ISW Series Managed Industrial Ethernet Switch Command Reference Guide

ISW 4-10/100P, 2-10/100T, 2-SFP
ISW 4GbP, 2GbT, 2-SFP
ISW 8-10/100P, 4-SFP
ISW 8GbP, 4-SFP

9034963-02 Rev. AA
April 2022

Copyright © 2022 Extreme Networks, Inc. All rights reserved.

Legal Notice

Extreme Networks, Inc. reserves the right to make changes in specifications and other information contained in this document and its website without prior notice. The reader should in all cases consult representatives of Extreme Networks to determine whether any such changes have been made.

The hardware, firmware, software or any specifications described or referred to in this document are subject to change without notice.

Trademarks

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries.

All other names (including any product names) mentioned in this document are the property of their respective owners and may be trademarks or registered trademarks of their respective companies/owners.

For additional information on Extreme Networks trademarks, please see:
www.extremenetworks.com/company/legal/trademarks

Software Licensing

Some software files have been licensed under certain open source or third-party licenses. End-user license agreements and open source declarations can be found at:
www.extremenetworks.com/support/policies/software-licensing

Support

For product support, phone the Global Technical Assistance Center (GTAC) at 1-800-998-2408 (toll-free in U.S. and Canada) or +1-408-579-2826. For the support phone number in other countries, visit: http://www.extremenetworks.com/support/contact/

For product documentation online, visit: https://www.extremenetworks.com/documentation/

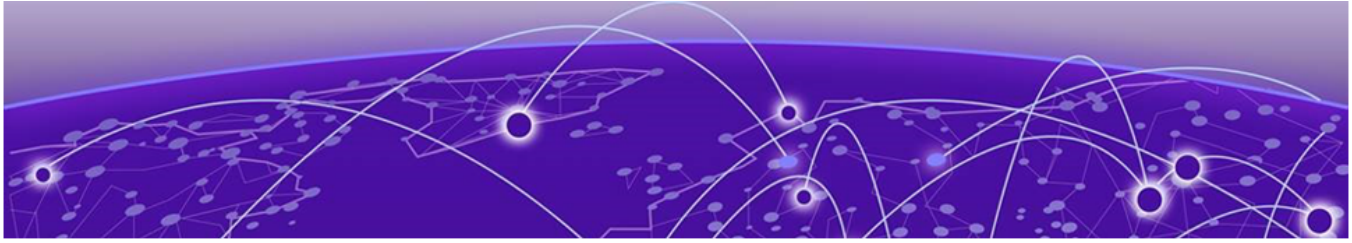


Table of Contents

Preface **13**
- Text Conventions 13
- Getting Help 14
- Extreme Networks Documentation 14
  - Open Source Declarations 14
- Providing Feedback to Us 14

Introduction to the Industrial Switches Command Reference Guide **16**
- Scope 16
- Audience 16
- Pre-required Knowledge 16
- Access to Hardware Interface 16

Getting Started with the ISW Switch **17**
- Connecting to the ISW Interface 17
- Execution Modes 18
- Using the CLI Help 19
- Terminal Key Function 19
- Syntax Conventions 20

ISW Commands **21**
- Initialize Mode Commands 21
  - exit 21
  - configure terminal 22
  - enable 22
  - show terminal 22
  - show history 23
  - show clock 23
- Enable Mode Commands 23
  - configure terminal 23
  - disable 24
  - show aaa 24
  - show access management 24
  - show access-list 24
  - show account 25
  - show aggregation 26
  - show aging time 26
  - show alarm 26
  - show cpu-load 26
  - show ddmi 27
  - show dot1x 27
  - show dot1x status 27
  - show dot1x statistics 27

