KGS-2422

Console & Telnet

Management Interface

User's Manual

DOC.120313

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 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

1.2 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
IGMP	: Internet Group Management Protocol snooping
LACP	: Link Aggregation Control Protocol
LLDP	: Link Layer Discovery Protocol
LLDPMED	: Link Layer Discovery Protocol Media
QoS	: Quality of Service
Mirror	: Port mirroring
Config	: Load/Save of configuration via TFTP
Firmware	: Download of firmware via TFTP

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_list>]**

System **Name [<name>]**

System **Contact [<contact>]**

System **Location [<location>]**

System **Timezone [<offset>]**

System **Reboot**

System **Restore Default [keep_ip]**

System **Load**

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

2.1 Configuration

System> Configuration help

Description:

Show system configuration.

Syntax:

System Configuration [all] [<port_list>]

Parameters:

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

2.2 Name

System> Name help

Description:

Set or show the system name.

Syntax:

System Name [<name>]

Parameters:

<name>	: System name string. Use 'clear' or "" to clear the string System name is a text string drawn from the alphabet (A-Za-z), digits (0-9), minus sign (-).

Note: In CLI, 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.

2.3 Contact

System>Contact help

Description:

Set or show the system contact.

Syntax:

System Contact [<contact>]

Parameters:

<contact> : System contact string. Use 'clear' or "" to clear the string
Note: No blank or space characters are permitted as part of a contact.(only in CLI)

2.4 Location

System> Location help

Description:

Set or show the system location.

Syntax:

System Location [<location>]

Parameters:

<location> : System location string. Use 'clear' or "" to clear the string
Note: In CLI, no blank or space characters are permitted as part of a contact.

2.5 Timezone

System>Timezone help

Description:

Set or show the system time zone offset.

Syntax:

System Timezone [<offset>]

Parameters:

<offset> : Time zone offset in minutes (-720 to 720) relative to UTC

2.6 Reboot

System> Reboot help

Description:

Reboot the system.

Syntax:

System Reboot

2.7 Restore Default

System>Restore Default help

Description:

Restore factory default configuration.

Syntax:

System Restore Default [keep_ip]

Parameters:

keep_ip : Keep IP configuration, default: Restore full configuration

2.8 Load

System>Load help

Description:

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

Syntax:

System Load

2.9 Log

System>Log help

Description:

Show or clear the system log.

Syntax:

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

Parameters:

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

3. IP (IP configuration and Ping)

Available Commands:

IP **Configuration**

IP **DHCP [enable|disable]**

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

IP **Ping <ip_addr_string> [<ping_length>]**

IP **SNTP [<ip_addr_string>]**

3.1 Configuration

IP> Configuration help

Description:

Show IP configuration.

Syntax:

IP Configuration

3.2 DHCP

IP> DHCP help

Description:

Set or show the DHCP client mode.

Syntax:

IP DHCP [enable|disable]

Parameters:

enable	: Enable or renew DHCP client
disable	: Disable DHCP client

3.3 Setup

IP> Setup help

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

3.4 Ping

IP>Ping help

Description:

Ping IP address (ICMP echo).

Syntax:

IP Ping <ip_addr_string> [<ping_length>]

Parameters:

<ip_addr_string>	: IP host address (a.b.c.d)
<ping_length>	: Ping data length (8-1400), excluding MAC, IP and ICMP header

3.5 SNTP

IP>SNTP help

Description:

Set or show the SNTP Time server address.

Syntax:

IP SNTP [<ip_addr_string>]

Parameters:

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

4. Port (Port management)

Available Commands:

Port **Configuration [<port_list>]**

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

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>]**

4.1 Configuration

Port> Configuration help

Description:

Show port configuration.

Syntax:

Port Configuration [<port_list>]

Parameters:

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

4.2 Mode

Port> Mode help

Description:

Set or show the port speed and duplex mode.

Syntax:

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

Parameters:

<port_list>	: Port list or 'all', default: All ports
10hdx	: 10 Mbps, half duplex (Not support for fiber port)
10fdx	: 10 Mbps, full duplex (Not support for fiber port)
100hdx	: 100 Mbps, half duplex (Not support for fiber port)
100fdx	: 100 Mbps, full duplex

1000fdx : 1 Gbps, full duplex (Not support for fiber port)

auto : Auto negotiation of speed and duplex

(default: Show configured and current mode)

4.3 FlowControl

Port> FlowControl help

Description:

Set or show the port flow control mode.

Syntax:

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

Parameters:

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

enable : Enable flow control

disable : Disable flow control

(default: Show flow control mode)

4.4 State

Port> State help

Description:

Set or show the port administrative state.

Syntax:

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

Parameters:

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

enable : Enable port

disable : Disable port

(default: Show administrative mode)

4.5 MaxFrame

Port>MaxFrame help

Description:

Set or show the port maximum frame size.

Syntax:

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

Parameters:

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

<max_frame> : Port maximum frame size (1518-9600),

(default: Show maximum frame size)

4.6 Power

Port>Power help

Description:

Set or show the port PHY power mode.

Syntax:

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

Parameters:

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

enable : Enable all power control

disable : Disable all power control

actiphy : Enable ActiPHY power control

dynamic : Enable Dynamic power control

4.7 Excessive

Port>Excessive help

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 back-off algorithm after 16 collisions

(default: Show mode)

4.8 Statistics

Port>Statistics help

Description:

Show port statistics.

Syntax:

Port Statistics [<port_list>] [<command>]

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
low	: Show low priority statistics
normal	: Show normal priority statistics
medium	: Show medium priority statistics
high	: Show high priority statistics

(default: Show all port statistics)

5. MAC (MAC address table)

Available Commands:

MAC **Configuration [<port_list>]**

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

MAC **Delete <mac_addr> [<vid>]**

MAC **Lookup <mac_addr> [<vid>]**

MAC **Agetime [<age_time>]**

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

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

MAC **Statistics [<port_list>]**

MAC **Flush**

5.1 Configuration

MAC>Configuration help

Description:

Show MAC address table configuration.

Syntax:

MAC Configuration [<port_list>]

Parameters:

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

5.2 Add

MAC>Add help

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)

<port_list> : Port list or 'all' or 'none'

<vid> : VLAN ID (1-4095), default: 1

5.3 Delete

MAC>Delete help

Description:

Delete MAC address entry.

Syntax:

MAC Delete <mac_addr> [<vid>]

Parameters:

<mac_addr>	: MAC address (xx-xx-xx-xx-xx-xx)
<vid>	: VLAN ID (1-4095), default: 1

5.4 Lookup

MAC>Lookup help

Description:

Lookup MAC address entry.

Syntax:

MAC Lookup <mac_addr> [<vid>]

Parameters:

<mac_addr>	: MAC address (xx-xx-xx-xx-xx-xx)
<vid>	: VLAN ID (1-4095), default: 1

5.5 Agetime

MAC>Agetime help

Description:

Set or show the MAC address age timer.

