KGS-1060
KGS-1060-HP

Console & Telnet

Management Interface

User's Manual

Software Rev.1.05 or up

DOC.150608

KTI Networks Inc. reserves the right to revise this documentation and to make changes in content from time to time without obligation on the part of KTI Networks Inc. to provide notification of such revision or change.

For more information, contact:

United States KTI Networks Inc.
P.O. BOX 631008
Houston, Texas 77263-1008

Phone: 713-2663891
Fax: 713-2663893
E-mail: kti@ktinet.com
URL: http://www.ktinet.com/

International Fax: 886-2-26983873
E-mail: kti@ktinet.com.tw
URL: http://www.ktinet.com.tw/

TRADEMARKS

Ethernet is a registered trademark of Xerox Corp.

Table of Contents

1. General

1.1 Start your hyperterminal

Message displayed after a successful connection:

```
Username: admin
Password:
Login in progress...
Welcome to    Command Line Interface (v1.0).
Type 'help' or '?' to get help.

>
```

1.2 General Commands

General Commands	Description
Help/?	: Get help on a group or a specific command
Up	: Move one command level up
/	: Move to Root level
Logout	: Exit CLI

1.3 Command 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
PoE	: Power Over Ethernet

QoS	: Quality of Service
Mirror	: Port mirroring
Ring	: Multi Ring Function
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
Debug	: Switch debug facilities

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. 'po co' instead of 'port configuration'.

2. System (System settings and reset options)

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

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

Description:

Show system log configuration.

Syntax:

System Log Configuration

2.3 Timezone Configuration

Description:

Show System Timezone configuration.

Syntax:

System Timezone Configuration

2.4 Version

Description:

Show system version information.

Syntax:

System Version

2.5 Log Server Mode

Description:

Set or show 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

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

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

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

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

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

Description:

Show Daylight Saving Time configuration.

Syntax:

System DST Configuration

2.12 Location

Description:

Show the system location configuration.

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

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

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

Description:

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

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

Description:

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

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

Description:

Reboot the system.

Syntax:

System Reboot

2.20 DST Offset

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

Description:

Restore factory default configuration.

Syntax:

System Restore Default [keep_ip]

Parameters:

keep_ip	: Keep IP configuration, default: Restore full configuration

2.22 Load

Description:

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

Syntax:

System Load

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

Description:

Show IP configuration.

Syntax:

IP Configuration

3.2 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

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

Description:

Ping command

Syntax:

IP Ping <ip_addr_string> [(Length <ping_length>)] [(Count <ping_count>)] [(Inter val <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

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

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

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

Description:

Set or show IPv6 address

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

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 IPv6 Ping6

Description:

Ping command for IPv6 device.

Syntax:

IP IPv6 Ping6 <ipv6_addr> [(Length <ping_length>)] [(Count <ping_count>)] [(Inte
rval <ping_interval>)]

Parameters:

<ipv6_addr>	: IPv6 host 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, 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'.
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)

3.11 NTP Configuration

Description:

Show NTP configuration.

Syntax:

IP NTP Configuration

3.12 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)

3.13 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

3.14 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'.

3.15 NTP Server Delete

Description:

Delete NTP server entry.

Syntax:

IP NTP Server Delete <server_index>

Parameters:

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

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 SFPDDM [<port_list>]

4.1 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

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

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

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

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

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

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

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

Description:

Run cable diagnostics.

Syntax:

Port VeriPHY [<port_list>]

Parameters:

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

4.10 SFPDDM

Description:

Show SFP with Digital Diagnostic Monitoring (DDM)..

Syntax:

Port SFPDDM [<port_list>]

Parameters:

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

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

Description:

Show MAC address table configuration.

Syntax:

MAC Configuration [<port_list>]

Parameters:

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

5.2 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

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

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

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

5.6 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

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

Description:

Show MAC address table statistics.

Syntax:

MAC Statistics [<port_list>]

Parameters:

Pport_list>	: Port list or 'all', default: All ports

5.9 Flush

Description:

Flush all learned entries.

Syntax:

MAC Flush

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

Description:

Show VLAN configuration.

Syntax:

VLAN Configuration [<port_list>]

Parameters:

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

6.2 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

6.3 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)

6.4 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)

6.5 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

6.6 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
unaware	: all frames are classified to the Port VLAN ID and tags are not removed.
c-port	: Customer port
s-port	: Service port
s-custom-port	: Custom Service port

6.7 EtypeCustomSport

Description:

Set or show the Custom S-port EtherType.

Syntax:

VLAN EtypeCustomSport [<etype>]

Parameters:

<etype>	: Ether Type (0x0600-0xFFFF)

6.8 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

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

Description:

Delete VLAN entry.

Syntax:

VLAN Delete <vid>|<name>

Parameters:

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

6.11 Forbidden Delete

Description:

Delete VLAN entry.

Syntax:

VLAN Forbidden Delete <vid>|<name>

Parameters:

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

6.12 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

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

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 alphabe ts or numbers. VLAN name should contain at least one alphabet.
<vid>	: VLAN ID (1-4095)

6.15 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

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

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)

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

Description:

Show Private VLAN configuration.

Syntax:

PVLAN Configuration [<port_list>]

Parameters:

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

7.2 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

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

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

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)

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 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

Description:

Show users configuration.

Syntax:

Security Switch Users Configuration

8.1.1.2 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

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 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

Description:

Show privilege configuration.

Syntax:

Security Switch Privilege Level Configuration

8.1.2.2 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

Description:

Show the current privilege level.

Syntax:

Security Switch Privilege Level Current

8.1.3 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

Description:

Show Auth configuration.

Syntax:

Security Switch Auth Configuration

8.1.3.2 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 SSH

Available Commands:

Security Switch SSH Configuration

Security Switch SSH Mode [enable|disable]

8.1.4.1 Configuration

Description:

Show SSH configuration.

Syntax:

Security Switch SSH Configuration

8.1.4.2 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 HTTPS

Available Commands:

Security Switch HTTPS Configuration

Security Switch HTTPS Mode [enable|disable]

Security Switch HTTPS Redirect [enable|disable]

8.1.5.1 Configuration

Description:

Show HTTPS configuration.

Syntax:

Security Switch HTTPS Configuration

8.1.5.2 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

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 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

Description:

Show access management configuration.

Syntax:

Security Switch Access Configuration

8.1.6.2 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

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

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/SS

8.1.6.5 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

Description:

Lookup access management entry.

Syntax:

Security Switch Access Lookup [<access_id>]

Parameters:

<access_id> : entry index (1-16)

8.1.6.7 Clear

Description:

Clear access management entry.

Syntax:

Security Switch Access Clear

8.1.6.8 Statistics

Description:

Show or clear access management statistics.

Syntax:

Security Switch Access Statistics [clear]

Parameters:

clear : Clear access management statistics

8.1.7 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

Description:

Show SNMP configuration.

Syntax:

Security Switch SNMP Configuration

8.1.7.2 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

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

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

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

Available Commands:

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>]

8.1.7.6.1 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)

8.1.7.6.2 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)

8.1.7.6.3 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)

8.1.7.6.4 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

8.1.7.6.5 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'.

8.1.7.6.6 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)

8.1.7.6.7 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)

8.1.7.6.8 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)

8.1.7.6.9 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)

8.1.7.6.10 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)

8.1.7.6.11 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)

8.1.7.6.12 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

8.1.7.6.13 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

8.1.7.7 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

8.1.7.8 Community

Available Commands:

Security Switch SNMP Configuration

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

Security Switch SNMP Community Delete <index>

Security Switch SNMP Community Lookup [<index>]

8.1.7.8.1 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

8.1.7.8.2 Delete

Description:

Delete SNMPv3 community entry.

Syntax:

Security Switch SNMP Community Delete <index>

Parameters:

<index> : entry index (1-64)

8.1.7.8.3 Lookup

Description:

Lookup SNMPv3 community entry.

Syntax:

Security Switch SNMP Community Lookup [<index>]

Parameters:

<index> : entry index (1-64)

8.1.7.9 User

Available Commands:

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>]

8.1.7.9.1 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

8.1.7.9.2 Delete

Description:

Delete SNMPv3 user entry.

Syntax:

Security Switch SNMP User Delete <index>

Parameters:

<index>	: entry index (1-64)

8.1.7.9.3 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

8.1.7.9.4 Lookup

Description:

Lookup SNMPv3 user entry.

Syntax:

Security Switch SNMP User Lookup [<index>]

Parameters:

<index>	: entry index (1-64)

8.1.7.10 Group

Available Commands:

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

Security Switch SNMP Group Delete <index>

Security Switch SNMP Group Lookup [<index>]

8.1.7.10.1 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

8.1.7.10.2 Delete

Description:

Delete SNMPv3 group entry.