show ext-tpid....28
show green-ethernet....28
show interface gigabit <portNo>....29
show interface gigabit <portNo> port-isolation....29
show interface gigabit <portNo> storm-control....29
show interface gigabit <portNo> transceiver....30
show interface gigabit <portNo> vlan....30
show interface....30
show interface priority....31
show interface statistics....31
show interface vlan....32
show ip....32
show ipmc....32
show ipv6....33
show lacp....33
show line....34
show logging....34
show loop-protec....34
show system inventory....35
show mac address-table (learning)....35
show mac address table learning....35
show mac-address-table (per gigabit port)....36
show mac address-table (per VLAN index)....36
show mac address-table conf....36
show mac address-table count....37
show mac address-table interface....37
show mac address-table static....37
show mac address-table vlan <vlanid>....38
show multicast-fdb....38
show mvr....38
show ntp....39
show platform phy....39
show poe....40
show port-mirror....40
show port-security....40
show port-shaper....41
show profile alarm....41
show protocol-vlan....41
show pvlan isolation [interface <port_type> [<port_type_list>]]....41
show pvlan [<pvlan_list>]....42
show qos....42
show qos maps....42
show qos maps (CoS queue mapping)....43
show qos qce....43
show qos storm....43
show que-scheduler profile....44
show queue-shaper....44
show radius-server [statistics]....44
show rfc2544 profile....45

show ringv2 45
show rmon 45
show running-cfg 46
show running-config interface Gigabit 46
show running-config interface vlan 46
show running-config all-defautls 47
show running-config feature 47
show running-config line 48
show running-config vlan 48
show sflow 48
show snmp 49
show spanning-tree 50
show switchport forbidden 51
show tacacs-server 51
show tech-support 51
show version 52
show vlan 52
show vlan brief 53
show vlan id 53
show vlan ip-subnet 53
show vlan mac 54
show vlan name 54
show vlan protocol 54
show vlan status 55
show vlan-trans 56
show voice 56
show web 56
Configure Mode Commands 57
aaa 57
access 57
access-list 58
account add <username> 58
account delete <username> 58
aggregation mode 59
alarm history clear 59
banner 59
clear ip igmp snooping statistics 60
clear logging 60
clear mac address-table 60
clock datetime 60
clock summer-time set [start-time] [end-time] 61
clock timezone 61
configuration save and replace 62
ddmi 62
debug 62
default access-list rate-limiter 63
delete 63
dir 63
do 63

duplex....64
editing....64
firmware....64
flowcontrol....65
flow-control {enable | disble}....65
frame-sizes....65
green-etherneteee....66
green-etherneteee optimize-for-power....66
green-etherneteee urgent-queues....66
help....67
interface gigabit <portNo>....67
interface vlan <vlanid>....67
iparp inspection....68
ip arp inspection entry....68
ip arp inspection translate....68
ip arp inspection vlan....69
ip dns proxy....69
ip http secure-redirect....69
ip http secure-server....69
ip name-server....70
ip route....70
ip routing....70
ip source binding interface....71
ip ssh....71
ip telnet....71
ip verify....71
ipmc profile....72
ipmc range....72
lacp....72
line....73
login host....73
login level....73
login on....74
logout....74
mac address-table aging-time....74
mac address-table aging-time <time>....74
mac address-table static....75
media-type....75
monitor destination interface....76
monitor source cpu....76
monitor source interface....76
more....77
mtu <value>....77
no....77
ntp server <1-5> ip-address <ip>....77
ping....78
port-security....78
port {enable/disable}....78
privilege....79

profile sch ... 79
reload ... 80
rmon ... 80
rmon alarm ... 80
rmon event ... 81
speed (Ethernet) ... 81
speed (interface) ... 82
syslog {enable | disable} ... 82
tacacs-server host ... 83
tacacs-server key ... 83
tacacs-server timeout ... 83
terminal ... 84
traps ... 84
upnp ... 85
upnp advertising-duration ... 85
upnp ttl ... 85
username ... 85
vlan <vlanid> ... 86
vlan <vlanid> <name> ... 86
vlan disable <vlanid> ... 87
web ... 87
VLAN Mode Commands ... 88
vlan ... 88
vlan ethertype s-custom-port ... 88
vlan protocol ... 88
vlan-trunking ... 89
switchport access vlan ... 89
switchport forbidden vlan ... 90
switchport hybrid acceptable-frame-type ... 90
switchport hybrid allowed vlan ... 90
switchport hybrid egress-tag ... 91
switchport hybrid ingress-filtering ... 91
switchport mode ... 91
switchport trunk allowed vlan ... 92
switchport vlan protocol group ... 92
Interface VLAN Mode Commands ... 93
interface ... 93
interface vlan ... 93
ip address ... 93
ip dhcp excluded-address ... 94
ip dhcp pool ... 94
ip dhcp relay ... 94
ip dhcp relay information option ... 95
ip dhcp retry interface vlan ... 95
ip dhcp server ... 95
ip dhcp snooping ... 95
ip helper-address ... 96
ip name-server ... 96
ipv6 address ... 96