Syntax:

MAC Agetime [<age_time>]

Parameters:

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

5.6 Learning

MAC>Learning help

Description:

Set or show the port learn mode.

Syntax:

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

Parameters:

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

(default: Show learn mode)

5.7 Dump

MAC>Dump help

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), default: MAC address zero
<vid>	: First VLAN ID (1-4095), default: 1

5.8 Statistics

MAC>Statistics help

Description:

Show MAC address table statistics.

Syntax:

MAC Statistics [<port_list>]

Parameters:

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

5.9 Flush

MAC>Flush help

Description:

Flush all learned entries.

Syntax:

MAC Flush

6. VLAN (Virtual LAN)

Available Commands:

VLAN **Configuration [<port_list>]**

VLAN **Aware [<port_list>] [enable|disable]**

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

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

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

VLAN **Add <vid> [<port_list>]**

VLAN **Delete <vid>**

VLAN **Lookup [<vid>]**

VLAN **Status [<port_list>] [combined|static|nas|mstp|all|conflicts]**

6.1 Configuration

VLAN>Configuration help

Description:

Show VLAN configuration.

Syntax:

VLAN Configuration [<port_list>]

Parameters:

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

6.2 Aware

VLAN>Aware help

Description:

Set or show the port VLAN awareness.

Syntax:

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

Parameters:

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

enable : Enable VLAN awareness

disable : Disable VLAN awareness

(default: Show VLAN awareness)

6.3 PVID

VLAN>PVID help

Description:

Set or show the port VLAN ID.

Syntax:

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

Parameters:

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

6.4 FrameType

VLAN>FrameType help

Description:

Set or show the port VLAN frame type.

Syntax:

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

Parameters:

<port_list>	: Port list or 'all', default: All ports
all	: Allow tagged and untagged frames
tagged	: Allow tagged frames only

(default: Show accepted frame types)

6.5 IngressFilter

VLAN> IngressFilter help

Description:

Set or show the port VLAN ingress filter..

Syntax:

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

Parameters:

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

enable : Enable VLAN ingress filtering

disable : Disable VLAN ingress filtering

(default: Show VLAN ingress filtering)

6.6 Add

VLAN>Add help

Description:

Add or modify VLAN entry.

Syntax:

VLAN Add <vid> [<port_list>]

Parameters:

<vid> : VLAN ID (1-4095)

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

6.7 Delete

VLAN>Delete help

Description:

Delete VLAN entry.

Syntax:

VLAN Delete <vid>

Parameters:

<vid> : VLAN ID (1-4095)

6.8 Lookup

VLAN>Lookup help

Description:

Lookup VLAN entry.

Syntax:

VLAN Lookup [<vid>]

Parameters:

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

6.9 Status

VLAN> Status help

Description:

VLAN Port Configuration Status

Syntax:

VLAN Status [<port_list>] [combined|static|nas|mstp|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
mstp	: MSTP port configuration
all	: All VLAN Users configuration

(default: combined VLAN Users configuration)

7. PVLAN (Private VLAN)

Available Commands:

PVLAN **Configuration [<port_list>]**

PVLAN **Add <pvlan_id> [<port_list>]**

PVLAN **Delete <pvlan_id>**

PVLAN **Lookup [<pvlan_id>]**

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

7.1 Configuration

PVLAN>Configuration help

Description:

Show Private VLAN configuration.

Syntax:

PVLAN Configuration [<port_list>]

Parameters:

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

7.2 Add

PVLAN>Add help

Description:

Add or modify Private VLAN entry.

Syntax:

PVLAN Add <pvlan_id> [<port_list>]

Parameters:

<pvlan_id> : Private VLAN ID

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

7.3 Delete

PVLAN>Delete help

Description:

Delete Private VLAN entry.

Syntax:

PVLAN Delete <pvlan_id>

Parameters:

<pvlan_id> : Private VLAN ID

7.4 Lookup

PVLAN>Lookup help

Description:

Lookup Private VLAN entry.

Syntax:

PVLAN Lookup [<pvlan_id>]

Parameters:

<pvlan_id> : Private VLAN ID, default: Show all PVLANs

7.5 Isolate

PVLAN>Isolate help

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 (Security management)

Available Command groups:

Switch: Switch security

Network: Network security

AuthServer: Authentication server configuration

8.1 Switch (Switch security)

Available command groups:

Security Switch **Password** : System password

Security Switch **Auth** : Authentication

Security Switch **SSH** : Secure Shell

Security Switch **HTTPS** : Hypertext Transfer Protocol over Secure Socket Layer

Security Switch **SNMP** : Simple Network Management Protocol

8.1.1 Password

Available Command:

Security / Switch > Password help

Description:

Set the system password.

Syntax:

Security Switch Password <password>

Parameters:

<password> : System password string, Use 'clear' or "" to clear the string

8.1.2 Auth (Authentication)

Available Commands:

Security Switch Auth **Configuration**

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

8.1.2.1 Configuration

Security / Switch /Auth> Configuration help

Description:

Show Auth configuration.

Syntax:

Security Switch Auth Configuration

8.1.2.2 Method

Security / Switch /Auth> Method help

Description:

Set or show Auth method.

Syntax:

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

Parameters:

console	: Settings for console
telnet	: Settings for telnet
ssh	: Settings for ssh
web	: Settings for web
none	: Authentication disabled
local	: Use local authentication
radius	: Use remote RADIUS authentication
	(default: Show client authentication method)
enable	: Enable local authentication if remote authentication fails
disable	: Disable local authentication if remote authentication fails
	(default: Show backup client authentication configuration)

8.1.3 SSH(Secure Shell)

Available Commands:

Security Switch SSH **Configuration**

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

8.1.3.1 Configuration

Security / Switch /SSH> Configuration help

Description:

Show SSH configuration.

Syntax:

Security Switch SSH Configuration

8.1.3.2 Mode [enable|disable]

Security / Switch / SSH > Mode help

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)

8.1.4 HTTPS (Hypertext Transfer Protocol over Secure Socket Layer)

Available Commands:

Security Switch HTTPS **Configuration**

Security Switch HTTPS **Mode [enable|disable]**

Security Switch HTTPS **Redirect [enable|disable]**

8.1.4.1 Configuration

Security / Switch / HTTPS > Configuration help

Description:

Show HTTPS configuration.

Syntax:

Security Switch HTTPS Configuration

8.1.4.2 Mode

Security / Switch / HTTPS > Mode help

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)

8.1.4.3 Redirect

Security / Switch / HTTPS > Redirect help

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)

8.1.5 SNMP (Simple Network Management Protocol)

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 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>]**

8.1.5.1 Configuration

Security / Switch / SNMP>Configuration help

Description:

Show SNMP configuration.

