specified and if it is a new entry added, the QCE will be placed last in the list. Otherwise if the next QCE ID is not specified and if existing QCE is modified, QCE will be in the same location in the list. To modify and move the entry to last in the list, use the word 'last' for <qce_id_next>.

Syntax:

```
QoS QCL Add [<qce_id>] [<qce_id_next>] [<port_list>] [<tag>] [<vid>] [<pcp>] [<dei>]
             [<smac>] [<dmac_type>] [(etype [<etype>]) |
             (LLC   [<DSAP>] [<SSAP>] [<control>]) |
             (SNAP   [<PID>]) |
            (ipv4   [<protocol>] [<sip>] [<dscp>] [<fragment>] [<sport>] [<dport>]) |
            (ipv6   [<protocol>] [<sip_v6>] [<dscp>] [<sport>] [<dport>])]
            [<class>] [<dp>] [<classified_dscp>]
```

Parameters:

<qce_id>	QCE ID (1-256), default: Next available ID
<qce_id_next>	Next QCE ID: "next_id (1-256) or 'last'"
<port_list>	Port List: "port <port_list> or 'all'", default: All ports
<tag>	Frame tag: untag|tag|any
<vid>	VID: 1-4095 or 'any', either a specific VID or range of VIDs
<pcp>	Priority Code Point: specific(0, 1, 2, 3, 4, 5, 6, 7) or range(0-1, 2-3, 4-5, 6-7, 0-3, 4-7) or 'any'
<dei>	Drop Eligible Indicator: 0-1 or 'any'
<smac>	Source MAC address: (xx-xx-xx) or 'any', 24 MS bits (OUI)
<dmac_type>	Destination MAC type: unicast|multicast|broadcast|any
etype	Ethernet Type keyword
<etype>	Ethernet Type: 0x600-0xFFFF or 'any' but excluding 0x800(IPv4) and 0x86DD(IPv6)
llc	LLC keyword
<dsap>	Destination Service Access Point: 0x00-0xFF or 'any'
<ssap>	Source Service Access Point: 0x00-0xFF or 'any'
<control>	LLC control: 0x00-0xFF or 'any'
snap	SNAP keyword
<pid>	Protocol ID (EtherType) or 'any'

ipv4	IPv4 keyowrd
<protocol>	IP protocol number: (0-255, TCP or UDP) or 'any'
<sip>	Source IP address: (a.b.c.d/n) or 'any'
<dscp>	DSCP: (0-63,BE,CS1-CS7,EF or AF11-AF43) or 'any', specific or range
<fragment>	IPv4 frame fragmented: yes|no|any
<sport>	Source TCP/UDP port:(0-65535) or 'any', specific or port range
<dport>	Dest. TCP/UDP port:(0-65535) or 'any', specific or port range
ipv6	IPv6 keyowrd
<sip_v6>	IPv6 source address: (a.b.c.d/n) or 'any', 32 LS bits
<class>	QoS Class: "class (0-7)", default: basic classification
<dp>	DP Level: "dp (0-1)", default: basic classification
<classified_dscp>	DSCP: "dscp (0-63, BE, CS1-CS7, EF or AF11-AF43)"

17.37 QCL Delete

QoS>QCL Delete ?

Description:

Delete QCE entry from QoS Control list.

Syntax:

QoS QCL Delete <qce_id>

Parameters:

<qce_id>: QCE ID (1-256), default: Next available ID

17.38 QCL Lookup

QoS>QCL Lookup ?

Description:

Lookup QoS Control List.

Syntax:

QoS QCL Lookup [<qce_id>]

Parameters:
<qce_id>: QCE ID (1-256), default: Next available ID

17.39 QCL Status

QoS>QCL Status ?
Description:
Show QCL status. This can be used to display if there is any
conflict in QCE for differnet user types.

Syntax:

QoS QCL Status [combined|static|voice_vlan|conflicts]

Parameters:
combined|static|voice_vlan|conflicts: combined : Shows the combined status
static Shows the static user configured status
voice_vlan Shows the status by Voice VLAN
conflicts Shows all conflict status
(default : Shows the combined status)

17.40 QCL Refresh

QoS>QCL Refresh ?
Description:

Resolve QCE conflict status. Same H/W resource is shared by multiple applications and it may not be available even before MAX QCE entry. So user can release the resource in use by other applications and use this command to acquire the resource.

Syntax:

QoS QCL Refresh

Chapter 18 MIRROR

~~18.MIRROR~~

Available Commands:

Mirror Configuration [<port_list>]
Mirror Port [<port>|disable]
Mirror Mode [<port_cpu_list>] [enable|disable|rx|tx]

18.1 Configuration

Mirror>Configuration ?
Description:
Show mirror configuration.

Syntax:

Mirror Configuration [<port_list>]

Parameters:

<port_list>	Port list or 'all', default: All ports

18.2 Port

Mirror>Port ?

Description:

Set or show the mirror port.

Syntax:

Mirror Port [<port>|disable]

Parameters:

<port>|disable	Mirror port or 'disable', default: Show port

18.3 Port

Mirror>Mode ?

Description:

Set or show the mirror mode.

Syntax:

Mirror Mode [<port_cpu_list>] [enable|disable|rx|tx]

Parameters:

<port_cpu_list>	Port list or CPU or 'all', default: All ports and CPU
enable	Enable Rx and Tx mirroring
disable	Disable Mirroring
rx	Enable Rx mirroring
tx	Enable Tx mirroring

(default: Show mirror mode)

Chapter 19 CONFIG

19.CONFIG

Available Commands:

Config Save <ip_server> <file_name>
Config Load <ip_server> <file_name> [check]

19.1 Save

Config>Save ?
Description:
Save configuration to TFTP server.