ipv6mtu....97
RingV2 Group Mode Commands....97
ringv2 protect....97
guard-time....97
mode....98
node1 interface GigabitEthernet <portNo>}....98
node2 interface GigabitEthernet <portNo>}....98
role....98
Spanning Tree....99
spanning-tree....99
spanning-tree aggregation....99
spanning-tree auto-edge....100
spanning-tree bpdu-guard....100
spanning-tree edge....100
spanning-tree edge bpdu-filter....101
spanning-tree mode....101
spanning-tree mst cost....101
spanning-tree mst port-priority....102
spanning-tree mst priority....102
spanning-tree mst vlan....102
spanning-tree mst forward-time....103
spanning-tree mst max-age....103
spanning-tree mst max-hops....103
spanning-tree mst name....104
spanning-tree mst <instance>....104
spanning-tree recovery....105
spanning-tree transmit....105
sFlow Configure Command....105
sflow....105
sflow agent-ip....106
sflow collector-address....106
sflow max-datagram-size....106
sflow max-sampling-size....106
sflow collector-port....107
sflow sampling-rate....107
sflow timeout....107
SNMP Configure Command....108
snmp-server....108
snmp-server access....108
snmp-server community v2c....109
snmp-server community v3....109
snmp-server host....109
snmp-server host traps....110
snmp-server trap....110
snmp-server user....110
snmp-server version....111
snmp-server view....111
SNMP trap receive ipv6 host....112
snmp-server contact....112

snmp-server engine-id ... 112
snmp-server location ... 113
snmp-server security-to-group ... 113
SNMP trap receive ipv4 host ... 113
QoS Function Command ... 114
qos qce ... 114
qos storm ... 114
qos cos ... 115
qos dscp-classify ... 115
qos dscp-remark ... 115
qos dscp-translate ... 116
qos map cos-dscp ... 116
qos map dscp-cos ... 116
qos map dscp-egress-translation ... 117
qos map dscp-ingress-translation ... 118
qos policer ... 118
qos wrr ... 119
qos queue-shaper ... 119
qos queue-policer ... 119
qos shaper <unit> ... 120
IGMP Functional Commands ... 120
ip igmp host-proxy [leave-proxy] ... 120
ip igmp snooping ... 120
ip imp snooping immediate-leave ... 121
ip igmp snooping last-member-query-interval ... 121
ip igmp snooping max-groups ... 121
ip igmp snooping mrouter ... 121
ip igmp snooping querier ... 122
ip igmp snooping query-interval ... 122
ip igmp snooping vlan ... 122
ip igmp ssm-range ... 123
ip igmp unknown-flooding ... 123
clear ip igmp snooping statistics ... 123
MVR Functional Commands ... 124
mvr ... 124
mvr immediate-leave ... 124
mvr name channel ... 124
mvr frame priority ... 124
mvr name <word16> frame tagged ... 125
mvr name <word16> igmp-address <ipv4_ucast> ... 125
mvr name <word16> last-member-query-interval <0-31744> ... 125
mvr name <word16> mode ... 126
mvr name <word16> type ... 126
mvr vlan ... 126
mvr vlan <vlan_list> channel ... 127
mvr vlan <vlan_list> frame priority ... 127
mvr vlan <vlan_list> frame tagged ... 127
mvr vlan <vlan_list> igmp-address ... 128
mvr vlan <vlan_list> mode ... 128