Syntax:

Security Switch SNMP Configuration

8.1.5.2 Mode

Security / Switch / SNMP>Mode help

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)

8.1.5.3 Version

Security / Switch / SNMP>Version help

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)

8.1.5.4 Read Community

Security / Switch / SNMP>Read Community help

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

(default: Show SNMP read community)

8.1.5.5 Write Community

Security / Switch / SNMP>Write Community help

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

(default: Show SNMP write community)

8.1.5.6 Trap Mode

Security / Switch / SNMP>Trap Mode help

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)

8.1.5.7 Trap Version

Security / Switch / SNMP>Trap Version help

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)

8.1.5.8 Trap Community

Security / Switch / SNMP>Trap Community help

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

(default: Show SNMP trap community)

8.1.5.9 Trap Destination

Security / Switch / SNMP>Trap Destination help

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)

8.1.5.10 Trap Authentication Failure

Security / Switch / SNMP>Trap Authentication Failure help

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)

8.1.5.11 Trap Link-up

Security / Switch / SNMP>Trap Link-up help

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)

8.1.5.12 Trap Inform Mode

Security / Switch / SNMP>Trap Inform Mode help

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)

8.1.5.13 Trap Inform Timeout

Security / Switch / SNMP>Trap Inform Timeout help

Description:

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

Syntax:

Security Switch SNMP Trap Inform Timeout [<timeout>]

Parameters:

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

(default: Show SNMP trap inform timeout)

8.1.5.14 Trap Inform Retry Times

Security / Switch / SNMP>Trap Inform Retry Times help

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)

8.1.5.15 Trap Probe Security Engine ID

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

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)

8.1.5.16 Trap Security Engine ID

Security / Switch / SNMP>Trap Security Engine ID help

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

8.1.5.17 Trap Security Name

Security / Switch / SNMP>Trap Security Name help

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)

8.1.5.18 Engine ID

Security / Switch / SNMP>Engine ID help

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

8.1.5.19 Community Add

Security / Switch / SNMP>Community Add help

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> : IP subnet mask (a.b.c.d), default: Show IP mask

8.1.5.20 Community Delete

Security / Switch / SNMP>Community Delete help

Description:

Delete SNMPv3 community entry.

Syntax:

Security Switch SNMP Community Delete <index>

Parameters:

<index> : entry index (1-64)

8.1.5.21 Community Lookup

Security / Switch / SNMP>Community Lookup help

Description:

Lookup SNMPv3 community entry.

Syntax:

Security Switch SNMP Community Lookup [<index>]

Parameters:

<index> : entry index (1-64)

8.1.5.22 User Add

Security / Switch / SNMP>User Add help

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 *md5*: An optional flag to indicate that this user using MD5 authentication protocol *sha*: An optional flag to indicate that this user using SHA authentication protocol
<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
<priv_password>	: A string identifying the privacy pass phrase

8.1.5.23 User Delete

Security / Switch / SNMP>User Delete help

Description:

Delete SNMPv3 user entry.

Syntax:

Security Switch SNMP User Delete <index>

Parameters:

<index> : entry index (1-64)

8.1.5.24 User Changekey

Security / Switch / SNMP>User Changekey help

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

<auth_password> : A string identifying the authentication pass phrase

<priv_password> : A string identifying the privacy pass phrase

8.1.5.25 User Lookup

Security / Switch / SNMP>User Lookup help

Description:

Lookup SNMPv3 user entry

Syntax:

Security Switch SNMP User Lookup [<index>]

Parameters:

<index> : entry index (1-64)

8.1.5.26 Group Add

Security / Switch / SNMP>Group Add help

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
<group_name>	: A string identifying the group name that this entry should belong to

8.1.5.27 Group Delete

Security / Switch / SNMP>Group Delete help

Description:

Delete SNMPv3 group entry.

Syntax:

Security Switch SNMP Group Delete <index>

Parameters:

<index>	: entry index (1-64)

8.1.5.28 Group Lookup

Security / Switch / SNMP>Group Lookup help

Description:

Lookup SNMPv3 group entry.

Syntax:

Security Switch SNMP Group Lookup [<index>]

Parameters:

<index>	: entry index (1-64)

8.1.5.29 View Add

Security / Switch / SNMP>View Add help

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
	included: Flag to indicate that this view subtree should included
	excluded: Flag to indicate that this view subtree should excluded
<oid_subtree>	: The OID defining the root of the subtree to add to the named vie

8.1.5.30 View Delete

Security / Switch / SNMP>View Delete help

Description:

Delete SNMPv3 view entry.

Syntax:

Security Switch SNMP View Delete <index>

Parameters:

<index>	: entry index (1-64)

8.1.5.31 View Lookup

Security / Switch / SNMP>View Lookup help

Description:

Lookup SNMPv3 view entry.

Syntax:

Security Switch SNMP View Lookup [<index>]

Parameters:

<index>	: entry index (1-64)

8.1.5.32 Access Add

Security / Switch / SNMP>Access Add help

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
<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
<write_view_name>	: The name of the MIB view defining the MIB objects for which this request may potentially SET new values

8.1.5.33 Access Delete

Security / Switch / SNMP>Access Delete help

Description:

Delete SNMPv3 access entry.

Syntax:

Security Switch SNMP Access Delete <index>

Parameters:

<index>	: entry index (1-64)

8.1.5.34 Access Lookup [<index>]

Security / Switch / SNMP>Access Lookup help

Description:

Lookup SNMPv3 access entry.

Syntax:

Security Switch SNMP Access Lookup [<index>]

Parameters:

<index> : entry index (1-64)

8.2 Network (Network security)

Available command groups:

Security Network **Psec** : Port Security Status

Security Network **NAS** : Network Access Server (IEEE 802.1X)

Security Network **ACL** : Access Control List

8.2.1 Psec (Port Security Status)

Available Commands:

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

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

8.2.1.1 Switch

Security / Network / Psec>Switch help

Description:

Show Port Security status.

Syntax:

Security Network Psec Switch [<port_list>]

Parameters:

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

8.2.1.2 Port

Security / Network / Psec>Port help

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 NAS (Network Access Server - IEEE 802.1X)

Available Commands:

Security Network NAS **Configuration [<port_list>]**

Security Network NAS **Mode [enable|disable]**

Security Network NAS **State [<port_list>] [auto|authorized|unauthorized|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 **Authenticate [<port_list>] [now]**

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

8.2.2.1 Configuration

Security / Network / NAS> Configuration help

Description:

Show 802.1X configuration.

Syntax:

Security Network NAS Configuration [<port_list>]

Parameters:

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

8.2.2.2 Mode

Security / Network / NAS > Mode help

Description:

Set or show the global NAS enabledness.

Syntax:

Security Network NAS Mode [enable|disable]

Parameters:

enable : Globally enable 802.1X

disable : Globally disable 802.1X

(default: Show current 802.1X global enabledness)

8.2.2.3 State

Security / Network / NAS > State help

Description:

Set or show the port security state.