Syntax:

Security Switch SNMP Group Delete <index>

Parameters:

<index> : entry index (1-64)

8.1.7.10.3 Lookup

Description:

Lookup SNMPv3 group entry.

Syntax:

Security Switch SNMP Group Lookup [<index>]

Parameters:

<index> : entry index (1-64)

8.1.7.11 View

Available Commands:

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

8.1.7.11.1 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

8.1.7.11.2 Delete

Description:
Delete SNMPv3 view entry.

Syntax:
Security Switch SNMP View Delete <index>

Parameters:

<index>	: entry index (1-64)

8.1.7.11.3 Lookup

Description:
Lookup SNMPv3 view entry.

Syntax:
Security Switch SNMP View Lookup [<index>]

Parameters:

<index>	: entry index (1-64)

8.1.7.12 Access

Available Commands:

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>]

8.1.7.12.1 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 whichthis 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

8.1.7.12.2 Delete

Description:

Delete SNMPv3 access entry.

Syntax:

Security Switch SNMP Access Delete <index>

Parameters:

<index> : entry index (1-64)

8.1.7.12.3 Lookup

Description:

Lookup SNMPv3 access entry.

Syntax:

Security Switch SNMP Access Lookup [<index>]

Parameters:

<index> : entry index (1-64)

8.1.8 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

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

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

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

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

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

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

Description:

Add 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

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

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

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

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

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 Psec

Available Commands:

Security Network Psec Switch [<port_list>]

Security Network Psec Port [<port_list>]

8.2.1.1 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

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 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

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

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

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

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

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 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

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

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 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

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

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

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

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

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

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

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

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

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

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

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

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

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 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_inspecti
on|ipmc|ip_source_guard|conflicts]
Security Network ACL Port State [<port_list>] [enable|disable]

8.2.4.1 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

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 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)

8.2.4.4 Add

Description:

Add or modify Access Control Entry (ACE).

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

8.2.4.5 Delete

Description:

Delete ACE.

Syntax:

Security Network ACL Delete <ace_id>

Parameters:

<ace_id> : ACE ID (1-256)

8.2.4.6 Lookup

Description:

Show ACE, default: All ACEs.

Syntax:

Security Network ACL Lookup [<ace_id>]

Parameters:

<ace_id> : ACE ID (1-256)

8.2.4.7 Clear

Description:

Clear all ACL counters.

Syntax:

Security Network ACL Clear

8.2.4.8 Status

Description:

Show ACL status.

Syntax:

Security Network ACL Status [combined|static|loop_protect|dhcp|upnp|arp_inspecti
on|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)

8.2.4.9 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 DHCP

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 DHCP Relay

8.2.5.1.1 Configuration

Description:

Show DHCP relay configuration.

Syntax:

Security Network DHCP Relay Configuration

8.2.5.1.2 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)

8.2.5.1.3 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

8.2.5.1.4 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)

8.2.5.1.5 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)

8.2.5.1.6 Statistics

Description:

Show or clear DHCP relay statistics.

Syntax:

Security Network DHCP Relay Statistics [clear]

Parameters:

clear : Clear DHCP relay statistics

8.2.5.2 DHCP Snooping

8.2.5.2.1 Configuration

Description:

Show DHCP snooping configuration.

Syntax:

Security Network DHCP Snooping Configuration

8.2.5.2.2 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)

8.2.5.2.3 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)

8.2.5.2.4 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 IP Source Guard

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 Configuration

Description:

Show IP source guard configuration.

Syntax:

Security Network IP Source Guard Configuration

8.2.6.2 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 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 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

8.2.6.5 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

8.2.6.6 Translation

Description:

Translate IP source guard dynamic entries into static entries.

Syntax:

Security Network IP Source Guard Translation

8.2.7 ARP Inspection

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 Configuration

Description:

Show ARP inspection configuration.

Syntax:

Security Network ARP Inspection Configuration

8.2.7.2 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 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 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 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 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

Description:

Show Auth configuration.

Syntax:

Security AAA Configuration

8.3.2 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

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

Description:

Set or show RADIUS authentication server setup.

Syntax:

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

Parameters:

<server_index> : 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

Description:

Set or show RADIUS accounting server setup.

Syntax:

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

Parameters:

<server_index>	: 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+

Description:

Set or show TACACS+ authentication server setup.

Syntax:

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

Parameters:

<server_index>	: 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

Description:

Show RADIUS statistics.

Syntax:

Security AAA Statistics [<server_index>]

Parameters:

<server_index>	: The server index (1-5)
	(default: Show statistics for all servers)

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

Description:

Show STP Bridge configuration.

Syntax:

STP Configuration

9.2 Version

Description:

Set or show the STP Bridge protocol version.

Syntax:

STP Version [<stp_version>]

Parameters:

<stp_version> : mstp|rstp|stp

9.3 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

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

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

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

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

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

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

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: disable)
(default: Show recovery timeout)

9.11 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

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

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

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

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

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

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

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

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

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

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 Port bpduGuard

Description:

Set or show the bpduGuard port parameter.

Syntax:

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

Parameters:

<stp_port_list>	: Port list or 'all'. Port zero means aggregations.
enable	: Enable port BPDU Guard
disable	: Disable port BPDU Guard

9.23 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

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

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

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

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)

10. Aggr

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

Description:

Show link aggregation configuration.

Syntax:

Aggr Configuration

10.2 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

Description:

Delete link aggregation.

Syntax:

Aggr Delete <aggr_id>

Parameters:

<aggr_id> : Aggregation ID: 1-5

10.4 Lookup

Description:

Lookup link aggregation.

Syntax:

Aggr Lookup [<aggr_id>]

Parameters:

<aggr_id> : Aggregation ID: 1-5

10.5 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

11. 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]

11.1 Configuration

Description:

Show LLDP configuration.

Syntax:

LLDP Configuration [<port_list>]

Parameters:

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

11.2 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)

11.3 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)

11.4 Interval

Description:

Set or show LLDP Tx interval.

Syntax:

LLDP Interval [<interval>]

Parameters:

<interval>	: LLDP transmission interval (5-32768)

11.5 Hold

Description:

Set or show LLDP Tx hold value.

Syntax:

LLDP Hold [<hold>]

Parameters:

<hold> : LLDP hold value (2-10)

11.6 Delay

Description:

Set or show LLDP Tx delay.

Syntax:

LLDP Delay [<delay>]

Parameters:

<delay> : LLDP transmission delay (1-8192)

11.7 Reinit

Description:

Set or show LLDP reinit delay.

Syntax:

LLDP Reinit [<reinit>]

Parameters:

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

11.8 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

11.9 Info

Description:

Show LLDP neighbor device information.

Syntax:

LLDP Info [<port_list>]

Parameters:

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

11.10 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)

12. 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>]

12.1 Configuration

Description:

Show LLDP-MED configuration.

Syntax:

LLDPMED Configuration [<port_list>]

Parameters:

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

12.2 Civic

Description:

Set or show LLDP-MED Civic Address Location.

Syntax:

LLDPMED Civic [country|state|county|city|district|block|street|leading_street_di
rection|trailing_street_suffix|str_suf|house_no|house_no_suffix|landmark|additio
nal_info|name|zip_code|building|apartment|floor|room_number|place_type|postal_co
m_name|p_o_box|additional_code] [<civic_value>]

Parameters:

country	: Country
state	: National subdivisions (state, caton, region, province, refecture)
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	: Name(residence and office occupant)
zip_code	: Postal/zip code
building	: Building (structure)
apartment	: Unit (apartment, suite)
floor	: Floor
room_number	: Room <civic_value>: lldpmed The value for the Civic Address Location entry.

12.3 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

12.4 policy delete

Description:

Delete the selected policy.

Syntax:

LLDPMED policy delete <policy_list>

Parameters:

<policy_list> : List of policies to delete

12.5 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,

tagged : The device is using tagged frames

unragged : 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.

12.6 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

12.7 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

12.8 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

12.9 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).

12.10 Info

Description:

Show LLDP-MED neighbor device information.

Syntax:

LLDPMED Info [<port_list>]

Parameters:

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

13. EEE

Available Commands:

EEE Configuration [<port_list>]

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

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

13.1 Configuration

Description:

Show EEE configuration.

Syntax:

EEE Configuration [<port_list>]

Parameters:

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

13.2 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)

13.3 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)

14. Thermal

Available Commands:

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

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

Thermal status

Thermal configuration

14.1 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

14.2 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)

14.3 status

Description:

Shows the chip temperature.

Syntax:

Thermal status

14.4 configuration

Description:

Show thermal_protect configuration.