mvr vlan <vlan_list> type....128
MLD Functional Commands....129
ipv6 mld host-proxy....129
ipv6 mld snooping....129
ipv6 mld snooping compatibility....129
ipv6 mld snooping immediate-leave....130
ipv6 mld snooping last-member-query-interval....130
ipv6 mld snooping max-groups....130
ipv6 mld snooping mrouter....131
ipv6 mld snooping query-interval....131
ipv6 mld snooping query-max-response-time....131
ipv6 mld snooping vlan....131
ipv6 mld ssm-range....132
ipv6 mld unknown-flooding....132
ipv6 route....132
Authenticate Mode Commands....133
radius-server attribute 32....133
radius-server attribute 4....133
radius-server attribute 95....133
radius-server deadtime....134
radius-server host [auth-port] [acct-port] [timeout] [retransmit] [key]....134
radius -server key....134
radius-server retransmit....135
radius-server timeout....135
tacacs-server deadtime <1-1440>....135
tacacs-server host....136
dot1x authentication timer....136
dot1x feature....136
dot1x guest-vlan....137
dot1x initialize....137
dot1x max-reauth-req....137
dot1x port-control....137
dot1x radius-vlan....138
dot1x re-authentication....138
dot1x system-auth-controln....138
dot1x timeout....139
show radius-server [statistics]....139
enable....139
end....140
exit....140
hostname....140
Loop-Protection Configure commands....141
loop-protect....141
loop-protect action....141
loop-protect shutdown-time....141
loop-protect transmit-time....142
loop-protect tx-mode....142
LLDP Configure commands....142
lldp holdtime....142

lldp med....142
lldp receive....143
lldp reinit <1-10>....143
lldp timer <5-32768>....144
lldp tlv-select....144
lldp transmission-delay....144
lldp transmit....145
RFC2544 Testing Configure Commands....145
rfc2544 profile <word32>....145
rfc2544 rename profile....145
rfc2544 save <word32> <word>....145
rfc2544 start <word32> profile <word32> [desc <line128>]....146
rfc2544 stop <word32>....146
show rfc2544 profile [<word32>]....146
GVRP Configure Commands....147
gvrp....147
gvrpjoin request vlan....147
gvrpleave request vlan....147
gvrp max-vlans....148
gvrp time { [join-time <1-20>] [leave-time <60-300>] [leave-all-time <1000-50>]148
Voice VLAN Configure Commands....148
voice vlan....148
voice vlan aging-time....149
voice vlan class....149
voice vlan oui....149
voice vlan vid....150
Profile Alarm Commands....150
profile alarm....150
alarm....150
PoE Commands....151
poe management mode....151
poe supply....151
poe mode....152
poe operation....152
poe power....152
poe priority....153
poe reset....153
poe schedule....153
Configuring ERPS from the CLI....154
Initial Switch Configuration....154
Configuring MEP and ERPS on Switch 1 (RPL Owner)....155
Configuring MEP and ERPS on Switch 2 (RPL Neighbor)....155
Configuring MEP and ERPS on Switch 3....155

Regulatory and Compliance Information....157
Federal Communications Commission (FCC) Notice....157
Industry Canada NoticeCAN ICES-3 (A)/NMB-3(A)....157
Product Safety....157
Electromagnetic Compatibility (EMC)....158
Korea EMC Statement (KCC)....158

BSMI EMC Statement - Taiwan.....158

Glossary.....159

Preface

This section discusses the conventions used in this guide, ways to provide feedback, additional help, and other Extreme Networks publications.

Text Conventions

The following tables list text conventions that are used throughout this guide.

Table 1: Notice Icons

Icon	Notice Type	Alerts you to...
	General Notice	Helpful tips and notices for using the product.
	Note	Important features or instructions.
	Caution	Risk of personal injury, system damage, or loss of data.
	Warning	Risk of severe personal injury.
New!	New Content	Displayed next to new content. This is searchable text within the PDF.