Syntax:

Config Save <ip_server> <file_name>

Parameters:

<ip_server>	TFTP server IPv4 address (a.b.c.d)
<file_name>	Configuration file name

19.2 Load

Config>Load ?

Description:

Load configuration from TFTP server.

Syntax:

Config Load <ip_server> <file_name> [check]

Parameters:

<ip_server>	TFTP server IPv4 address (a.b.c.d)
<file_name>	Configuration file name
check	Check configuration file only, default: Check and apply file

Chapter 20 FIRMWARE

20.FIRMWARE

Available Commands:

Firmware Load <ip_addr_string> <file_name>
Firmware IPv6 Load <ipv6_server> <file_name>
Firmware Information
Firmware Swap

20.1 Load

Firmware>Load ?
Description:
Load new firmware from TFTP server.

Syntax:

Firmware Load <ip_addr_string> <file_name>

Parameters:

<ip_addr_string>	IP host address (a.b.c.d) or a host name string
<file_name>	Firmware file name

20.2 IPv6 Load

Firmware>IPv6 LOad ?

Description:

Load new firmware from IPv6 TFTP server.

Syntax:

Firmware IPv6 Load <ipv6_server> <file_name>

Parameters:

<ipv6_server>	TFTP server IPv6 address
<file_name>	Firmware file name

20.3 Information

Firmware>Information ?

Description:

Display information about active and alternate firmware images.

Syntax:

Firmware Information

20.4 Swap

Firmware>Swap ?

Description:

Activate the alternate firmware image..

Syntax:

Firmware Swap

Chapter 21 UPnP

21.UPnP

Available Commands:

UPnP Configuration
UPnP Mode [enable|disable]
UPnP TTL [<ttl>]
UPnP AdvertisingDuration [<duration>]

21.1 Configuration

UPnP>Configuration ?
Description:
Show UPnP configuration.

Syntax:

UPnP Configuration

21.2 Mode

UPnP>Mode ?
Description:
Set or show the UPnP mode.

Syntax:

UPnP Mode [enable|disable]

Parameters:
enable Enable UPnP
disable Disable UPnP
(default: Show UPnP mode)

21.3 TTL

UPnP>TTL ?
Description:
Set or show the TTL value of the IP header in SSDP messages.

Syntax:

UPnP TTL [<ttl>]

Parameters:

<ttl>	ttl range (1..255), default: Show UPnP TTL

21.4 AdvertisingDuration

UPnP>AdvertisingDuration ?

Description:

Set or show UPnP Advertising Duration.

Syntax:

UPnP AdvertisingDuration [<duration>]

Parameters:

<duration>	duration range (100..86400), default: Show UPnP duration range

Chapter 22 MVR

22.MVR

Available Commands:

MVR Configuration
MVR Mode [enable|disable]
MVR VLAN Setup [<mvid>] [add|del|upd] [(Name <mvr_name>)]
MVR VLAN Mode [<vid>|<mvr_name>] [dynamic|compatible]
MVR VLAN Port [<vid>|<mvr_name>] [<port_list>] [source|receiver|inactive]
MVR VLAN LLQI [<vid>|<mvr_name>] [mvr_param_llqi]
MVR VLAN Channel [<vid>|<mvr_name>] [add|del|upd] [channel] [channel_bound] [(Name <grp_name>)]
MVR VLAN Priority [<vid>|<mvr_name>] [priority] [tagged|untagged]
MVR Immediate Leave [<port_list>] [enable|disable]
MVR Status [<vid>] [clear]
MVR Groups [<vid>]
MVR SFM [<vid>] [<port_list>]

22.1 Configuration

MVR>Configuration ?
Description:
Show MVR configuration.

Syntax:

MVR Configuration

22.2 Mode

MVR>Mode ?
Description:
Set or show system MVR mode.

Syntax:

MVR Mode [enable|disable]

Parameters:
enable : Enable MVR Mode
disable : Disable MVR Mode
(default: Show MVR mode)

22.3 VLAN Setup

MVR>VLAN Setup ?

Description:

Set or show per MVR VLAN configuration.

Syntax:

MVR VLAN Setup [<mvid>] [add|del|upd] [(Name <mvr_name>)]

Parameters:

<mvid>	MVR VLAN ID (1-4095)
add	Add operation
del	Delete operation
upd	Update operation
name	MVR Name keyword
<mvr_name>	MVR VLAN name (Maximum of 32 characters)

22.4 VLAN Mode

MVR>VLAN Mode ?

Description:

Set or show per MVR VLAN mode.

Syntax:

MVR VLAN Mode [<vid>|<mvr_name>] [dynamic|compatible]

Parameters:

<vid>|<mvr_name>	MVR VLAN ID (1-4095) or Name (Maximum of 32 characters)
dynamic	Dynamic MVR mode

compatible Compatible MVR mode
(default: Show MVR VLAN mode)

22.5 VLAN Port

MVR>VLAN Port ?
Description:
Set or show per MVR VLAN port role.

Syntax:

MVR VLAN Port [<vid>|<mvr_name>] [<port_list>] [source|receiver|inactive]

Parameters:
<vid>|<mvr_name>: MVR VLAN ID (1-4095) or Name (Maximum of 32 characters)
<port_list> : Port list or 'all', default: All ports
source : MVR source port
receiver : MVR receiver port
inactive : Disable MVR
(default: Show MVR port role)

22.6 VLAN LLQI

MVR>VLAN LLQI ?
Description:
Set or show per MVR VLAN LLQI (Last Listener Query Interval).

Syntax:

MVR VLAN LLQI [<vid>|<mvr_name>] [mvr_param_llqi]

Parameters:
<vid>|<mvr_name> MVR VLAN ID (1-4095) or Name (Maximum of 32 characters)
mvr_param_llqi

-1	Default Value (5)
0~31744	Last Listener Query Interval in tenths of seconds

(default: Show MVR Interface Last Listener Query Interval

22.7 VLAN Channel

MVR>VLAN Channel ?