Syntax:

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

macbased : Switch authenticates on behalf of the client

(default: Show 802.1X state)

8.2.2.4 Reauthentication

Security / Network / NAS > Reauthentication help

Description:

Set or show Reauthentication enabledness.

Syntax:

Security Network NAS Reauthentication [enable|disable]

Parameters:

enable : Enable reauthentication

disable : Disable reauthentication

(default: Show current reauthentication mode)

8.2.2.5 ReauthPeriod

Security / Network / NAS > ReauthPeriod help

Description:

Set or show the period between reauthentications.

Syntax:

Security Network NAS ReauthPeriod [<reauth_period>]

Parameters:

<reauth_period> : Period between reauthentications (1-3600 seconds)

(default: Show current reauthentication period)

8.2.2.6 EapolTimeout

Security / Network / NAS > EapolTimeout help

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)

8.2.2.7 Agetime

Security / Network / NAS > Agetime help

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 for activity on a MAC address that succeeded authentication

(default: Show current age time)

8.2.2.8 Holdtime

Security / Network / NAS > Holdtime help

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> : Hold time before MAC addresses that failed authentication expire

(default: Show current hold time)

8.2.2.9 Authenticate

Security / Network / NAS > Authenticate help

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 re-authentication immediately

8.2.2.10 Statistics

Security / Network / NAS > Statistics help

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)

8.2.3 ACL (Access Control List)

Available Commands:

Security Network ACL **Configuration [<port_list>]**

Security Network ACL **Action [<port_list>] [permit|deny] [<rate_limiter>][<port_copy>] [<logging>] [<shutdown>]**

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

Security Network ACL **Rate [<rate_limiter_list>] [<packet_rate>]**

Security Network ACL **Add [<ace_id>] [<ace_id_next>][switch | (port <port>) | (policy <policy>)][<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_copy>] [<logging>] [<shutdown>]**

Security Network ACL **Delete <ace_id>**

Security Network ACL **Lookup [<ace_id>]**

Security Network ACL **Clear**

Security Network ACL **Status [combined|static|conflicts]**

8.2.3.1 Configuration

Security / Network / ACL > Configuration help

Description:

Show ACL Configuration.

Syntax:

Security Network ACL Configuration [<port_list>]

Parameters:

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

8.2.3.2 Action

Security / Network / ACL > Action help

Description:

Set or show the ACL port default action.

Syntax:

Security Network ACL Action [<port_list>] [permit|deny] [<rate_limiter>]

[<port_copy>] [<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_copy>	: Port number for copy of frames or 'disable'
<logging>	: System logging of frames: *log* | *log_disable*
<shutdown>	: Shut down ingress port: *shut* | *shut_disable*

8.2.3.3 Policy

Security / Network / ACL > Policy help

Description:

Set or show the ACL port policy.

Syntax:

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

Parameters:

<port_list>	: Port list or 'all', default: All ports
<policy>	: Policy number (1-8)

8.2.3.4 Rate

Security / Network / ACL > Rate help

Description:

Set or show the ACL rate limiter.

Syntax:

Security Network ACL Rate [<rate_limiter_list>] [<packet_rate>]

Parameters:

<rate_limiter_list>	: Rate limiter list (1-15), default: All rate limiters
<packet_rate>	: Rate in pps (1, 2, 4, ..., 512, 1k, 2k, 4k, ..., 1024k)

8.2.3.5 Add

Security / Network / ACL > Add help

Description:

Add or modify Access Control Entry (ACE).

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

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

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

Syntax:

Security Network ACL Add [<ace_id>] [<ace_id_next>] [switch | (port <port>) | (policy <policy>)] [<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_copy>] [<logging>] [<shutdown>]

Parameters:

<ace_id>	: ACE ID (1-128), default: Next available ID
<ace_id_next>	: Next ACE ID (1-128), default: Add ACE last
switch	: Switch ACE keyword
port	: Port ACE keyword
<port>	: Port number
policy	: Policy ACE keyword
<policy>	: Policy number (1-8)
<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 or 'any'
<smac>	: Source MAC address (xx-xx-xx-xx-xx-xx) or 'any'
<dmac>	: Destination MAC address (xx-xx-xx-xx-xx-xx) 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_copy> : Port number for copy of frames or 'disable'
<logging> : System logging of frames: log|log_disable
<shutdown> : Shut down ingress port: shut|shut_disable

8.2.3.6 Delete

Security / Network / ACL > Delete help

Description:

Delete ACE.

Syntax:

Security Network ACL Delete <ace_id>

Parameters:

<ace_id> : ACE ID (1-128)

8.2.3.7 Lookup

Security / Network / ACL > Lookup help

Description:

Show ACE, default: All ACEs.

Syntax:

Security Network ACL Lookup [<ace_id>]

Parameters:

<ace_id> : ACE ID (1-128)

8.2.3.8 Clear

Security / Network / ACL > Clear help

Description:

Clear all ACL counters.

Syntax:

Security Network ACL Clear

8.2.3.9 Status

Security / Network / ACL > Status help

Description:

Show ACL status.

Syntax:

Security Network ACL Status [combined|static|conflicts]

Parameters:

combined : Shows the combined status

static : Shows the static user configured status

conflicts : Shows all conflict status

(default: Shows the combined status)

8.3 AuthServer (Authentication Server Configuration)

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 Statistics [<server_index>]

8.3.1 Configuration

Security / AAA > Configuration help

Description:

Show Auth configuration.

Syntax:

Security AAA Configuration

8.3.2 Timeout

Security / AAA > Timeout help

Description:

Set or show server timeout.

Syntax:

Security AAA Timeout [<timeout>]

Parameters:

<timeout> : Server response timeout (3-3600 seconds)

(default: Show server timeout configuration)

8.3.3 Deadtime

Security / AAA > Deadtime help

Description:

Set or show server dead time.

Syntax:

Security AAA Deadtime [<dead_time>]

Parameters:

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

(default: Show server dead time configuration)

8.3.4 RADIUS

Security / AAA > RADIUS help

Description:

Set or show RADIUS authentication server setup.

Syntax:

Security AAA RADIUS [<server_index>] [enable|disable] [<ip_addr_string>] [<secre
t>] [<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)
<secret>	: Secret shared with external authentication server.
	To set an empty secret, use two quotes ("").
	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 Statistics

Security / AAA > Statistics help

Description:

Show RADIUS statistics.