Syntax:

Thermal configuration

15. PoE

Available Commands:

PoE Configuration [<port_list>]

PoE Mode [<port_list>] [disabled|poe|poe+]

PoE Priority [<port_list>] [low|high|critical]

PoE Mgmt_mode [class_con|class_res|al_con|al_res|lldp_res|lldp_con]

PoE Maximum_Power [<port_list>] [<port_power>]

PoE Status

PoE Primary_Supply [<supply_power>]

15.1 Configuration

Description:

Show PoE configuration.

Syntax:

PoE Configuration [<port_list>]

Parameters:

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

15.2 Mode

Description:

Set or show PoE mode.

Syntax:

PoE Mode [<port_list>] [disabled|poe|poe+]

Parameters:

<port_list>	: Port list or 'all', default: All ports
disables	: Disable PoE
poe	: Enables PoE IEEE 802.3af (Class 4 limited to 15.4W)
poe+	: Enables PoE+ IEEE 802.3at (Class 4 limited to 30W)
	(default: Show PoE's mode)

15.3 Priority

Description:

Set or show PoE mode.

Syntax:

PoE Mode [<port_list>] [disabled|poe|poe+]

Parameters:

<port_list>	: Port list or 'all', default: All ports
disables	: Disable PoE
poe	: Enables PoE IEEE 802.3af (Class 4 limited to 15.4W)
poe+	: Enables PoE+ IEEE 802.3at (Class 4 limited to 30W)
	(default: Show PoE's mode)

15.4 Mgmt_mode

Description:

Set or show PoE management mode.

Syntax:

PoE Mgmt_mode [class_con|class_res|al_con|al_res|lldp_res|lldp_con]

Parameters:

class_con	: Max. port power determined by class, and power management mode to consumption
class_res	: Max. port power determined by class, and power management mode to reserved power
al_con	: Max. port power determined by allocation, and power management mode to consumption
al_res	: Max. port power determined by allocation, and power management mode to reserved power
lldp_con	: Max. port power determined by lldp media, and power management mode to consumption
lldp_res	: Max. port power determined by lldp media, and power management mode to reserved power
	(default: Show PoE power management)

15.5 Maximum_Power

Description:

Set or show PoE maximum power per port (0-30 Watt), with one digit).

Syntax:

PoE Maximum_Power [<port_list>] [<port_power>]

Parameters:

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

<port_power> : PoE maximum power for the port (0-15.4 Watt for PoE mode, 0-30.0 Watt for PoE+ mode)

15.6 Status

Description:

Show PoE status.

Syntax:

PoE Status

15.7 Primary_Supply

Description:

Set or show the value of the primary power supply (0-2000 W), default: Show maximum primary power.

Syntax:

PoE Primary_Supply [<supply_power>]

Parameters:

<supply_power> : PoE power for a power supply

16. 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

16.1 Configuration

Description:

Show QoS Configuration.

Syntax:

QoS Configuration [<port_list>]

Parameters:

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

16.2 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)

16.3 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)

16.4 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)

16.5 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)

16.6 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)

16.7 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)

16.8 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)

16.9 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)

16.10 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)

16.11 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)

16.12 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)

16.13 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)

16.14 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)

16.15 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)

16.16 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)

16.17 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)

16.18 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)

16.19 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)

16.20 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)

16.21 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)

16.22 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)

16.23 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)

16.24 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)

16.25 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)

16.26 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)

16.27 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)

16.28 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

16.29 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)

16.30 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)

16.31 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

16.32 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

16.33 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)

16.34 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)

16.35 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)

16.36 QCL Add

Description:

Add QCE entry to QoS Control list.

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)"

16.37 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

16.38 QCL Lookup

Description:

Lookup QoS Control List.

Syntax:

QoS QCL Lookup [<qce_id>]

Parameters:

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

16.39 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)

16.40 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

17. Mirror

Available Commands:

Mirror Configuration [<port_list>]

Mirror Port [<port>|disable]

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

17.1 Configuration

Description:

Show mirror configuration.

Syntax:

Mirror Configuration [<port_list>]

Parameters:

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

17.2 Port

Description:

Set or show the mirror port.

Syntax:

Mirror Port [<port>|disable]

Parameters:

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

17.3 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)

18. Ring

Available Commands:

Ring Configuration

Ring Port [<ring_group_no>] [<ring_port_id>] [<port_no>]

Ring Backup [<ring_group_no>] [<ring_port_id>] [enable|disable]

Ring ID [<ring_group_no>] [<set_ring_id>]

Ring Status

Ring List [<ring_group_no>]

18.1 Configuration

Description:

Show Ring configuration.

Syntax:

Ring Configuration

18.2 Port

Description:

Set Ring Port.

Syntax:

Ring Port [<ring_group_no>] [<ring_port_id>] [<port_no>]

Parameters:

<ring_group_no> : ring_group_no 1 - 5

<ring_port_id> : ring_port_id 1 or 2

<port_no> : port_no 1 – 10

18.3 Backup

Description:

Set Ring Backup Port.

Syntax:

Ring Backup [<ring_group_no>] [<ring_port_id>] [enable|disable]

Parameters:

<ring_group_no> : ring_group_no 1 - 5

<ring_port_id> : ring_port_id 1 or 2
enable : Backup Port Enable
disable : Backup Port Disable

18.4 ID

Description:
Set Ring Ring ID.

Syntax:
Ring ID [<ring_group_no>] [<set_ring_id>]

Parameters:
<ring_group_no> : ring_group_no 1 - 5
<set_ring_id> : ring_id 0 – 65535

18.5 Status

Description:
Show Ring Status.

Syntax:
Ring Status

18.6 List

Description:
Show Ring List.

Syntax:
Ring List [<ring_group_no>]

Parameters:
<ring_group_no> : ring_group_no 1 – 5

19. Config

Available Commands:

Config Save <ip_server> <file_name>

Config Load <ip_server> <file_name> [check]

19.1 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

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

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

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

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

Description:

Display information about active and alternate firmware images.

Syntax:

Firmware Information

20.4 Swap

Description:

Activate the alternate firmware image..

Syntax:

Firmware Swap

21. UPnP

Available Commands:

UPnP Configuration

UPnP Mode [enable|disable]

UPnP TTL [<ttl>]

UPnP AdvertisingDuration [<duration>]

21.1 Configuration

Description:

Show UPnP configuration.

Syntax:

UPnP Configuration

21.2 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

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

Description:

Set or show UPnP Advertising Duration.

Syntax:

UPnP AdvertisingDuration [<duration>]

Parameters:

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

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

Description:

Show MVR configuration.

Syntax:

MVR Configuration

22.2 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

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

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

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)

22.6 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 VLAN ID (1-4095)
<mvr_name>	: Name (Maximum of 32 characters)
mvr_param_llqi	: 0~31744 Last Listener Query Interval in tenths of seconds
	: Default Value (5)
	(default: Show MVR Interface Last Listener Query Interval

22.7 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

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

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

Description:

Show/Clear MVR operational status.

Syntax:

MVR Status [<vid>] [clear]

Parameters:

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

22.11 Groups

Description:

Show MVR group addresses.

Syntax:

MVR Groups [<vid>]

Parameters:

<vid> : VLAN ID (1-4095)

22.12 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

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

Description:

Show Voice VLAN configuration.

Syntax:

Voice VLAN Configuration

23.2 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

Description:

Set or show Voice VLAN ID.

Syntax:

Voice VLAN ID [<vid>]

Parameters:

<vid> : VLAN ID (1-4095)

23.4 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

Description:

Set or show Voice VLAN ID.

Syntax:

Voice VLAN Traffic Class [<class>]

Parameters:

<class> : Traffic class (0-7)

23.6 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

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

Description:

Clear Voice VLAN OUI entry.

Modify OUI table will restart auto detect OUI process.

Syntax:

Voice VLAN OUI Clear

23.9 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

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

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

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)

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

Description:

Show Loop Protection configuration.

Syntax:

Loop Protect Configuration

24.2 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

Description:

Set or show the Loop Protection transmit interval.

Syntax:

Loop Protect Transmit [<transmit-time>]

Parameters:

<transmit_time> : Transmit time interval (1-10 seconds)

24.4 Shutdown

Description:

Set or show the Loop Protection shutdown time.

Syntax:

Loop Protect Shutdown [<shutdown-time>]

Parameters:

<shutdown-time> : Shutdown time interval (0-604800 seconds)
A value of zero disables re-enabling the port

24.5 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

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

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

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

Description:

Show the Loop Protection status.

Syntax:

Loop Protect Status [<port_list>]

Parameters:

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

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

Description:

Show IPMC snooping configuration.

Syntax:

IPMC Configuration [mld|igmp]

Parameters:

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

25.2 Mode

Description:

Set or show the IPMC snooping mode.

Syntax:

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

Parameters:

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

Description:

Set or show the IPMC unregistered addresses flooding operation.

Syntax:

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

Parameters:

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

Description:

Set or show the mode of IPMC Leave Proxy.