Description:

Set or show per MVR VLAN channel.

Syntax:

MVR VLAN Channel [<vid>|<mvr_name>] [add|del|upd] [channel] [channel_bound] [(Name <grp_name>)]

Parameters:

<vid>|<mvr_name>	MVR VLAN ID (1-4095) or Name (Maximum of 32 characters)
add	Add operation
del	Delete operation
upd	Update operation
channel	IPv4/IPv6 multicast group address
channel_bound	The boundary IPv4/IPv6 multicast group address for the channel
name	MVR Name keyword
<grp_name>	MVR Channel name. (Maximum of 32 characters)

22.8 VLAN Priority

MVR>VLAN Priority ?

Description:

Set or show per MVR VLAN priority and VLAN tag.

Syntax:

MVR VLAN Priority [<vid>|<mvr_name>] [priority] [tagged|untagged]

Parameters:

<vid>|<mvr_name>	MVR VLAN ID (1-4095) or Name (Maximum of 32 characters)
priority	CoS priority value ranges from 0 ~ 7
tagged	Tagged IGMP/MLD frames will be sent
untagged	Untagged IGMP/MLD frames will be sent

22.9 Immediate Leave

MVR>Immediate Leave ?

Description:

Set or show MVR immediate leave per port.

Syntax:

MVR Immediate Leave [<port_list>] [enable|disable]

Parameters:

<port_list>	Port list or 'all', default: All ports
enable	Enable Immediate Leave
disable	Disable Immediate Leave

(default: Show MVR Immediate Leave)

22.10 Status

MVR>Status ?

Description:

Show/Clear MVR operational status.

Syntax:

MVR Status [<vid>] [clear]

Parameters:

<vid>	VLAN ID (1-4095)
clear	Clear log

22.11 Groups

MVR>Groups ?

Description:

Show MVR group addresses.

Syntax:

MVR Groups [<vid>]

Parameters:

<vid>	VLAN ID (1-4095)

22.12 SFM

MVR>SFM ?

Description:

Show SFM (including SSM) related information for MVR.

Syntax:

MVR SFM [<vid>] [<port_list>]

Parameters:

<vid>	VLAN ID (1-4095)
<port_list>	Port list or 'all', default: All ports

Chapter 23 VOICE VLAN

23.VOICE VLAN

Available Commands:

Voice VLAN Configuration
Voice VLAN Mode [enable|disable]
Voice VLAN ID [<vid>]
Voice VLAN Agetime [<age_time>]
Voice VLAN Traffic Class [<class>]
Voice VLAN OUI Add <oui_addr> [<description>]
Voice VLAN OUI Delete <oui_addr>
Voice VLAN OUI Clear
Voice VLAN OUI Lookup [<oui_addr>]
Voice VLAN Port Mode [<port_list>] [disable|auto|force]
Voice VLAN Security [<port_list>] [enable|disable]
Voice VLAN Discovery Protocol [<port_list>] [oui|lldp|both]

23.1 Configuration

Voice/VLAN>Configuration ?
Description:
Show Voice VLAN configuration.

Syntax:

Voice VLAN Configuration

23.2 Mode

Voice/VLAN>Mode ?
Description:
Set or show the Voice VLAN mode.
We must disable MSTP feature before we enable Voice VLAN.
It can avoid the conflict of ingress filter.

Syntax:

Voice VLAN Mode [enable|disable]

Parameters:
enable : Enable Voice VLAN mode.
disable: Disable Voice VLAN mode
(default: Show flow Voice VLAN mode)

23.3 ID

Voice/VLAN>ID ?

Description:

Set or show Voice VLAN ID.

Syntax:

Voice VLAN ID [<vid>]

Parameters:

<vid>: VLAN ID (1-4095)

23.4 Agetime

Voice/VLAN>Agetime ?

Description:

Set or show Voice VLAN age time.

Syntax:

Voice VLAN Agetime [<age_time>]

Parameters:

<age_time>	MAC address age time (10-10000000) default: Show age time

23.5 Traffic Class

Voice/VLAN>Traffic Class ?
Description:
Set or show Voice VLAN ID.

Syntax:

Voice VLAN Traffic Class [<class>]

Parameters:

<class>	Traffic class (0-7)

23.6 OUI Add

Voice/VLAN>OUI Add ?
Description:
Add Voice VLAN OUI entry.
Modify OUI table will restart auto detect OUI process.
The maximum entry number is (16).

Syntax:

Voice VLAN OUI Add <oui_addr> [<description>]

Parameters:

<oui_addr>	OUI address (xx-xx-xx). The null OUI address isn't allowed
<description>	Entry description. Use 'clear' or "" to clear the string No blank or space characters are permitted as part of a contact. (only in CLI)

23.7 OUI Delete

Voice/VLAN>OUI Delete ?

Description:

Delete Voice VLAN OUI entry.

Modify OUI table will restart auto detect OUI process.

Syntax:

Voice VLAN OUI Delete <oui_addr>

Parameters:

<oui_addr>	OUI address (xx-xx-xx). The null OUI address isn't allowed

23.8 OUI Clear

Voice/VLAN>OUI Clear ?

Description:

Clear Voice VLAN OUI entry.

Modify OUI table will restart auto detect OUI process.

Syntax:

Voice VLAN OUI Clear

23.9 OUI Lookup

Voice/VLAN>OUI Lookup ?
Description:
Lookup Voice VLAN OUI entry.

Syntax:

Voice VLAN OUI Lookup [<oui_addr>]

Parameters:

<oui_addr>	OUI address (xx-xx-xx), default: Show OUI address

23.10 Port Mode

Voice/VLAN>Port Mode ?
Description:
Set or show the Voice VLAN port mode.
When the port mode isn't disabled, we must disable MSTP feature
before we enable Voice VLAN. It can avoid the conflict of ingress filter.