Syntax:

Security AAA Statistics [<server_index>]

Parameters:

<server_index>	: The server index (1-5)
(default: Show RADIUS authentication server statistics)	

9. STP (Spanning Tree Protocol)

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>] [<port_list>]**

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

STP **Msti Map [<msti>] [clear]**

STP **Msti Add <msti> <vid>**

STP **Port Configuration [<port_list>]**

STP **Port Mode [<port_list>] [enable|disable]**

STP **Port Edge [<port_list>] [enable|disable]**

STP **Port AutoEdge [<port_list>] [enable|disable]**

STP **Port P2P [<port_list>] [enable|disable|auto]**

STP **Port RestrictedRole [<port_list>] [enable|disable]**

STP **Port RestrictedTcn [<port_list>] [enable|disable]**

STP **Port bpduGuard [<port_list>] [enable|disable]**

STP **Port Statistics [<port_list>]**

STP **Port Mcheck [<port_list>]**

STP **Msti Port Configuration [<msti>] [<port_list>]**

STP **Msti Port Cost [<msti>] [<port_list>] [<path_cost>]**

STP **Msti Port Priority [<msti>] [<port_list>] [<priority>]**

9.1 Configuration

STP>Configuration help

Description:

Show STP Bridge configuration.

Syntax:

STP Configuration

9.2 Version

STP>Version help

Description:

Set or show the STP Bridge protocol version.

Syntax:

STP Version [<stp_version>]

Parameters:

<stp_version>: mstp|rstp|stp

9.3 Txhold

STP>Txhold help

Description:

Set or show the STP Bridge Transmit Hold Count parameter.

Syntax:

STP Txhold [<holdcount>]

Parameters:

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

9.4 MaxHops

STP>MaxHops help

Description:

Set or show the MSTP Bridge Max Hop Count parameter.

Syntax:

STP MaxHops [<maxhops>]

Parameters:

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

9.5 MaxAge

STP>MaxAge help

Description:

Set or show the CIST/MSTI bridge maximum age.

Syntax:

STP MaxAge [<max_age>]

Parameters:

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

9.6 FwdDelay

STP>FwdDelay help

Description:

Set or show the CIST/MSTI bridge forward delay.

Syntax:

STP FwdDelay [<delay>]

Parameters:

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

9.7 CName

STP>CName help

Description:

Set or show MSTP configuration name and revision.

Syntax:

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

Parameters:

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

<integer> : Integer value

9.8 bpduFilter

STP>bpduFilter help

Description:

Set or show edge port BPDU Filtering.

Syntax:

STP bpduFilter [enable|disable]

Parameters:

enable|disable : enable or disable BPDU Filtering for Edge ports

9.9 bpduGuard

STP>bpduGuard help

Description:

Set or show edge port BPDU Guard.

Syntax:

STP bpduGuard [enable|disable]

Parameters:

enable|disable : enable or disable BPDU Guard for Edge ports

9.10 recovery

STP>recovery help

Description:

Set or show edge port error recovery timeout.

Syntax:

STP recovery [<timeout>]

Parameters:

<timeout> : Time before error-disabled ports are re-enabled (30-86400 seconds, 0 disables)

(default: Show recovery timeout)

9.11 Status

STP>Status help

Description:

Show STP Bridge status.

Syntax:

STP Status [<msti>] [<port_list>]

Parameters:

<msti>	: STP bridge instance no (0-7, CIST=0, MSTI1=1, ...)
<port_list>	: Port list or 'all', default: All ports

9.12 Msti Priority

STP>Msti Priority help

Description:

Set or show the CIST/MSTI bridge priority.

Syntax:

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

Parameters:

<msti>	: STP bridge instance no (0-7, CIST=0, MSTI1=1, ...)
<priority>	: STP bridge priority (0/16/32/48/.../224/240)

9.13 Msti Map

STP>Msti Map help

Description:

Show or clear MSTP MSTI VLAN mapping configuration.

Syntax:

STP Msti Map [<msti>] [clear]

Parameters:

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

9.14 Msti Add

STP>Msti Add help

Description:

Add a VLAN to a MSTI.

Syntax:

STP Msti Add <msti> <vid>

Parameters:

<msti>	: STP bridge instance no (0-7, CIST=0, MSTI1=1, ...)
<vid>	: VLAN ID (1-4095)

9.15 Port Configuration

STP>Port Configuration help

Description:

Show STP Port configuration.

Syntax:

STP Port Configuration [<port_list>]

Parameters:

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

9.16 Port Mode

STP>Port Mode help

Description:

Set or show the STP enabling for a port.

Syntax:

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

Parameters:

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

9.17 Port Edge

STP>Port Edge help

Description:

Set or show the STP adminEdge port parameter.

Syntax:

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

Parameters:

<port_list>	: Port list or 'all', default: All ports
enable	: Configure MSTP adminEdge to Edge
disable	: Configure MSTP adminEdge to Non-edge

9.18 Port AutoEdge

STP>Port AutoEdge help

Description:

Set or show the STP autoEdge port parameter.

Syntax:

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

Parameters:

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

9.19 Port P2P

STP>Port P2P help

Description:

Set or show the STP point2point port parameter.

Syntax:

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

Parameters:

<port_list>	: Port list or 'all', default: All ports
enable	: Enable MSTP point2point
disable	: Disable MSTP point2point
auto	: Automatic MSTP point2point detection

9.20 Port RestrictedRole

STP>Port RestrictedRole help

Description:

Set or show the MSTP restrictedRole port parameter.

Syntax:

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

Parameters:

<port_list>	: Port list or 'all', default: All ports
enable	: Enable MSTP restricted role
disable	: Disable MSTP restricted role

9.21 Port RestrictedTcn

STP>Port RestrictedTcn help

Description:

Set or show the MSTP restrictedTcn port parameter.

Syntax:

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

Parameters:

<port_list>	: Port list or 'all', default: All ports
enable	: Enable MSTP restricted TCN
disable	: Disable MSTP restricted TCN

9.22 Port bpduGuard

STP>Port bpduGuard help

Description:

Set or show the bpduGuard port parameter.

Syntax:

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

Parameters:

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

9.23 Port Statistics

STP>Port Statistics help

Description:

Show STP port statistics.

Syntax:

STP Port Statistics [<port_list>]

Parameters:

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

9.24 Port Mcheck

STP>Port Mcheck help

Description:

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

Syntax:

STP Port Mcheck [<port_list>]

Parameters:

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

9.25 Msti Port Configuration

STP>Msti Port Configuration help

Description:

Show the STP CIST/MSTI port configuration.

Syntax:

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

Parameters:

<msti> : STP bridge instance no (0-7, CIST=0, MSTI1=1, ...)

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

9.26 Msti Port Cost

STP>Msti Port Cost help

Description:

Set or show the STP CIST/MSTI port path cost.

Syntax:

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

Parameters:

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

9.27 Msti Port Priority

STP>Msti Port Priority help

Description:

Set or show the STP CIST/MSTI port priority.

Syntax:

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

Parameters:

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

10. IGMP (Internet Group Management Protocol snooping)

Available Commands:

IGMP **Configuration [<port_list>]**

IGMP **Mode [enable|disable]**

IGMP **State [<vid>] [enable|disable]**

IGMP **Querier [<vid>] [enable|disable]**

IGMP **Fastleave [<port_list>] [enable|disable]**

IGMP **Router [<port_list>] [enable|disable]**

IGMP **Flooding [enable|disable]**

IGMP **Groups [<vid>]**

IGMP **Status [<vid>]**

10.1 Configuration

IGMP>Configuration help

Description:

Show IGMP snooping configuration.