Syntax:

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

Parameters:

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

Description:

Set or show the mode of IPMC Proxy.

Syntax:

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

Parameters:

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

Description:

Set or show the IPMC SSM Range.

Syntax:

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

Parameters:

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

Description:

Add the IPMC snooping VLAN interface.

Syntax:

IPMC VLAN Add [mld|igmp] <vid>

Parameters:

mld	: IPMC for IPv6 MLD
igmp	: IPMC for IPv4 IGMP
<vid>	: VLAN ID (1-4095)

25.8 VLAN Delete

Description:

Delete the IPMC snooping VLAN interface.

Syntax:

IPMC VLAN Delete [mld|igmp] <vid>

Parameters:

mld	: IPMC for IPv6 MLD
igmp	: IPMC for IPv4 IGMP
<vid>	: VLAN ID (1-4095)

25.9 State

Description:

Set or show the IPMC snooping state for VLAN.

Syntax:

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

Parameters:

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

Description:

Set or show the IPMC snooping querier mode for VLAN.

Syntax:

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

Parameters:

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

Description:

Set or show the IPMC Compatibility.

Syntax:

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

Parameters:

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

Description:

Set or show the IPMC snooping fast leave port mode.

Syntax:

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

Parameters:

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

Description:

Set or show the IPMC port throttling status.

Syntax:

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

Parameters:

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

Description:

Set or show the IPMC port group filtering list.

Syntax:

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

Parameters:

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

Description:

Set or show the IPMC snooping router port mode.

Syntax:

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

Parameters:

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

Description:

Show IPMC operational status, accordingly.

Syntax:

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

Parameters:

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

25.17 Groups

Description:

Show IPMC group addresses, accordingly.

Syntax:

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

Parameters:

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

25.18 Version

Description:

Show IPMC Versions.

Syntax:

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

Parameters:

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

25.19 SFM

Description:

Show SFM (including SSM) related information for IPMC.

Syntax:

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

Parameters:

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

Description:

Set or show the IPMC Robustness Variable.

Syntax:

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

Parameters:

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

Description:

Set or show the IPMC Query Interval.

Syntax:

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

Parameters:

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

Description:

Set or show the IPMC Query Response Interval.

Syntax:

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

Parameters:

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

Description:

Set or show the IPMC Last Listener Query Interval.

Syntax:

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

Parameters:

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

Description:

Set or show the IPMC Unsolicited Report Interval.

Syntax:

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

Parameters:

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

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

Description:

Show global and per port sFlow configuration.

Syntax:

sFlow Configuration

26.2 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

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 samplingrate. 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

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

Description:

Get or clear receiver statistics.

Syntax:

sFlow Statistics Receiver [clear]

Parameters:

clear : Clear statistics.

26.6 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.

27. OPA

Available Commands:

OPA Configuration

OPA MinMode [<port_list>] [enable|disable]

OPA MaxMode [<port_list>] [enable|disable]

OPA Minlimit [<port_list>] [value]

OPA Maxlimit [<port_list>] [value]

27.1 Configuration

Description:

Show OPA configuration.

Syntax:

OPA Configuration

27.2 MinMode

Description:

Enable alarm if power is less than the lower threshold.

Syntax:

OPA MinMode [<port_list>] [enable|disable]

Parameters:

<port_list>	: Fiber port list or 'all', default: All ports
enable	: Enable lower threshold alarm
disable	: Disable lower threshold alarm

27.3 MaxMode

Description:

Enable alarm if power is higher than the upper threshold.

Syntax:

OPA MaxMode [<port_list>] [enable|disable]

Parameters:

<port_list>	: Fiber port list or 'all', default: All ports
enable	: Enable upper threshold alarm

disable : Disable upper threshold alarm

27.4 Minlimit

Description:

Set lower threshold power limit, unit dBm.

Syntax:

OPA Minlimit [<port_list>] [value]

Parameters:

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

range : -30 - 8.2 (dBm)

27.5 Maxlimit

Description:

Set upper threshold power limit, unit dBm.

Syntax:

OPA Maxlimit [<port_list>] [value]

Parameters:

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

range : -30 - 8.2 (dBm)

28. ALS

Available Commands:

ALS Configuration

ALS Restart [<port_list>]

ALS Restart Mode [<port_list>] [disable|manual|automatic]

ALS Restart Pulse Interval [<port_list>] [interval]

ALS Restart Pulse Width [<port_list>] [width]

Note: This function is supported in H/W Ver.E or later.

28.1 Configuration

Description:

Show ALS configuration.

Syntax:

ALS Configuration

28.2 Restart

Description:

Restart optical transmitter one test pulse in manual mode.

Syntax:

ALS Restart [<port_list>]

Parameters:

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

28.3 Restart Mode

Description:

Set transmitter restart mode.

Syntax:

ALS Restart Mode [<port_list>] [disable|manual|automatic]

Parameters:

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

disable disable ALS function

manual	Set manual mode - restart transmitter for one test pulse
automatic	Set automatic mode – restart transmitter for one test pulse every interval time

28.4 Restart Pulse Interval

Description:

Set transmitter restart interval ime in automatic mode.

Syntax:

ALS Restart Pulse Interval [<port_list>] [interval]

Parameters:

<port_list>	: Port list or 'all', default: All ports
interval	Transmitter is turned on for a short period as a test pulse every interval time (unit second) in automatic mode, range : 100 - 20000 (sec)

28.5 Restart Pulse Width

Description:

Set width of transmitter restart test pulse in manual mode and automatic mode.

Syntax:

ALS Restart Pulse Width [<port_list>] [width]

Parameters:

<port_list>	: Port list or 'all', default: All ports
width	The width of the test pulse (unit second), default 2 sec, range : 2 - 200 (sec)

Glossary

A

ACE

ACE is an acronym for Access Control Entry. It describes access permission associated with a particular ACE ID.
There are three ACE frame types (Ethernet Type, ARP, and IPv4) and two ACE actions (permit and deny). The ACE also contains many detailed, different parameter options that are available for individual application.

ACL

ACL is an acronym for Access Control List. It is the list table of ACEs, containing access control entries that specify individual users or groups permitted or denied to specific traffic objects, such as a process or a program. Each accessible traffic object contains an identifier to its ACL. The privileges determine whether there are specific traffic object access rights.
ACL implementations can be quite complex, for example, when the ACEs are prioritized for the various situation. In networking, the ACL refers to a list of service ports or network services that are available on a host or server, each with a list of hosts or servers permitted or denied to use the service. ACL can generally be configured to control inbound traffic, and in this context, they are similar to firewalls.

There are 3 web-pages associated with the manual ACL configuration:
ACL|Access Control List: The web page shows the ACEs in a prioritized way, highest (top) to lowest (bottom). Default the table is empty. An ingress frame will only get a hit on one ACE even though there are more matching ACEs. The first matching ACE will take action (permit/deny) on that frame and a counter associated with that ACE is incremented. An ACE can be associated with a Policy, 1 ingress port, or any ingress port (the whole switch). If an ACE Policy is created then that Policy can be associated with a group of ports under the "Ports" web-page. There are number of parameters that can be configured with an ACE. Read the Web page help text to get further information for each of them. The maximum number of ACEs is 64.
ACL|Ports: The ACL Ports configuration is used to assign a Policy ID to an ingress port. This is useful to group ports to obey the same traffic rules. Traffic Policy is created under the "Access Control List" - page. You can you also set

up specific traffic properties (Action / Rate Limiter / Port copy, etc) for each ingress port. They will though only apply if the frame gets past the ACE matching without getting matched. In that case a counter associated with that port is incremented. See the Web page help text for each specific port property.
ACL|Rate Limiters: Under this page you can configure the rate limiters. There can be 15 different rate limiters, each ranging from 1-1024K packets per seconds. Under "Ports" and "Access Control List" web-pages you can assign a Rate Limiter ID to the ACE(s) or ingress port(s).

AES

AES is an acronym for Advanced Encryption Standard. The encryption key protocol is applied in 802.1i standard to improve WLAN security. It is an encryption standard by the U.S. government, which will replace DES and 3DES. AES has a fixed block size of 128 bits and a key size of 128, 192, or 256 bits.

AMS

AMS is an acronym for Auto Media Select. AMS is used for dual media ports (ports supporting both copper (cu) and fiber (SFP) cables. AMS automatically determines if a SFP or a CU cable is inserted and switches to the corresponding media. If both SFP and cu cables are inserted, the port will select the prefered media.

APS

APS is an acronym for Automatic Protection Switching. This protocol is used to secure that switching is done bidirectional in the two ends of a protection group, as defined in G.8031.

Aggregation

Using multiple ports in parallel to increase the link speed beyond the limits of a port and to increase the redundancy for higher availability.
(Also *Port Aggregation*, *Link Aggregation*).