Syntax:

Voice VLAN Port Mode [<port_list>] [disable|auto|force]

Parameters:

<port_list>	Port list or 'all', default: All ports
disable	Disjoin from Voice VLAN.
auto	Enable auto detect mode. It detects whether there is VoIP phone attached on the specific port and configure the Voice VLAN members automatically.

force Forced join to Voice VLAN.
(default: Show Voice VLAN port mode)

23.11 Security

Voice/VLAN>Security ?

Description:

Set or show the Voice VLAN port security mode. When the function is enabled, all non-telephone MAC address in Voice VLAN will be blocked 10 seconds.

Syntax:

Voice VLAN Security [<port_list>] [enable|disable]

Parameters:

<port_list> Port list or 'all', default: All ports
enable Enable Voice VLAN security mode.
disable Disable Voice VLAN security mode
(default: Show flow Voice VLAN security mode)

23.12 Discovery Protocol

Voice/VLAN>Discovery Protocol ?

Description:

Set or show the Voice VLAN port discovery protocol mode.
It only work under auto detect mode is enabled.
We should enable LLDP feature before configure discovery protocol to 'LLDP' or 'Both'.
Change discovery protocol to 'OUI' or 'LLDP' will restart auto detect process.

Syntax:

Voice VLAN Discovery Protocol [<port_list>] [oui|lldp|both]

Parameters:

<port_list>	Port list or 'all', default: All ports
OUI	Detect telephony device by OUI address.
LLDP	Detect telephony device by LLDP.
Both	Both OUI and LLDP.

(default: Show Voice VLAN discovery protocol)

Chapter 24 LOOP PROTECT

24.LOOP PROTECT

Available Commands:

Loop Protect Configuration
Loop Protect Mode [enable|disable]
Loop Protect Transmit [<transmit-time>]
Loop Protect Shutdown [<shutdown-time>]
Loop Protect Port Configuration [<port_list>]
Loop Protect Port Mode [<port_list>] [enable|disable]
Loop Protect Port Action [<port_list>] [shutdown|shut_log|log]
Loop Protect Port Transmit [<port_list>] [enable|disable]
Loop Protect Status [<port_list>]

24.1 Configuration

Loop/Protect>Configuration ?

Description:

Show Loop Protection configuration.

Syntax:

Loop Protect Configuration

24.2 Mode

Loop/Protect>Mode ?

Description:

Set or show the Loop Protection mode.

Syntax:

Loop Protect Mode [enable|disable]

Parameters:

enable	Enable Loop Protection
disable	Disable Loop Protection

24.3 Transmit

Loop/Protect>Transmit ?

Description:

Set or show the Loop Protection transmit interval.

Syntax:

Loop Protect Transmit [<transmit-time>]

Parameters:

Transmit time interval (1-10 seconds)

24.4 Shutdown

Loop/Protect>Shutdown ?

Description:

Set or show the Loop Protection shutdown time.

Syntax:

Loop Protect Shutdown [<shutdown-time>]

Parameters:

Shutdown time interval (0-604800 seconds)

A value of zero disables re-enabling the port

24.5 Port Configuration

Loop/Protect>Port Configuration ?

Description:

Show Loop Protection port configuration.

Syntax:

Loop Protect Port Configuration [<port_list>]

Parameters:

<port_list>	Port list or 'all', default: All ports

24.6 Port Mode

Loop/Protect>Port Mode ?

Description:

Set or show the Loop Protection port mode.

Syntax:

Loop Protect Port Mode [<port_list>] [enable|disable]

Parameters:

<port_list>	Port list or 'all', default: All ports
enable	Enable Loop Protection
disable	Disable Loop Protection

24.7 Port Action

Loop/Protect>Port Action ?

Description:

Set or show the Loop Protection port action.

Syntax:

Loop Protect Port Action [<port_list>] [shutdown|shut_log|log]

Parameters:

<port_list>	Port list or 'all', default: All ports
shutdown	Shutdown the port
shut_log	Shutdown the port and Log event
log	(Only) Log the event

24.8 Port Transmit

Loop/Protect>Port Transmit ?

Description:

Set or show the Loop Protection port transmit mode.

Syntax:

Loop Protect Port Transmit [<port_list>] [enable|disable]

Parameters:

<port_list>	Port list or 'all', default: All ports
enable	Enable Loop Protection
disable	Disable Loop Protection

24.9 Status

Loop/Protect>Status ?

Description:

Show the Loop Protection status.

Syntax:

Loop Protect Status [<port_list>]

Parameters:

<port_list>	Port list or 'all', default: All ports

Chapter 25 IPMC

25.IPMC

Available Commands:

IPMC Configuration [mld|igmp]
IPMC Mode [mld|igmp] [enable|disable]
IPMC Flooding [mld|igmp] [enable|disable]
IPMC Leave Proxy [mld|igmp] [enable|disable]
IPMC Proxy [mld|igmp] [enable|disable]
IPMC SSM [mld|igmp] [(Range <prefix> <mask_len>)]
IPMC VLAN Add [mld|igmp] <vid>
IPMC VLAN Delete [mld|igmp] <vid>
IPMC State [mld|igmp] [<vid>] [enable|disable]
IPMC Querier [mld|igmp] [<vid>] [enable|disable]
IPMC Compatibility [mld|igmp] [<vid>] [auto|v1|v2|v3]
IPMC Fastleave [mld|igmp] [<port_list>] [enable|disable]
IPMC Throttling [mld|igmp] [<port_list>] [limit_group_number]
IPMC Filtering [mld|igmp] [<port_list>] [add|del] [group_addr]
IPMC Router [mld|igmp] [<port_list>] [enable|disable]
IPMC Status [mld|igmp] [<vid>]
IPMC Groups [mld|igmp] [<vid>]
IPMC Version [mld|igmp] [<vid>]
IPMC SFM [mld|igmp] [<vid>] [<port_list>]
IPMC Parameter RV [mld|igmp] [<vid>] [ipmc_param_rv]
IPMC Parameter QI [mld|igmp] [<vid>] [ipmc_param_qi]
IPMC Parameter QRI [mld|igmp] [<vid>] [ipmc_param_qri]
IPMC Parameter LLQI [mld|igmp] [<vid>] [ipmc_param_llqi]
IPMC Parameter URI [mld|igmp] [<vid>] [ipmc_param_uri]

25.1 Configuration

IPMC>Configuration ?
Description:
Show IPMC snooping configuration.