Syntax:

IGMP Configuration [<port_list>]

Parameters:

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

10.2 Mode

IGMP>Mode help

Description:

Set or show the IGMP snooping mode.

Syntax:

IGMP Mode [enable|disable]

Parameters:

enable : Enable IGMP snooping

disable : Disable IGMP snooping

(default: Show IGMP snooping mode)

10.3 State

IGMP>State help

Description:

Set or show the IGMP snooping state for VLAN.

Syntax:

IGMP State [<vid>] [enable|disable]

Parameters:

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

enable : Enable IGMP snooping

disable : Disable IGMP snooping

(default: Show IGMP snooping mode)

10.4 Querier

IGMP>Querier help

Description:

Set or show the IGMP snooping querier mode for VLAN.

Syntax:

IGMP Querier [<vid>] [enable|disable]

Parameters:

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

enable : Enable IGMP querier

disable : Disable IGMP querier

(default: Show IGMP querier mode)

10.5 Fastleave

IGMP>Fastleave help

Description:

Set or show the IGMP snooping fast leave port mode.

Syntax:

IGMP Fastleave [<port_list>] [enable|disable]

Parameters:

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

enable : Enable IGMP fast leave

disable : Disable IGMP fast leave

(default: Show IGMP fast leave mode)

10.6 Router

IGMP>Router help

Description:

Set or show the IGMP snooping router port mode.

Syntax:

IGMP Router [<port_list>] [enable|disable]

Parameters:

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

enable : Enable IGMP router port

disable : Disable IGMP router port

(default: Show IGMP router port mode)

10.7 Flooding

IGMP>Flooding help

Description:

Set or show the IGMP snooping unregistered flood operation.

Syntax:

IGMP Flooding [enable|disable]

Parameters:

enable : Enable IGMP flooding

disable : Disable IGMP flooding

(default: Show IGMP flood mode)

10.8 Groups

IGMP>Groups help

Description:

Show IGMP groups.

Syntax:

IGMP Groups [<vid>]

Parameters:

<vid> : VLAN ID (1-4095)

10.9 Status

IGMP>Status help

Description:

Show IGMP status.

Syntax:

IGMP Status [<vid>]

Parameters:

<vid> : VLAN ID (1-4095)

11. LACP (Link Aggregation Control Protocol)

Available Commands:

LACP **Configuration [<port_list>]**

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

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

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

LACP **Status [<port_list>]**

LACP **Statistics [<port_list>] [clear]**

11.1 Configuration

LACP>Configuration help

Description:

Show LACP configuration.

Syntax:

LACP Configuration [<port_list>]

Parameters:

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

11.2 Mode

LACP>Mode help

Description:

Set or show LACP mode.

Syntax:

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

Parameters:

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

enable : Enable LACP protocol

disable : Disable LACP protocol

(default: Show LACP mode)

11.3 Key

LACP>Key help

Description:

Set or show the LACP key.

Syntax:

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

Parameters:

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

<key> : LACP key (1-65535) or 'auto

11.4 Role

LACP>Role help

Description:

Set or show the LACP role.

Syntax:

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

Parameters:

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

active : Initiate LACP negotiation

passive : Listen for LACP packets

(default: Show LACP role)

11.5 Status

LACP>Status help

Description:

Show LACP Status.

Syntax:

LACP Status [<port_list>]

Parameters:

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

11.6 Statistics

LACP>Statistics help

Description:

Show LACP Statistics.

Syntax:

LACP Statistics [<port_list>] [clear]

Parameters:

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

12. LLDP (Link Layer Discovery Protocol)

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>]**

12.1 Configuration

LLDP>Configuration help

Description:

Show LLDP configuration.

Syntax:

LLDP Configuration [<port_list>]

Parameters:

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

12.2 Mode

LLDP>Mode help

Description:

Set or show LLDP mode.

Syntax:

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

Parameters:

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

enable : Enable LLDP reception and transmission

disable : Disable LLDP

rx : Enable LLDP reception only

tx : Enable LLDP transmission only

(default: Show LLDP mode)

12.3 Optional_TLV

LLDP>Optional_TLV help

Description:

Set or show LLDP Optional TLVs.

Syntax:

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

Parameters:

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

port_descr : Description of the port

sysm_name : System name

sys_descr : Description of the system

sys_capa : System capabilities

mgmt_addr : Master's IP address

(default: Show optional TLV's configuration)

enable : Enables TLV

disable : Disable TLV

(default: Show optional TLV's configuration)

12.4 Interval [<interval>]

LLDP>Interval help

Description:

Set or show LLDP Tx interval.

Syntax:

LLDP Interval [<interval>]

Parameters:

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

12.5 Hold

LLDP>Hold help

Description:

Set or show LLDP Tx hold value.

Syntax:

LLDP Hold [<hold>]

Parameters:

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

12.6 Delay

LLDP>Delay help

Description:

Set or show LLDP Tx delay.

Syntax:

LLDP Delay [<delay>]

Parameters:

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

12.7 Reinit

LLDP>Reinit help

Description:

Set or show LLDP reinit delay.

Syntax:

LLDP Reinit [<reinit>]

Parameters:

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

12.8 Statistics

LLDP>Statistics help

Description:

Show LLDP Statistics.

Syntax:

LLDP Statistics [<port_list>] [clear]

Parameters:

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

12.9 Info

LLDP>Info help

Description:

Show LLDP neighbor device information.

Syntax:

LLDP Info [<port_list>]

Parameters:

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

13. LLDPMED (Link Layer Discovery Protocol Media)

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 [voice|voice_signaling|guest_voice|guest_voice_signaling|softphone_voice|video_conferencing|streaming_video|video_signaling] [tagged|untagged] [<vlan_id>] [<l2_priority>] [<dscp>]

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

LLDPMED Coordinates [latitude|longitude|altitude] [north|south|west|east|meters|floor] [coordinate_value]

LLDPMED Datum [wgs84|nad83_navd88|nad83_mllw]

LLDPMED Fast [<count>]

LLDPMED Info [<port_list>]

LLDPMED debug_med_transmit_var [<port_list>] [enable|disable]

13.1 Configuration

LLDPMED >Configuration help

Description:

Show LLDP-MED configuration.

Syntax:

LLDPMED Configuration [<port_list>]

Parameters:

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

13.2 Civic

LLDPMED > Civic help

Description:

Set or show LLDP-MED Civic Address Location.

Syntax:

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

Parameters:

country	: Country
state	: National subdivisions (state, caton, region, province, prefecture)
county	: County, parish, gun (JP), district(IN)
city	: City, township, 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 information name
name	: Name(residence and office occupant)
zip_code	: Postal/zip code
building	: Building (structure)
apartment	: Unit (apartment, suite)
floor	: Floor
room_number	: Room number
place_type	: Place type
postal_com_name	: Postal community name
p_o_box	: Post office box (P.O. Box)
additional_code	: Additional code

(default: Show Civic Address Location configuration)

<civic_value> : The value for the Civic Address Location entry.