ARP

ARP is an acronym for Address Resolution Protocol. It is a protocol that used to convert an IP address into a physical address, such as an Ethernet address. ARP allows a host to communicate with other hosts when only the Internet address of its neighbors is known. Before using IP, the host sends a broadcast ARP request containing the Internet address of the desired destination system.

ARP Inspection

ARP Inspection is a secure feature. Several types of attacks can be launched against a host or devices connected to Layer 2 networks by "poisoning" the ARP caches. This feature is used to block such attacks. Only valid ARP

requests and responses can go through the switch device.

Auto-Negotiation

Auto-negotiation is the process where two different devices establish the mode of operation and the speed settings that can be shared by those devices for a link.

C

CC

CC is an acronym for Continuity Check. It is a MEP functionality that is able to detect loss of continuity in a network by transmitting CCM frames to a peer MEP.

CCM

CCM is an acronym for Continuity Check Message. It is a OAM frame transmitted from a MEP to it's peer MEP and used to implement CC functionality.

CDP

CDP is an acronym for Cisco Discovery Protocol.

CIST

Within MSTP network, ISTs in different regions are interconnected through a common spanning tree (CST). The collection of the ISTs in each MST region, and the common spanning tree that interconnects the MST regions and single spanning trees are called the common and internal spanning tree (CIST).

D

DDM

Modern optical SFP transceivers support digital diagnostics monitoring (DDM) functions according to the industry-standard SFF-8472. This feature is also known as digital optical monitoring (DOM). Modules with this capability give the end user the ability to monitor parameters of the SFP, such as optical output power, optical input power, temperature, laser bias current, and transceiver supply voltage, in real time.

DEI

DEI is an acronym for Drop Eligible Indicator. It is a 1-bit field in the VLAN tag.

DES

DES is an acronym for Data Encryption Standard. It provides a complete description of a mathematical algorithm for encrypting (enciphering) and decrypting (deciphering) binary coded information.

Encrypting data converts it to an unintelligible form called cipher. Decrypting cipher converts the data back to its original form called plaintext. The

algorithm described in this standard specifies both enciphering and deciphering operations which are based on a binary number called a key.

DHCP

DHCP is an acronym for Dynamic Host Configuration Protocol. It is a protocol used for assigning dynamic IP addresses to devices on a network. DHCP used by networked computers (clients) to obtain IP addresses and other parameters such as the default gateway, subnet mask, and IP addresses of DNS servers from a DHCP server.

The DHCP server ensures that all IP addresses are unique, for example, no IP address is assigned to a second client while the first client's assignment is valid (its lease has not expired). Therefore, IP address pool management is done by the server and not by a human network administrator.

Dynamic addressing simplifies network administration because the software keeps track of IP addresses rather than requiring an administrator to manage the task. This means that a new computer can be added to a network without the hassle of manually assigning it a unique IP address.

DHCP Relay

DHCP Relay is used to forward and to transfer DHCP messages between the clients and the server when they are not on the same subnet domain.

The DHCP option 82 enables a DHCP relay agent to insert specific information into a DHCP request packets when forwarding client DHCP packets to a DHCP server and remove the specific information from a DHCP reply packets when forwarding server DHCP packets to a DHCP client. The DHCP server can use this information to implement IP address or other assignment policies. Specifically the option works by setting two sub-options: Circuit ID (option 1) and Remote ID (option2). The Circuit ID sub-option is supposed to include information specific to which circuit the request came in on. The Remote ID sub-option was designed to carry information relating to the remote host end of the circuit.

The definition of Circuit ID in the switch is 4 bytes in length and the format is "vlan_id" "module_id" "port_no". The parameter of "vlan_id" is the first two bytes represent the VLAN ID. The parameter of "module_id" is the third byte for the module ID (in standalone switch it always equal 0, in stackable switch it means switch ID). The parameter of "port_no" is the fourth byte and it means the port number.

The Remote ID is 6 bytes in length, and the value is equal the DHCP relay agents MAC address.

DHCP Snooping

DHCP Snooping is used to block intruder on the untrusted ports of the switch device when it tries to intervene by injecting a bogus DHCP reply packet to a legitimate conversation between the DHCP client and server.

DNS

DNS is an acronym for Domain Name System. It stores and associates many types of information with domain names. Most importantly, DNS translates human-friendly domain names and computer hostnames into computer-friendly IP addresses. For example, the domain name www.example.com might translate to 192.168.0.1.

DoS

DoS is an acronym for Denial of Service. In a denial-of-service (DoS) attack, an attacker attempts to prevent legitimate users from accessing information or services. By targeting at network sites or network connection, an attacker may be able to prevent network users from accessing email, web sites, online accounts (banking, etc.), or other services that rely on the affected computer.

Dotted Decimal Notation

Dotted Decimal Notation refers to a method of writing IP addresses using decimal numbers and dots as separators between octets.
An IPv4 dotted decimal address has the form x.y.z.w, where x, y, z, and w are decimal numbers between 0 and 255.

Drop Precedence Level

Every incoming frame is classified to a Drop Precedence Level (DP level), which is used throughout the device for providing congestion control guarantees to the frame according to what was configured for that specific DP level. A DP level of 0 (zero) corresponds to 'Committed' (Green) frames and a DP level of 1 or higher corresponds to 'Discard Eligible' (Yellow) frames.

DSCP

DSCP is an acronym for Differentiated Services Code Point. It is a field in the header of IP packets for packet classification purposes.

E

EEE

EEE is an abbreviation for Energy Efficient Ethernet defined in IEEE 802.3az.

EPS

EPS is an abbreviation for Ethernet Protection Switching defined in ITU/T G.8031.

Ethernet Type

Ethernet Type, or EtherType, is a field in the Ethernet MAC header, defined by the Ethernet networking standard. It is used to indicate which protocol is being

transported in an Ethernet frame.

F

FTP

FTP is an acronym for File Transfer Protocol. It is a transfer protocol that uses the Transmission Control Protocol (TCP) and provides file writing and reading. It also provides directory service and security features.

Fast Leave

Multicast snooping Fast Leave processing allows the switch to remove an interface from the forwarding-table entry without first sending out group specific queries to the interface. The VLAN interface is pruned from the multicast tree for the multicast group specified in the original leave message. Fast-leave processing ensures optimal bandwidth management for all hosts on a switched network, even when multiple multicast groups are in use simultaneously. This processing applies to IGMP and MLD.

H

HTTP

HTTP is an acronym for Hypertext Transfer Protocol. It is a protocol that used to transfer or convey information on the World Wide Web (WWW).
HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands. For example, when you enter a URL in your browser, this actually sends an HTTP command to the Web server directing it to fetch and transmit the requested Web page. The other main standard that controls how the World Wide Web works is HTML, which covers how Web pages are formatted and displayed. Any Web server machine contains, in addition to the Web page files it can serve, an HTTP daemon, a program that is designed to wait for HTTP requests and handle them when they arrive. The Web browser is an HTTP client, sending requests to server machines. An HTTP client initiates a request by establishing a Transmission Control Protocol (TCP) connection to a particular port on a remote host (port 80 by default). An HTTP server listening on that port waits for the client to send a request message.

HTTPS

HTTPS is an acronym for Hypertext Transfer Protocol over Secure Socket Layer. It is used to indicate a secure HTTP connection.
HTTPS provide authentication and encrypted communication and is widely used on the World Wide Web for security-sensitive communication such as payment transactions and corporate logons.
HTTPS is really just the use of Netscape's Secure Socket Layer (SSL) as a

sublayer under its regular HTTP application layering. (HTTPS uses port 443 instead of HTTP port 80 in its interactions with the lower layer, TCP/IP.) SSL uses a 40-bit key size for the RC4 stream encryption algorithm, which is considered an adequate degree of encryption for commercial exchange.

I

ICMP

ICMP is an acronym for Internet Control Message Protocol. It is a protocol that generated the error response, diagnostic or routing purposes. ICMP messages generally contain information about routing difficulties or simple exchanges such as time-stamp or echo transactions. For example, the PING command uses ICMP to test an Internet connection.

IEEE 802.1X

IEEE 802.1X is an IEEE standard for port-based Network Access Control. It provides authentication to devices attached to a LAN port, establishing a point-to-point connection or preventing access from that port if authentication fails. With 802.1X, access to all switch ports can be centrally controlled from a server, which means that authorized users can use the same credentials for authentication from any point within the network.

IGMP

IGMP is an acronym for Internet Group Management Protocol. It is a communications protocol used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships. It is an integral part of the IP multicast specification, like ICMP for unicast connections. IGMP can be used for online video and gaming, and allows more efficient use of resources when supporting these uses.

IGMP Querier

A router sends IGMP Query messages onto a particular link. This router is called the Querier.