Syntax:

IPMC Configuration [mld|igmp]

Parameters:
mld|igmp:

mld	IPMC for IPv6 MLD
igmp	IPMC for IPv4 IGMP

25.2 Mode

IPMC>Mode ?
Description:
Set or show the IPMC snooping mode.

Syntax:

IPMC Mode [mld|igmp] [enable|disable]

Parameters:
mld|igmp:

mld	IPMC for IPv6 MLD
igmp	IPMC for IPv4 IGMP
enable	Enable IPMC snooping

disable Disable IPMC snooping
(default: Show global IPMC snooping mode)

25.3 Flooding

IPMC>Flooding ?
Description:
Set or show the IPMC unregistered addresses flooding operation.

Syntax:

IPMC Flooding [mld|igmp] [enable|disable]

Parameters:
mld|igmp:
mld IPMC for IPv6 MLD
igmp IPMC for IPv4 IGMP

enable Enable IPMC flooding
disable Disable IPMC flooding
(default: Show IPMC flooding mode)

25.4 Leave Proxy

IPMC>Leave Proxy ?
Description:
Set or show the mode of IPMC Leave Proxy.

Syntax:

IPMC Leave Proxy [mld|igmp] [enable|disable]

Parameters:
mld|igmp:
mld IPMC for IPv6 MLD

igmp IPMC for IPv4 IGMP
enable Enable IPMC Leave Proxy
disable Disable IPMC Leave Proxy
(default: Show IPMC Leave Proxy mode)

25.5 Proxy

IPMC>Proxy ?
Description:
Set or show the mode of IPMC Proxy.

Syntax:

IPMC Proxy [mld|igmp] [enable|disable]

Parameters:
mld|igmp:
mld IPMC for IPv6 MLD
igmp IPMC for IPv4 IGMP

enable Enable IPMC Proxy
disable Disable IPMC Proxy
(default: Show IPMC Proxy mode)

25.6 SSM

IPMC>SSM ?
Description:
Set or show the IPMC SSM Range.

Syntax:

IPMC SSM [mld|igmp] [(Range <prefix> <mask_len>)]

Parameters:
mld|igmp :
mld IPMC for IPv6 MLD
igmp IPMC for IPv4 IGMP

range SSM Range keyword
<prefix> IPv4/IPv6 multicast group address, accordingly
<mask_len> Mask length for IPv4(4 ~ 32)/IPv6(8 ~ 128) ssm range, accordingly

25.7 VLAN Add

IPMC>VLAN Add ?
Description:
Add the IPMC snooping VLAN interface.

Syntax:

IPMC VLAN Add [mld|igmp] <vid>

Parameters:
mld|igmp:

mld IPMC for IPv6 MLD
igmp IPMC for IPv4 IGMP

<vid> VLAN ID (1-4095)

25.8 VLAN Delete

IPMC>VLAN Delete ?

Description:

Delete the IPMC snooping VLAN interface.

Syntax:

IPMC VLAN Delete [mld|igmp] <vid>

Parameters:

mld|igmp:

mld IPMC for IPv6 MLD
igmp IPMC for IPv4 IGMP

<vid> VLAN ID (1-4095)

25.9 State

IPMC>State ?

Description:

Set or show the IPMC snooping state for VLAN.

Syntax:

IPMC State [mld|igmp] [<vid>] [enable|disable]

Parameters:

mld|igmp:

mld IPMC for IPv6 MLD
igmp IPMC for IPv4 IGMP

<vid> VLAN ID (1-4095) or 'any', default: Show all VLANs
enable Enable MLD snooping
disable Disable MLD snooping

25.10 Querier

IPMC>Querier ?

Description:

Set or show the IPMC snooping querier mode for VLAN.

Syntax:

IPMC Querier [mld|igmp] [<vid>] [enable|disable]

Parameters:

mld|igmp:
mld IPMC for IPv6 MLD
igmp IPMC for IPv4 IGMP

<vid> VLAN ID (1-4095) or 'any', default: Show all VLANs
enable Enable IPMC querier
disable Disable IPMC querier

25.11 Compatibility

IPMC>Compatibility ?

Description:

Set or show the IPMC Compatibility.

Syntax:

IPMC Compatibility [mld|igmp] [<vid>] [auto|v1|v2|v3]

Parameters:

mld|igmp :

mld IPMC for IPv6 MLD

igmp IPMC for IPv4 IGMP

<vid> VLAN ID (1-4095) or 'any', default: Show all VLANs

auto|v1|v2|v3:

auto Auto Compatibility (Default Value)

v1 Forced Compatibility of IGMPv1 or MLDv1

v2 Forced Compatibility of IGMPv2 or MLDv2

v3 Forced Compatibility of IGMPv3

(default: Show IPMC Interface Compatibility

25.12 Fastleave

IPMC>Fastleave ?

Description:

Set or show the IPMC snooping fast leave port mode.