13.3 ecs

LLDPMED > ecs help

Description:

Set or show LLDP-MED Emergency Call Service.

Syntax:

LLDPMED ecs [<ecs_value>]

Parameters:

<ecs_value> : The value for the Emergency Call Service

13.4 policy delete

LLDPMED > policy delete help

Description:

Delete the selected policy.

Syntax:

LLDPMED policy delete [<policy_list>]

Parameters:

<policy_list> : List of policies to delete

13.5 policy add

LLDPMED > policy add help

Description:

Adds a policy to the list of polices.

Syntax:

LLDPMED policy add [voice|voice_signaling|guest_voice|guest_voice_signaling|soft phone_voice|video_conferencing|streaming_video|video_signaling] [tagged|untagged] [<vlan_id>] [<l2_priority>] [<dscp>]

Parameters:

vhoice : Voice for use by dedicated IP Telephony handsets and other similar appliances supporting interactive voice services. These devices are typically deployed on a separate VLAN for ease of deployment and enhanced security by isolation from data applications.

voice_signaling : Voice Signaling (conditional) for use in network topologies that require a different policy for the voice signaling than for the voice media.

guest_voice	: Guest Voice to support a separate limited feature-set voice service for guest users and visitors with their own IP Telephony handsets and other similar appliances supporting interactive voice services.
guest_voice_signaling	: Guest Voice Signaling (conditional) for use in network topologies that require a different policy for the guest voice signaling than for the guest voice media.
softphone_voice	: Softphone Voice for use by softphone applications on typical data centric devices, such as PCs or laptops. This class of endpoints frequently does not support multiple VLANs, if at all, and are typically configured to use an untagged VLAN or a single tagged data specific VLAN.
video_conferencing	: Video Conferencing for use by dedicated Video Conferencing equipment and other similar appliances supporting real-time interactive video/audio services.
streaming_video	: Streaming Video for use by broadcast or multicast based video content distribution and other similar applications supporting streaming video services that require specific network policy treatment. Video applications relying on TCP with buffering would not be an intended use of this application type.
video_signaling	: Video Signaling (conditional) for use in network topologies that require a separate policy for the video signaling than for the video media.
tagged	: The device is using tagged 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.

13.6 port policies

LLDPMED > port policies help

Description:

Set or show LLDP-MED port policies.

Syntax:

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

Parameters:

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

<policy_list> : List of policies to delete

13.7 Coordinates

LLDPMED > Coordinates help

Description:

Set or show LLDP-MED Location.

Syntax:

LLDPMED Coordinates [latitude|longitude|altitude] [north|south|west|east|meters |floor] [coordinate_value]

Parameters:

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, Meters or floors with max. 4 digits.

(default: Show coordinate location configuration)

north|south|west|east|meters|floor

: North : North (Valid for latitude)

South : South (Valid for latitude)

West : West (Valid for longitude)

East : East (Valid for longitude)

Meters : Meters (Valid for altitude)

Floor : Floor (Valid for altitude)

coordinate_value : Coordinate value

13.8 Datum

LLDPMED > Datum help

Description:

Set or show LLDP-MED Coordinates map datum.

Syntax:

LLDPMED Datum [wgs84|nad83_navd88|nad83_mllw]

Parameters:

wgs84|nad83_navd88|nad83_mllw

: WGS84

nad83_navd88 : NAD83_NAVD88

nad83_mllw : NAD83_MLLW

13.9 Fast

LLDPMED > Fast help

Description:

Set or show LLDP-MED Fast Start Repeat Count.

Syntax:

LLDPMED Fast [<count>]

Parameters:

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

13.10 Info

LLDPMED > Info help

Description:

Show LLDP-MED neighbor device information.

Syntax:

LLDPMED Info [<port_list>]

Parameters:

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

13.11 debug_med_transmit_var

LLDPMED > debug_med_transmit_var help

Description:

Set or show if the current value of the global medTansmitEnable variable (Section Section 11.2.1, TIA 1057).

Syntax:

LLDPMED debug_med_transmit_var [<port_list>] [enable|disable]

Parameters:

<port_list>	: Port list or 'all', default: All ports
enable	: Enable - Set medTansmitEnable variable to true
disable	: Disable - Set medTansmitEnable variable to false

(default: Show medTansmitEnable variable value)

14. QoS (Quality of Service)

Available Commands:

QoS **Configuration [<port_list>]**

QoS **Classes [<class>]**

QoS **Default [<port_list>] [<class>]**

QoS **Tagprio [<port_list>] [<tag_prio>]**

QoS **QCL Port [<port_list>] [<qcl_id>]**

QoS **QCL Add [<qcl_id>] [<qce_id>] [<qce_id_next>]**
(etype <etype>) | (vid <vid>) | (port <udp_tcp_port>) |
(dscp <dscp>) | (tos <tos_list>) | (tag_prio <tag_prio_list>)
<class>

QoS **QCL Delete <qcl_id> <qce_id>**

QoS **QCL Lookup [<qcl_id>] [<qce_id>]**

QoS **Mode [<port_list>] [strict|weighted]**

QoS **Weight [<port_list>] [<class>] [<weight>]**

QoS **Rate Limiter [<port_list>] [enable|disable] [<bit_rate>]**

QoS **Shaper [<port_list>] [enable|disable] [<bit_rate>]**

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

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

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

14.1 Configuration

QoS>Configuration help

Description:

Show QoS Configuration.

Syntax:

QoS Configuration [<port_list>]

Parameters:

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

14.2 Classes

QoS>Classes help

Description:

Set or show the number of traffic classes.

Syntax:

QoS Classes [<class>]

Parameters:

<class> : Number of traffic classes (1,2 or 4)

14.3 Default

QoS>Default help

Description:

Set or show the default port priority.

Syntax:

QoS Default [<port_list>] [<class>]

Parameters:

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

<class> : Traffic class low/normal/medium/high or 1/2/3/4

14.4 Tagprio

QoS>Tagprio help

Description:

Set or show the port VLAN tag priority.

Syntax:

QoS Tagprio [<port_list>] [<tag_prio>]

Parameters:

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

<tag_prio> : VLAN tag priority (0-7)

14.5 QCL Port

QoS>QCL Port help

Description:

Set or show the port QCL ID.

Syntax:

QoS QCL Port [<port_list>] [<qcl_id>]

Parameters:

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

14.6 QCL Add

QoS>QCL Add help

Description:

Add or modify QoS Control Entry (QCE).