IMAP

IMAP is an acronym for Internet Message Access Protocol. It is a protocol for email clients to retrieve email messages from a mail server.

IMAP is the protocol that IMAP clients use to communicate with the servers, and SMTP is the protocol used to transport mail to an IMAP server.

The current version of the Internet Message Access Protocol is IMAP4. It is similar to Post Office Protocol version 3 (POP3), but offers additional and more complex features. For example, the IMAP4 protocol leaves your email messages on the server rather than downloading them to your computer. If you

wish to remove your messages from the server, you must use your mail client to generate local folders, copy messages to your local hard drive, and then delete and expunge the messages from the server.

IP

IP is an acronym for Internet Protocol. It is a protocol used for communicating data across an internet network.

IP is a "best effort" system, which means that no packet of information sent over is assured to reach its destination in the same condition it was sent. Each device connected to a Local Area Network (LAN) or Wide Area Network (WAN) is given an Internet Protocol address, and this IP address is used to identify the device uniquely among all other devices connected to the extended network.

The current version of the Internet protocol is IPv4, which has 32-bits Internet Protocol addresses allowing for in excess of four billion unique addresses. This number is reduced drastically by the practice of webmasters taking addresses in large blocks, the bulk of which remain unused. There is a rather substantial movement to adopt a new version of the Internet Protocol, IPv6, which would have 128-bits Internet Protocol addresses. This number can be represented roughly by a three with thirty-nine zeroes after it. However, IPv4 is still the protocol of choice for most of the Internet.

IPv6

IPv6, which would have 128-bits Internet Protocol addresses. This number can be represented roughly by a three with thirty-nine zeroes after it. However, IPv4 is still the protocol of choice for most of the Internet.

IPMC

IPMC is an acronym for IP MultiCast.

IPMC supports IPv4 and IPv6 multicasting. IPMCv4 denotes multicast for IPv4. IPMCv6 denotes multicast for IPv6.

IP Source Guard

IP Source Guard is a secure feature used to restrict IP traffic on DHCP snooping untrusted ports by filtering traffic based on the DHCP Snooping Table or manually configured IP Source Bindings. It helps prevent IP spoofing attacks when a host tries to spoof and use the IP address of another host.

L

LACP

LACP is an IEEE 802.3ad standard protocol. The Link Aggregation Control Protocol, allows bundling several physical ports together to form a single logical port.

LLC

The IEEE 802.2 Logical Link Control (LLC) protocol provides a link mechanism for upper layer protocols. It is the upper sub-layer of the Data Link Layer and provides multiplexing mechanisms that make it possible for several network protocols (IP, IPX) to coexist within a multipoint network. LLC header consists of 1 byte DSAP (Destination Service Access Point), 1 byte SSAP (Source Service Access Point), 1 or 2 bytes Control field followed by LLC information.

LLDP

LLDP is an IEEE 802.1ab standard protocol.

The Link Layer Discovery Protocol(LLDP) specified in this standard allows stations attached to an IEEE 802 LAN to advertise, to other stations attached to the same IEEE 802 LAN, the major capabilities provided by the system incorporating that station, the management address or addresses of the entity or entities that provide management of those capabilities, and the identification of the stations point of attachment to the IEEE 802 LAN required by those management entity or entities. The information distributed via this protocol is stored by its recipients in a standard Management Information Base (MIB), making it possible for the information to be accessed by a Network Management System (NMS) using a management protocol such as the Simple Network Management Protocol (SNMP).

LLDP-MED

LLDP-MED is an extension of IEEE 802.1ab and is defined by the telecommunication industry association (TIA-1057).

LLQI

LLQI (Last Listener Query Interval) is the maximun response time used to calculate the Maximun Respse Code inserted into Specific Queries. It is used to detect the departure of the last listener for a multicast address or source. In IGMP, this term is called LMQI (Last Member Query Interval).

LOC

LOC is an acronym for Loss Of Connectivity and is detected by a MEP and is indicating lost connectivity in the network. Can be used as a switch criteria by EPS

M

MAC Table

Switching of frames is based upon the DMAC address contained in the frame. The switch builds up a table that maps MAC addresses to switch ports for knowing which ports the frames should go to (based upon the DMAC address

in the frame). This table contains both static and dynamic entries. The static entries are configured by the network administrator if the administrator wants to do a fixed mapping between the DMAC address and switch ports.
The frames also contain a MAC address (SMAC address), which shows the MAC address of the equipment sending the frame. The SMAC address is used by the switch to automatically update the MAC table with these dynamic MAC addresses. Dynamic entries are removed from the MAC table if no frame with the corresponding SMAC address have been seen after a configurable age time.

MEP

MEP is an acronym for Maintenance Entity Endpoint and is an endpoint in a Maintenance Entity Group (ITU-T Y.1731).

MD5

MD5 is an acronym for Message-Digest algorithm 5. MD5 is a message digest algorithm, used cryptographic hash function with a 128-bit hash value. It was designed by Ron Rivest in 1991. MD5 is officially defined in RFC 1321 - The MD5 Message-Digest Algorithm.

Mirroring

For debugging network problems or monitoring network traffic, the switch system can be configured to mirror frames from multiple ports to a mirror port. (In this context, mirroring a frame is the same as copying the frame.)
Both incoming (source) and outgoing (destination) frames can be mirrored to the mirror port.

MLD

MLD is an acronym for Multicast Listener Discovery for IPv6. MLD is used by IPv6 routers to discover multicast listeners on a directly attached link, much as IGMP is used in IPv4. The protocol is embedded in ICMPv6 instead of using a separate protocol.

MSTP

In 2002, the IEEE introduced an evolution of RSTP: the Multiple Spanning Tree Protocol. The MSTP protocol provides for multiple spanning tree instances, while ensuring RSTP and STP compatibility. The standard was originally defined by IEEE 802.1s, but was later incorporated in IEEE 802.1D-2005.

MSTI

It may be necessary to have different topologies for different VLANs, for load-sharing or other purposes. MSTP enables the grouping of multiple VLANs with the same topology requirements into one MST instance (MSTI).

Instances are not supported in STP or RSTP, so those two versions have the same spanning-tree in common for all of the VLANs.

MVR

Multicast VLAN Registration (MVR) is a protocol for Layer 2 (IP)-networks that enables multicast-traffic from a source VLAN to be shared with subscriber-VLANs.

The main reason for using MVR is to save bandwidth by preventing duplicate multicast streams being sent in the core network, instead the stream(s) are received on the MVR-VLAN and forwarded to the VLANs where hosts have requested it/them(Wikipedia).

N

NAS

NAS is an acronym for Network Access Server. The NAS is meant to act as a gateway to guard access to a protected source. A client connects to the NAS, and the NAS connects to another resource asking whether the client's supplied credentials are valid. Based on the answer, the NAS then allows or disallows access to the protected resource. An example of a NAS implementation is IEEE 802.1X.

NetBIOS

NetBIOS is an acronym for Network Basic Input/Output System. It is a program that allows applications on separate computers to communicate within a Local Area Network (LAN), and it is not supported on a Wide Area Network (WAN).

The NetBIOS giving each computer in the network both a NetBIOS name and an IP address corresponding to a different host name, provides the session and transport services described in the Open Systems Interconnection (OSI) model.

NFS

NFS is an acronym for Network File System. It allows hosts to mount partitions on a remote system and use them as though they are local file systems.

NFS allows the system administrator to store resources in a central location on the network, providing authorized users continuous access to them, which means NFS supports sharing of files, printers, and other resources as persistent storage over a computer network.

NTP

NTP is an acronym for Network Time Protocol, a network protocol for synchronizing the clocks of computer systems. NTP uses UDP (datagrams) as

transport layer.

O

OAM

OAM is an acronym for Operation Administration and Maintenance.
It is a protocol described in ITU-T Y.1731 used to implement carrier ethernet functionality. MEP functionality like CC and RDI is based on this

Optional TLVs.

A LLDP frame contains multiple TLVs
For some TLVs it is configurable if the switch shall include the TLV in the LLDP frame. These TLVs are known as optional TLVs. If an optional TLVs is disabled the corresponding information is not included in the LLDP frame.

OUI

OUI is the organizationally unique identifier. An OUI address is a globally unique identifier assigned to a vendor by IEEE. You can determine which vendor a device belongs to according to the OUI address which forms the first 24 bits of a MAC address.

P

PCP

PCP is an acronym for Priority Code Point. It is a 3-bit field storing the priority level for the 802.1Q frame. It is also known as User Priority.

PD

PD is an acronym for Powered Device. In a PoE system the power is delivered from a PSE (power sourcing equipment) to a remote device. The remote device is called a PD.

PHY

PHY is an abbreviation for Physical Interface Transceiver and is the device that implement the Ethernet physical layer (IEEE-802.3).