Syntax:

IPMC Fastleave [mld|igmp] [<port_list>] [enable|disable]

Parameters:

mld|igmp :

mld IPMC for IPv6 MLD

igmp IPMC for IPv4 IGMP

<port_list> Port list or 'all', default: All ports

enable Enable IPMC fast leave

disable Disable IPMC fast leave

(default: Show IPMC fast leave mode)

25.13 Throttling

IPMC>Throttling ?

Description:

Set or show the IPMC port throttling status.

Syntax:

IPMC Throttling [mld|igmp] [<port_list>] [limit_group_number]

Parameters:

mld|igmp :

mld IPMC for IPv6 MLD

igmp IPMC for IPv4 IGMP

<port_list> Port list or 'all', default: All ports

0 No limit

1~10 Group learn limit

(default: Show IPMC Port Throttling)

25.14 Filtering

IPMC>Filtering ?

Description:

Set or show the IPMC port group filtering list.

Syntax:

IPMC Filtering [mld|igmp] [<port_list>] [add|del] [group_addr]

Parameters:

mld|igmp :

mld	IPMC for IPv6 MLD
igmp	IPMC for IPv4 IGMP

<port_list>	Port list or 'all', default: All ports
add	Add new port group filtering entry
del	Del existing port group filtering entry

(default: Show IPMC port group filtering list)

group_addr	IPv4/IPv6 multicast group address, accordingly

25.15 Router

IPMC>Router ?
Description:
Set or show the IPMC snooping router port mode.

Syntax:

IPMC Router [mld|igmp] [<port_list>] [enable|disable]

Parameters:
mld|igmp :
mld IPMC for IPv6 MLD
igmp IPMC for IPv4 IGMP

<port_list> Port list or 'all', default: All ports
enable Enable IPMC router port
disable Disable IPMC router port
(default: Show IPMC router port mode)

25.16 Status

IPMC>Status ?
Description:
Show IPMC operational status, accordingly.

Syntax:

IPMC Status [mld|igmp] [<vid>]

Parameters:
mld|igmp:

mld IPMC for IPv6 MLD
igmp IPMC for IPv4 IGMP
<vid> VLAN ID (1-4095) or 'any', default: Show all VLANs

25.17 Groups

IPMC>Groups ?

Description:

Show IPMC group addresses, accordingly.

Syntax:

IPMC Groups [mld|igmp] [<vid>]

Parameters:

mld|igmp:

mld IPMC for IPv6 MLD
igmp IPMC for IPv4 IGMP
<vid> VLAN ID (1-4095) or 'any', default: Show all VLANs

25.18 Version

IPMC>Version ?

Description:

Show IPMC Versions.

Syntax:

IPMC Version [mld|igmp] [<vid>]

Parameters:

mld|igmp:

mld IPMC for IPv6 MLD
igmp IPMC for IPv4 IGMP

<vid> VLAN ID (1-4095) or 'any', default: Show all VLANs

25.19 SFM

IPMC>SFM ?

Description:

Show SFM (including SSM) related information for IPMC.

Syntax:

IPMC SFM [mld|igmp] [<vid>] [<port_list>]

Parameters:

mld|igmp :

mld IPMC for IPv6 MLD

igmp IPMC for IPv4 IGMP

<vid> VLAN ID (1-4095) or 'any', default: Show all VLANs

<port_list> Port list or 'all', default: All ports

25.20 Parameter RV

IPMC>Parameter RV ?

Description:

Set or show the IPMC Robustness Variable.

Syntax:

IPMC Parameter RV [mld|igmp] [<vid>] [ipmc_param_rv]

Parameters:

mld|igmp :

mld IPMC for IPv6 MLD

igmp IPMC for IPv4 IGMP

<vid> VLAN ID (1-4095) or 'any', default: Show all VLANs

ipmc_param_rv:

-1 Default Value (2)

1~255 Robustness Variable

(default: Show IPMC Interface Robustness Variable

25.21 Parameter QI

IPMC>Parameter QI ?

Description:

Set or show the IPMC Query Interval.

Syntax:

IPMC Parameter QI [mld|igmp] [<vid>] [ipmc_param_qi]

Parameters:

mld|igmp :

mld IPMC for IPv6 MLD

igmp IPMC for IPv4 IGMP

<vid> VLAN ID (1-4095) or 'any', default: Show all VLANs

ipmc_param_qi:

-1 Default Value (125)

1~31744 Query Interval in seconds

(default: Show IPMC Interface Query Interval

25.22 Parameter QRI

IPMC>Parameter QRI ?

Description:

Set or show the IPMC Query Response Interval.

Syntax:

IPMC Parameter QRI [mld|igmp] [<vid>] [ipmc_param_qri]

Parameters:

mld|igmp :

mld IPMC for IPv6 MLD

igmp IPMC for IPv4 IGMP

<vid> VLAN ID (1-4095) or 'any', default: Show all VLANs

ipmc_param_qri:

-1 Default Value (100)

0~31744 Query Response Interval in tenths of seconds

(default: Show IPMC Interface Query Response Interval

25.23 Parameter LLQI

IPMC>Parameter LLQI ?

Description:

Set or show the IPMC Last Listener Query Interval.

Syntax:

IPMC Parameter LLQI [mld|igmp] [<vid>] [ipmc_param_llqi]

Parameters:

mld|igmp :

mld IPMC for IPv6 MLD

igmp IPMC for IPv4 IGMP

<vid> VLAN ID (1-4095) or 'any', default: Show all VLANs

ipmc_param_llqi:

-1 Default Value (10)

0~31744 Last Listener Query Interval in tenths of seconds

(default: Show IPMC Interface Last Listener Query Interval

25.24 Parameter URI

IPMC>Parameter URI ?

Description:

Set or show the IPMC Unsolicited Report Interval.