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

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

Syntax:

QoS QCL Add [<qcl_id>] [<qce_id>] [<qce_id_next>]
(etype <etype>) | (vid <vid>) | (port <udp_tcp_port>) |
(dscp <dscp>) | (tos <tos_list>) | (tag_prio <tag_prio_list>)
<class>

Parameters:

<qcl_id>	: QCL ID
<qce_id>	: QCE ID (1-24)
<qce_id_next>	: Next QCE ID (1-24)
etype	: Ethernet Type keyword
<etype>	: Ethernet Type
vid	: VLAN ID keyword
<vid>	: VLAN ID (1-4095)
port	: UDP/TCP port keyword
<udp_tcp_port>	: Source or destination UDP/TCP port (0-65535)
dscp	: IP DSCP keyword
<dscp>	: IP DSCP (0-63)
tos	: IP ToS keyword

<tos_list> : IP ToS list (0-7)
tag_prio : VLAN tag priority keyword
<tag_prio_list> : VLAN tag priority list (0-7)
<class> : Traffic class low/normal/medium/high or 1/2/3/4

14.7 QCL Delete

QoS>QCL Delete help

Description:

Delete QCE.

Syntax:

QoS QCL Delete <qcl_id> <qce_id>

Parameters:

<qcl_id> : QCL ID
<qce_id> : QCE ID (1-24)

14.8 QCL Lookup

QoS>QCL Lookup help

Description:

Lookup QCE.

Syntax:

QoS QCL Lookup [<qcl_id>] [<qce_id>]

Parameters:

<qcl_id> : QCL ID
<qce_id> : QCE ID (1-24)

14.9 Mode

QoS>Mode help

Description:

Set or show the port egress scheduler mode.

Syntax:

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

Parameters:

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

strict : Strict mode

weighted : Weighted mode

(default: Show QoS mode)

14.10 Weight

QoS>Weight help

Description:

Set or show the port egress scheduler weight.

Syntax:

QoS Weight [<port_list>] [<class>] [<weight>]

Parameters:

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

<class> : Traffic class low/normal/medium/high or 1/2/3/4

<weight> : Traffic class weight 1/2/4/8

14.11 Rate Limiter

QoS>Rate Limiter help

Description:

Set or show the port rate limiter.

Syntax:

QoS Rate Limiter [<port_list>] [enable|disable] [<bit_rate>]

Parameters:

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

enable : Enable rate limiter

disable : Disable rate limiter

(default: Show rate limiter mode)

<bit_rate> : Rate in 1000 bits per second (500-1000000 kbps)

14.12 Shaper

QoS>Shaper help

Description:

Set or show the port shaper.

Syntax:

QoS Shaper [<port_list>] [enable|disable] [<bit_rate>]

Parameters:

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

(default: Show shaper mode)

<bit_rate>	: Rate in 1000 bits per second (500-1000000 kbps)

14.13 Storm Unicast

QoS>Storm Unicast help

Description:

Set or show the unicast storm rate limiter.

Syntax:

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

Parameters:

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

14.14 Storm Multicast

QoS>Storm Multicast help

Description:

Set or show the multicast storm rate limiter.

Syntax:

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

Parameters:

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

14.15 Storm Broadcast

QoS>Storm Broadcast help

Description:

Set or show the multicast storm rate limiter.

Syntax:

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

Parameters:

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

15. Mirror (Port mirroring)

Available Commands:

Mirror **Configuration [<port_list>]**

Mirror **Port [<port>|disable]**

Mirror **Mode [<port_list>] [enable|disable|rx|tx]**

15.1 Configuration

Mirror>Configuration help

Description:

Show mirror configuration.

Syntax:

Mirror Configuration [<port_list>]

Parameters:

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

15.2 Port

Mirror>Port help

Description:

Set or show the mirror port.

Syntax:

Mirror Port [<port>|disable]

Parameters:

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

(default: Show port)

15.3 Mode

Mirror>Mode help

Description:

Set or show the mirror mode.

Syntax:

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

Parameters:

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

(default: Show mirror mode)

16. Config (Load/Save of configuration via TFTP)

Available Commands:

Config **Save <ip_server> <file_name>**

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

16.1 Save

Config>Save help

Description:

Save configuration to TFTP server.

Syntax:

Config Save <ip_server> <file_name>

Parameters:

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

16.2 Load

Config>Load help

Description:

Load configuration from TFTP server.

Syntax:

Config Load <ip_server> <file_name> [check]

Parameters:

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

17. Firmware (Download of firmware via TFTP)

>Firmware ?

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)
<file_name>	: Firmware file name

Glossary

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

A

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.

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

Use 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 DUT.

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.

D

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 agent¡¦s MAC address.

DHCP Snooping

DHCP Snooping is used to block intruder on the untrusted ports of DUT 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.

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

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

IGMP 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.

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 a internet network.
IP is a "best effort" system, which means that no packet of information sent over it 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.

IPMC

IPMC is an acronym for IP MultiCast.

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.

LLDP

LLDP is an IEEE 802.1ab standard protocol. The Link Layer Discovery Protocol, is used for network discovery, and works by having the units in the network exchanging information with their neighbors using LLDP frames.

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.

N

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.

P

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

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, communication between ports in that private VLAN is not

permitted. A VLAN can be configured as a private VLAN.

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.
There are 4 web-pages associated with the QoS configuration:
QoS|QoS Control List: The web page shows the QCEs in a prioritized way, highest (top) to lowest (bottom). Default the table is empty. An ingress frame will only get a hit on one QCE even though there are more matching QCEs. The first matching QCE will give that frame a priority: Low, Normal, Medium or High. 5 different QCLs can be created, each with 8 different QCEs. You assign each port a QCL id under QoS|Ports page. The QoS counters can be viewed under Monitor|Ports|QoS statistics. There are number of parameters that can be configured with a QCE. Read the Web page help text to get further information for each of them.
QoS|Ports: The Ports QoS page is used to assign a QCL id to an ingress port.

Furthermore you can assign a default class to a port and a queuing mode. Strict queuing means that the higher priority frame will always be served before a lower priority frame. Weighted priority will give each class some weight of the bandwidth.

QoS|Rate Limiters: Under this page you can configure the policer (ingress) and shaper (egress) rate for each port. See the help page for details.

QoS|Storm Control: Here you can limit the flooding in the switch, i.e. the rate you choose applies to the whole switch. Choose the mix of Unicast, Multicast and Broadcast storm control. See the help page for details.

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

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

SFP (Small form-factor pluggable) is a compact, hot-pluggable transceiver used for both telecommunication and data communications applications. It interfaces a network device mother board (for a switch, router, media converter or similar device) to a fiber optic or copper networking cable. It is a popular industry format supported by many network component vendors. SFP transceivers are designed to support SONET, Gigabit Ethernet, Fiber Channel, and other communications standards.

SFP DDM

DDM (Digital Diagnostics Monitoring) 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). This feature gives the end user the ability to monitor real-time parameters of the SFP, such as optical output power, optical input power, temperature, laser bias current, and transceiver supply voltage.

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.

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 (1-16) 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 provides 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.

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.

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 use 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).

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.