PING

PINGv6

PING is a program that sends a series of packets over a network or the Internet to a specific computer in order to generate a response from that computer. The other computer responds with an acknowledgment that it received the packets. Ping was created to verify whether a specific computer on a network or the Internet exists and is connected.
ping uses Internet Control Message Protocol (ICMP) packets. The PING Request is the packet from the origin computer, and the PING Reply is the packet response from the target.

PoE

PoE is an acronym for Power Over Ethernet.

Power Over Ethernet is used to transmit electrical power, to remote devices over standard Ethernet cable. It could for example be used for powering IP telephones, wireless LAN access points and other equipment, where it would be difficult or expensive to connect the equipment to main power supply.

Policer

A policer can limit the bandwidth of received frames. It is located in front of the ingress queue.

POP3

POP3 is an acronym for Post Office Protocol version 3. It is a protocol for email clients to retrieve email messages from a mail server.

POP3 is designed to delete mail on the server as soon as the user has downloaded it. However, some implementations allow users or an administrator to specify that mail be saved for some period of time. POP can be thought of as a "store-and-forward" service.

An alternative protocol is Internet Message Access Protocol (IMAP). IMAP provides the user with more capabilities for retaining e-mail on the server and for organizing it in folders on the server. IMAP can be thought of as a remote file server.

POP and IMAP deal with the receiving of e-mail and are not to be confused with the Simple Mail Transfer Protocol (SMTP). You send e-mail with SMTP, and a mail handler receives it on your recipient's behalf. Then the mail is read using POP or IMAP. IMAP4 and POP3 are the two most prevalent Internet standard protocols for e-mail retrieval. Virtually all modern e-mail clients and servers support both.

PPPoE

PPPoE is an acronym for Point-to-Point Protocol over Ethernet.

It is a network protocol for encapsulating Point-to-Point Protocol (PPP) frames inside Ethernet frames. It is used mainly with ADSL services where individual users connect to the ADSL transceiver (modem) over Ethernet and in plain Metro Ethernet networks (Wikipedia).

Private VLAN

In a private VLAN, PVLANs provide layer 2 isolation between ports within the same broadcast domain. Isolated ports configured as part of PVLAN cannot communicate with each other. Member ports of a PVLAN can communicate with each other.

PTP

PTP is an acronym for Precision Time Protocol, a network protocol for

synchronizing the clocks of computer systems.

Q

QCE

QCE is an acronym for QoS Control Entry. It describes QoS class associated with a particular QCE ID.

There are six QCE frame types: Ethernet Type, VLAN, UDP/TCP Port, DSCP, TOS, and Tag Priority. Frames can be classified by one of 4 different QoS classes: "Low", "Normal", "Medium", and "High" for individual application.

QCL

QCL is an acronym for QoS Control List. It is the list table of QCEs, containing QoS control entries that classify to a specific QoS class on specific traffic objects.

Each accessible traffic object contains an identifier to its QCL. The privileges determine specific traffic object to specific QoS class.

QL

QL In SyncE this is the Quality Level of a given clock source. This is received on a port in a SSM indicating the quality of the clock received in the port.

QoS

QoS is an acronym for Quality of Service. It is a method to guarantee a bandwidth relationship between individual applications or protocols.

A communications network transports a multitude of applications and data, including high-quality video and delay-sensitive data such as real-time voice. Networks must provide secure, predictable, measurable, and sometimes guaranteed services.

Achieving the required QoS becomes the secret to a successful end-to-end business solution. Therefore, QoS is the set of techniques to manage network resources.

QoS class

Every incoming frame is classified to a QoS class, which is used throughout the device for providing queuing, scheduling and congestion control guarantees to the frame according to what was configured for that specific QoS class. There is a one to one mapping between QoS class, queue and priority. A QoS class of 0 (zero) has the lowest priority.

R

RARP

RARP is an acronym for Reverse Address Resolution Protocol. It is a protocol that is used to obtain an IP address for a given hardware address, such as an Ethernet address. RARP is the complement of ARP.

RADIUS

RADIUS is an acronym for Remote Authentication Dial In User Service. It is a networking protocol that provides centralized access, authorization and accounting management for people or computers to connect and use a network service.

RDI

RDI is an acronym for Remote Defect Indication. It is a OAM functionality that is used by a MEP to indicate defect detected to the remote peer MEP

RMON

Remote Monitoring (RMON) is a standard monitoring specification that enables various network monitors and console systems to exchange network-monitoring data. RMON provides network administrators with more freedom in selecting network-monitoring probes and consoles with features that meet their particular networking needs. An RMON implementation typically operates in a client/server model. Monitoring devices (commonly called "probes" in this context) contain RMON software agents that collect information and analyze packets. These probes act as servers and the Network Management applications that communicate with them act as clients. While both agent configuration and data collection use SNMP, RMON is designed to operate differently than other SNMP-based systems:

Router Port

A router port is a port on the Ethernet switch that leads switch towards the Layer 3 multicast device.

RSTP

In 1998, the IEEE with document 802.1w introduced an evolution of STP: the Rapid Spanning Tree Protocol, which provides for faster spanning tree convergence after a topology change. Standard IEEE 802.1D-2004 now incorporates RSTP and obsoletes STP, while at the same time being backwards-compatible with STP.

S

SAMBA

Samba is a program running under UNIX-like operating systems that provides seamless integration between UNIX and Microsoft Windows machines. Samba acts as file and print servers for Microsoft Windows, IBM OS/2, and other SMB client machines. Samba uses the Server Message Block (SMB) protocol and Common Internet File System (CIFS), which is the underlying protocol used in Microsoft Windows networking.

Samba can be installed on a variety of operating system platforms, including

Linux, most common Unix platforms, OpenVMS, and IBM OS/2.
Samba can also register itself with the master browser on the network so that it would appear in the listing of hosts in Microsoft Windows "Neighborhood Network".

SFP

The small form-factor pluggable (SFP) is a compact, hot-pluggable transceiver used for both telecommunication and data communications applications. The form factor and electrical interface are specified by a multi-source agreement (MSA). It interfaces a network device motherboard (for a switch, router, media converter or similar device) to a fiber optic or copper networking cable. It is a popular industry format jointly developed and supported by many network component vendors. SFP transceivers are designed to support SONET, Gigabit Ethernet, Fibre Channel, and other communications standards.

sFlow

sFlow is an industry standard technology for monitoring switched networks through random sampling of packets on switch ports and time-based sampling of port counters. The sampled packets and counters (referred to as flow samples and counter samples, respectively) are sent as sFlow UDP datagrams to a central network traffic monitoring server. This central server is called an sFlow receiver or sFlow collector.
Additional information can be found at http://sflow.org.

SHA

SHA is an acronym for Secure Hash Algorithm. It designed by the National Security Agency (NSA) and published by the NIST as a U.S. Federal Information Processing Standard. Hash algorithms compute a fixed-length digital representation (known as a message digest) of an input data sequence (the message) of any length.

Shaper

A shaper can limit the bandwidth of transmitted frames. It is located after the ingress queues.

SMTP

SMTP is an acronym for Simple Mail Transfer Protocol. It is a text-based protocol that uses the Transmission Control Protocol (TCP) and provides a mail service modeled on the FTP file transfer service. SMTP transfers mail messages between systems and notifications regarding incoming mail.

SNAP

The SubNetwork Access Protocol (SNAP) is a mechanism for multiplexing, on networks using IEEE 802.2 LLC, more protocols than can be distinguished

by the 8-bit 802.2 Service Access Point (SAP) fields. SNAP supports identifying protocols by Ethernet type field values; it also supports vendor-private protocol identifier.

SNMP

SNMP is an acronym for Simple Network Management Protocol. It is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol for network management. SNMP allow diverse network objects to participate in a network management architecture. It enables network management systems to learn network problems by receiving traps or change notices from network devices implementing SNMP.

SNTP

SNTP is an acronym for Simple Network Time Protocol, a network protocol for synchronizing the clocks of computer systems. SNTP uses UDP (datagrams) as transport layer.

SPROUT

Stack Protocol using ROUting Technology. An advanced protocol for almost instantaneous discovery of topology changes within a stack as well as election of a master switch. SPROUT also calculates parameters for setting up each switch to perform shortest path forwarding within the stack.

SSID

Service Set Identifier is a name used to identify the particular 802.11 wireless LANs to which a user wants to attach. A client device will receive broadcast messages from all access points within range advertising their SSIDs, and can choose one to connect to based on pre-configuration, or by displaying a list of SSIDs in range and asking the user to select one (wikipedia).