Syntax:

IPMC Parameter URI [mld|igmp] [<vid>] [ipmc_param_uri]

Parameters:

mld|igmp :

mld IPMC for IPv6 MLD

igmp IPMC for IPv4 IGMP

<vid> VLAN ID (1-4095) or 'any', default: Show all VLANs

ipmc_param_uri:

-1 Default Value (1)

0~31744 Unsolicited Report Interval in seconds

(default: Show IPMC Interface Unsolicited Report Interval

Chapter 26 sFlow

26.sFLOW

Available Commands:

sFlow Configuration
sFlow Receiver [release] [<timeout>] [<ip_addr_host>] [<udp_port>] [<datagram_size>]
sFlow FlowSampler [<port_list>] [<sampling_rate>] [<max_hdr_size>]
sFlow CounterPoller [<port_list>] [<interval>]
sFlow Statistics Receiver [clear]
sFlow Statistics Samplers [<port_list>] [clear]

26.1 Configuration

sFlow>Configuration ?
Description:
Show global and per port sFlow configuration.

Syntax:

sFlow Configuration

26.2 Receiver

sFlow>Receiver ?

Description:

Set or show the sFlow receiver timeout, IP address, and UDP port.

Syntax:

sFlow Receiver [release] [<timeout>] [<ip_addr_host>] [<udp_port>] [<datagram_size>]

Parameters:

release	Release the current owner of the receiver. The owner can either be "<none>" if the receiver is not currently owned by anyone, it can be "<Configured through local management>" if it's currently set up by CLI or Web, or it can be anything else if is set-up through SNMP. You can only (re-)configure the receiver if it is not currently owned by anyone or owned by CLI or Web. If this argument is specified, the remaining arguments are ignored.
<timeout>	Receiver timeout measured in seconds. The switch decrements the timeout once per second, and as long as it is non-zero, the receiver receives samples. Once the timeout reaches 0, the receiver and all its configuration is reset to defaults. Valid range is 0 - 2147483647 seconds.
<ip_addr_host>	IPv4/IPv6 address or a hostname identifying the receiver.
<udp_port>	Receiver's UDP port. Valid range is 0 - 65535. Use 0 to get default port (which is 6343).
<datagram_size>	Maximum datagram size. Valid range is 200 - 1468 bytes. Default is 1400 bytes.

26.3 FlowSampler

sFlow>FlowSampler ?

Description:

Set or show flow sampler configuration per port.
When operational,the sampling rate 'N' is rounded off to the nearest supported value.

Syntax:

sFlow FlowSampler [<port_list>] [<sampling_rate>] [<max_hdr_size>]

Parameters:

<port_list>	Port list or 'all'. Default: All ports.
<sampling_rate>	Specifies the statistical sampling rate The sample rate is specified as N to sample 1/Nth of the packets in the monitored flows. There are no restrictions on the value, but the switch will adjust it to the closest possible sampling rate. 0 disables sampling.
<max_hdr_size>	Specifies the maximum number of bytes to transmit per flow sample. Valid range is 14 - 200 bytes. Default: 128 bytes.

26.4 CounterPoller

sFlow>CounterPoller ?

Description:

Set or show counter polling interval configuration per port.

Syntax:

sFlow CounterPoller [<port_list>] [<interval>]

Parameters:

<port_list>	Port list or 'all'. Default: All ports.
<interval>	Polling interval in range 0 - 3600. Set to 0 to release this port's resources.

26.5 Statistics Receiver

sFlow>Statistics Receiver ?

Description:

Get or clear receiver statistics.

Syntax:

sFlow Statistics Receiver [clear]

Parameters:

clear	Clear statistics.

26.6 Statistics Samplers

sFlow>Statistics Samplers ?

Description:

Get or clear per-port statistics.

Syntax:

sFlow Statistics Samplers [<port_list>] [clear]

Parameters:

<port_list>	Port list or 'all'. Default: All ports.
clear	Clear statistics.

Chapter 27 VCL

27.VCL

Available Commands:

VCL Macvlan Configuration
VCL Macvlan Add <mac_addr> <vid> [<port_list>]
VCL Macvlan Del <mac_addr>
VCL Status [combined|static|nas|all]
VCL ProtoVlan Protocol Add Eth2 <ether_type>|arp|ip|ipx|at <group_id>
VCL ProtoVlan Protocol Add Snap <oui>|rfc_1042|snap_8021h <pid> <group_id>
VCL ProtoVlan Protocol Add Llc <dsap> <ssap> <group_id>
VCL ProtoVlan Protocol Delete Eth2 <ether_type>|arp|ip|ipx|at
VCL ProtoVlan Protocol Delete Snap <oui>|rfc_1042|snap_8021h <pid>
VCL ProtoVlan Protocol Delete Llc <dsap> <ssap>
VCL ProtoVlan Vlan Add [<port_list>] <group_id> <vid>
VCL ProtoVlan Vlan Delete [<port_list>] <group_id>
VCL ProtoVlan Conf
VCL IPVlan Configuration [<vce_id>]
VCL IPVlan Add [<vce_id>] <ip_addr_mask> <vid> [<port_list>]
VCL IPVlan Delete <vce_id>

27.1 Macvlan Configuration

VCL>Macvlan Configuration ?
Description:
Show VCL MAC-based VLAN configuration.

Syntax:

VCL Macvlan Configuration

27.2 Macvlan Add

VCL>Macvlan Add ?
Description:
Add or modify VCL MAC-based VLAN entry. The maximum Macvlan entries are limited to 256.

Syntax:

VCL Macvlan Add <mac_addr> <vid> [<port_list>]

Parameters:

<mac_addr>	MAC address ('xx-xx-xx-xx-xx-xx' or 'xx.xx.xx.xx.xx.xx' or 'xxxxxxxxxxxx', x is a hexadecimal digit)
<vid>	VLAN ID (1-4095)
<port_list>	Port list or 'all', default: All ports

27.3 Macvlan Del

VCL>Macvlan Del ?
Description:
Delete VCL MAC-based VLAN entry.