SSH

SSH is an acronym for Secure SHell. It is a network protocol that allows data to be exchanged using a secure channel between two networked devices. The encryption used by SSH provides confidentiality and integrity of data over an insecure network. The goal of SSH was to replace the earlier rlogin, TELNET and rsh protocols, which did not provide strong authentication or guarantee confidentiality (Wikipedia).

SSM

SSM In SyncE this is an abbreviation for Synchronization Status Message and is containing a QL indication.

STP

Spanning Tree Protocol is an OSI layer-2 protocol which ensures a loop free topology for any bridged LAN. The original STP protocol is now obsolete by

RSTP.

Switch ID

Switch IDs (1-?) are used to uniquely identify the switches within a stack. The Switch ID of each switch is shown on the display on the front of the switch and is used widely in the web pages as well as in the CLI commands.

SyncE

SyncE Is an abbreviation for Synchronous Ethernet. This functionality is used to make a network 'clock frequency' synchronized. Not to be confused with real time clock synchronized (IEEE 1588).

T

TACACS+

TACACS+ is an acronym for Terminal Acess Controller Access Control System Plus. It is a networking protocol which provides access control for routers, network access servers and other networked computing devices via one or more centralized servers. TACACS+ provides separate authentication, authorization and accounting services.

Tag Priority

Tag Priority is a 3-bit field storing the priority level for the 802.1Q frame.

TCP

TCP is an acronym for Transmission Control Protocol. It is a communications protocol that uses the Internet Protocol (IP) to exchange the messages between computers.

The TCP protocol guarantees reliable and in-order delivery of data from sender to receiver and distinguishes data for multiple connections by concurrent applications (for example, Web server and e-mail server) running on the same host.

The applications on networked hosts can use TCP to create connections to one another. It is known as a connection-oriented protocol, which means that a connection is established and maintained until such time as the message or messages to be exchanged by the application programs at each end have been exchanged. TCP is responsible for ensuring that a message is divided into the packets that IP manages and for reassembling the packets back into the complete message at the other end.

Common network applications that use TCP include the World Wide Web (WWW), e-mail, and File Transfer Protocol (FTP).

TELNET

TELNET is an acronym for TELetype NETwork. It is a terminal emulation protocol that uses the Transmission Control Protocol (TCP) and provides a

virtual connection between TELNET server and TELNET client.
TELNET enables the client to control the server and communicate with other servers on the network. To start a Telnet session, the client user must log in to a server by entering a valid username and password. Then, the client user can enter commands through the Telnet program just as if they were entering commands directly on the server console.

TFTP

TFTP is an acronym for Trivial File Transfer Protocol. It is transfer protocol that uses the User Datagram Protocol (UDP) and provides file writing and reading, but it does not provide directory service and security features.

ToS

ToS is an acronym for Type of Service. It is implemented as the IPv4 ToS priority control. It is fully decoded to determine the priority from the 6-bit ToS field in the IP header. The most significant 6 bits of the ToS field are fully decoded into 64 possibilities, and the singular code that results is compared against the corresponding bit in the IPv4 ToS priority control bit (0~63).

TLV

TLV is an acronym for Type Length Value. A LLDP frame can contain multiple pieces of information. Each of these pieces of information is known as TLV.

TKIP

TKIP is an acronym for Temporal Key Integrity Protocol. It used in WPA to replace WEP with a new encryption algorithm. TKIP comprises the same encryption engine and RC4 algorithm defined for WEP. The key used for encryption in TKIP is 128 bits and changes the key used for each packet.

U

UDP

UDP is an acronym for User Datagram Protocol. It is a communications protocol that uses the Internet Protocol (IP) to exchange the messages between computers.
UDP is an alternative to the Transmission Control Protocol (TCP) that uses the Internet Protocol (IP). Unlike TCP, UDP does not provide the service of dividing a message into packet datagrams, and UDP doesn't provide reassembling and sequencing of the packets. This means that the application program that uses UDP must be able to make sure that the entire message has arrived and is in the right order. Network applications that want to save processing time because they have very small data units to exchange may prefer UDP to TCP.

UDP provides two services not provided by the IP layer. It provides port numbers to help distinguish different user requests and, optionally, a checksum capability to verify that the data arrived intact.

Common network applications that use UDP include the Domain Name System (DNS), streaming media applications such as IPTV, Voice over IP (VoIP), and Trivial File Transfer Protocol (TFTP).

UPnP

UPnP is an acronym for Universal Plug and Play. The goals of UPnP are to allow devices to connect seamlessly and to simplify the implementation of networks in the home (data sharing, communications, and entertainment) and in corporate environments for simplified installation of computer components

User Priority

User Priority is a 3-bit field storing the priority level for the 802.1Q frame. It is also known as PCP.

V

VLAN

Virtual LAN. A method to restrict communication between switch ports. VLANs can be used for the following applications:

VLAN unaware switching: This is the default configuration. All ports are VLAN unaware with Port VLAN ID 1 and members of VLAN 1. This means that MAC addresses are learned in VLAN 1, and the switch does not remove or insert VLAN tags.

VLAN aware switching: This is based on the IEEE 802.1Q standard. All ports are VLAN aware. Ports connected to VLAN aware switches are members of multiple VLANs and transmit tagged frames. Other ports are members of one VLAN, set up with this Port VLAN ID, and transmit untagged frames.

Provider switching: This is also known as Q-in-Q switching. Ports connected to subscribers are VLAN unaware, members of one VLAN, and set up with this unique Port VLAN ID. Ports connected to the service provider are VLAN aware, members of multiple VLANs, and set up to tag all frames. Untagged frames received on a subscriber port are forwarded to the provider port with a single VLAN tag. Tagged frames received on a subscriber port are forwarded to the provider port with a double VLAN tag.

VLAN ID

VLAN ID is a 12-bit field specifying the VLAN to which the frame belongs.

Voice VLAN

Voice VLAN is VLAN configured specially for voice traffic. By adding the

ports with voice devices attached to voice VLAN, we can perform QoS-related configuration for voice data, ensuring the transmission priority of voice traffic and voice quality.

W

WEP

WEP is an acronym for Wired Equivalent Privacy. WEP is a deprecated algorithm to secure IEEE 802.11 wireless networks. Wireless networks broadcast messages using radio, so are more susceptible to eavesdropping than wired networks. When introduced in 1999, WEP was intended to provide confidentiality comparable to that of a traditional wired network (Wikipedia).

WiFi

WiFi is an acronym for Wireless Fidelity. It is meant to be used generically when referring of any type of 802.11 network, whether 802.11b, 802.11a, dual-band, etc. The term is promulgated by the Wi-Fi Alliance.

WPA

WPA is an acronym for Wi-Fi Protected Access. It was created in response to several serious weaknesses researchers had found in the previous system , Wired Equivalent Privacy (WEP). WPA implements the majority of the IEEE 802.11i standard, and was intended as an intermediate measure to take the place of WEP while 802.11i was prepared. WPA is specifically designed to also work with pre-WPA wireless network interface cards (through firmware upgrades), but not necessarily with first generation wireless access points. WPA2 implements the full standard, but will not work with some older network cards (Wikipedia).

WPA-PSK

WPA-PSK is an acronym for Wi-Fi Protected Access - Pre Shared Key. WPA was designed to enhance the security of wireless networks. There are two flavors of WPA: enterprise and personal. Enterprise is meant for use with an IEEE 802.1X authentication server, which distributes different keys to each user. Personal WPA utilizes less scalable 'pre-shared key' (PSK) mode, where every allowed computer is given the same passphrase. In PSK mode, security depends on the strength and secrecy of the passphrase. The design of WPA is based on a Draft 3 of the IEEE 802.11i standard (Wikipedia)

WPA-Radius

WPA-Radius is an acronym for Wi-Fi Protected Access - Radius (802.1X authentication server). WPA was designed to enhance the security of wireless networks. There are two flavors of WPA: enterprise and personal. Enterprise is meant for use with an IEEE 802.1X authentication server, which distributes

different keys to each user. Personal WPA utilizes less scalable 'pre-shared key' (PSK) mode, where every allowed computer is given the same passphrase. In PSK mode, security depends on the strength and secrecy of the passphrase. The design of WPA is based on a Draft 3 of the IEEE 802.11i standard (Wikipedia)

WPS

WPS is an acronym for Wi-Fi Protected Setup. It is a standard for easy and secure establishment of a wireless home network. The goal of the WPS protocol is to simplify the process of connecting any home device to the wireless network (Wikipedia).

WRED

WRED is an acronym for Weighted Random Early Detection. It is an active queue management mechanism that provides preferential treatment of higher priority frames when traffic builds up within a queue. A frame's DP level is used as input to WRED. A higher DP level assigned to a frame results in a higher probability that the frame is dropped during times of congestion.

WTR

WTR is an acronym for Wait To Restore. This is the time a fail on a resource has to be 'not active' before restoration back to this (previously failing) resource is done.