Syntax:

VCL Macvlan Del <mac_addr>

Parameters:
<mac_addr> MAC address ('xx-xx-xx-xx-xx-xx' or 'xx.xx.xx.xx.xx.xx' or 'xxxxxxxxxxxx', x is a hexadecimal digit)

27.4 Status

VCL>Status ?
Description:
Show VCL MAC-based VLAN users configuration.

Syntax:

VCL Status [combined|static|nas|all]

Parameters:
combined|static|nas|all VCL User

27.5 ProtoVlan Protocol Add Eth2

VCL>ProtoVlan Protocol Add Eth2 ?

Description:

Add VCL protocol-based VLAN Ethernet-II protocol to group mapping. The maximum protocol to group mappings are limited to 128.

Syntax:

VCL ProtoVlan Protocol Add Eth2 <ether_type>|arp|ip|ipx|at <group_id>

Parameters:

<ether_type>|arp|ip|ipx|at	Ether Type (0x0600 - 0xFFFF)
<group_id>	Protocol group ID

27.6 ProtoVlan Protocol Add Snap

VCL>ProtoVlan Protocol Add Snap ?

Description:

Add VCL protocol-based VLAN SNAP protocol to group mapping. The maximum protocol to group mappings are limited to 128.

Syntax:

VCL ProtoVlan Protocol Add Snap <oui>|rfc_1042|snap_8021h <pid> <group_id>

Parameters:

<oui>|rfc_1042|snap_8021h	OUI value (Hexadecimal 00-00-00 to FF-FF-FF).
<pid>	PID value (0x0-0xFFFF). If OUI is 00-00-00, valid range of PID is from 0x0600-0xFFFF.
<group_id>	Protocol group ID

27.7 ProtoVlan Protocol Add Llc

VCL>ProtoVlan Protocol Add Llc ?

Description:

Add VCL protocol-based VLAN LLC protocol to group mapping. The maximum protocol to group mappings are limited to 128.

Syntax:

VCL ProtoVlan Protocol Add Llc <dsap> <ssap> <group_id>

Parameters:

<dsap>	DSAP value (0x00-0xFF)
<ssap>	SSAP value (0x00-0xFF)
<group_id>	Protocol group ID

27.8 ProtoVlan Protocol Delete Eth2

VCL>ProtoVlan Protocol Delete Eth2 ?

Description:

Delete VCL protocol-based VLAN Ethernet-II protocol to group mapping.

Syntax:

VCL ProtoVlan Protocol Delete Eth2 <ether_type>|arp|ip|ipx|at

Parameters:

<ether_type>|arp|ip|ipx|at	Ether Type (0x0600 - 0xFFFF)

27.9 ProtoVlan Protocol Delete Snap

VCL>ProtoVlan Protocol Delete Snap ?

Description:

Delete VCL protocol-based VLAN SNAP protocol to group mapping.

Syntax:

VCL ProtoVlan Protocol Delete Snap <oui>|rfc_1042|snap_8021h <pid>

Parameters:

<oui>|rfc_1042|snap_8021h	OUI value (Hexadecimal 00-00-00 to FF-FF-FF).
<pid>	PID value (0x0-0xFFFF). If OUI is 00-00-00, valid range of PID is from 0x0600-0xFFFF.

27.10 ProtoVlan Protocol Delete Llc

VCL>ProtoVlan Protocol Delete Llc ?

Description:

Delete VCL protocol-based VLAN LLC protocol to group mapping.

Syntax:

VCL ProtoVlan Protocol Delete Llc <dsap> <ssap>

Parameters:

<dsap>: DSAP value (0x00-0xFF)

<ssap>: SSAP value (0x00-0xFF)

27.11 ProtoVlan Vlan Add

VCL>ProtoVlan Vlan Add ?

Description:

Add VCL protocol-based VLAN group to VLAN mapping. The maximum group to VLAN mappings are limited to 64.

Syntax:

VCL ProtoVlan Vlan Add [<port_list>] <group_id> <vid>

Parameters:

<port_list>	Port list or 'all', default: All ports
<group_id>	Protocol group ID
<vid>	VLAN ID (1-4095)

27.12 ProtoVlan Vlan Delete

VCL>ProtoVlan Vlan Delete ?

Description:

Delete VCL protocol-based VLAN group to VLAN mapping.

Syntax:

VCL ProtoVlan Vlan Delete [<port_list>] <group_id>

Parameters:

<port_list>	Port list or 'all', default: All ports
<group_id>	Protocol group ID

27.13 ProtoVlan Conf

VCL>ProtoVlan Conf ?
Description:
Show VCL protocol-based VLAN entries.

Syntax:

VCL ProtoVlan Conf

27.14 IPVlan Configuration

VCL>IPVlan Configuration ?
Description:
Show VCL IP Subnet-based VLAN configuration.

Syntax:

VCL IPVlan Configuration [<vce_id>]

Parameters:

<vce_id>	Unique VCE ID (1-128) for each VCL entry

27.15 IPVlan Add

VCL>IPVlan Add ?

Description:

Add or modify VCL IP Subnet-based VLAN entry. The maximum IPVlan entries are limited to 128.

Syntax:

VCL IPVlan Add [<vce_id>] <ip_addr_mask> <vid> [<port_list>]

Parameters:

<vce_id>	Unique VCE ID (1-128) for each VCL entry
<ip_addr_mask>	Source IP address and mask (Format: a.b.c.d/n).
<vid>	VLAN ID (1-4095)
<port_list>	Port list or 'all', default: All ports

27.16 IPVlan Delete

VCL>IPVlan Delete ?

Description:

Delete VCL IP Subnet-based VLAN entry.

Syntax:

VCL IPVlan Delete <vce_id>

Parameters:

<vce_id>: Unique VCE ID (1-128) for each VCL entry