Table 2: Text Conventions

Convention	Description
`Screen displays`	This typeface indicates command syntax, or represents information as it appears on the screen.
The words **enter** and **type**	When you see the word “enter” in this guide, you must type something, and then press the Return or Enter key. Do not press the Return or Enter key when an instruction simply says “type.”
[Key] names	Key names are written with brackets, such as **[Return]** or **[Esc]**. If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press **[Ctrl]**+**[Alt]**+**[Del]**
Words in italicized type	Italics emphasize a point or denote new terms at the place where they are defined in the text. Italics are also used when referring to publication titles.

Getting Help

If you require assistance, contact Extreme Networks using one of the following methods:

- GTAC (Global Technical Assistance Center) for Immediate Support
  - **Phone:** 1-800-998-2408 (toll-free in U.S. and Canada) or +1 408-579-2826. For the support phone number in your country, visit: www.extremenetworks.com/support/contact
  - **Email:** support@extremenetworks.com. To expedite your message, enter the product name or model number in the subject line.
- Extreme Portal — Search the GTAC knowledge base, manage support cases and service contracts, download software, and obtain product licensing, training, and certifications.
- The Hub — A forum for Extreme Networks customers to connect with one another, answer questions, and share ideas and feedback. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.

Before contacting Extreme Networks for technical support, have the following information ready:

- Your Extreme Networks service contract number and/or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any action(s) already taken to resolve the problem
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load at the time of trouble (if known)
- The device history (for example, if you have returned the device before, or if this is a recurring problem)
- Any related RMA (Return Material Authorization) numbers

Extreme Networks Documentation

To find Extreme Networks product guides, visit our documentation pages at:

Current Product Documentation	www.extremenetworks.com/documentation/
Archived Documentation (for earlier versions and legacy products)	www.extremenetworks.com/support/documentation-archives/
Release Notes	www.extremenetworks.com/support/release-notes

Open Source Declarations

Some software files have been licensed under certain open source licenses. More information is available at: www.extremenetworks.com/support/policies/software-licensing/.

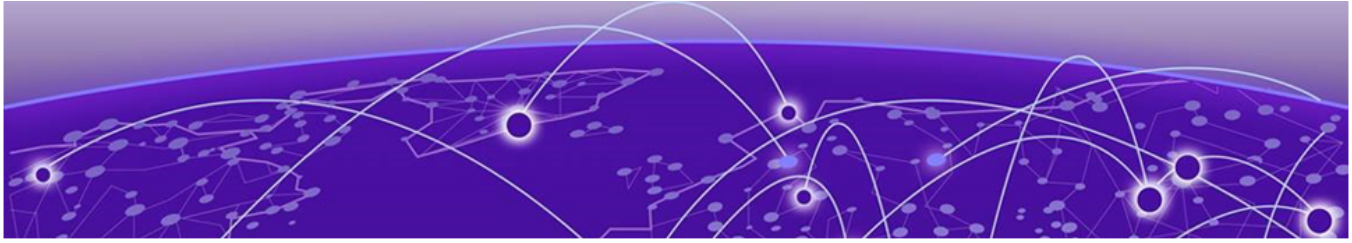
Providing Feedback to Us

We are always striving to improve our documentation and help you work better, so we want to hear from you! We welcome all feedback but especially want to know about:

- Content errors or confusing or conflicting information.
- Ideas for improvements to our documentation so you can find the information you need faster.

- Broken links or usability issues.

If you would like to provide feedback to the Extreme Networks Information Development team about this document, please contact us using our short https://www.extremenetworks.com/documentation-feedback/. You can also email us directly at documentation@extremenetworks.com.



Introduction to the Industrial Switches Command Reference Guide

Scope

This user guide describes the commands and parameters of the Command Line Interface (CLI) as implemented in the current version of ISW-Series Managed Industrial Ethernet Switch software. These commands are used to set up, administer, and maintain the system.

Audience

The guide is intended for Operating personnel.

Pre-required Knowledge

You must be familiar with the:

- Basic operations of Industrial Switches.
- Security and activity monitoring constraints that limit how a command is implemented.

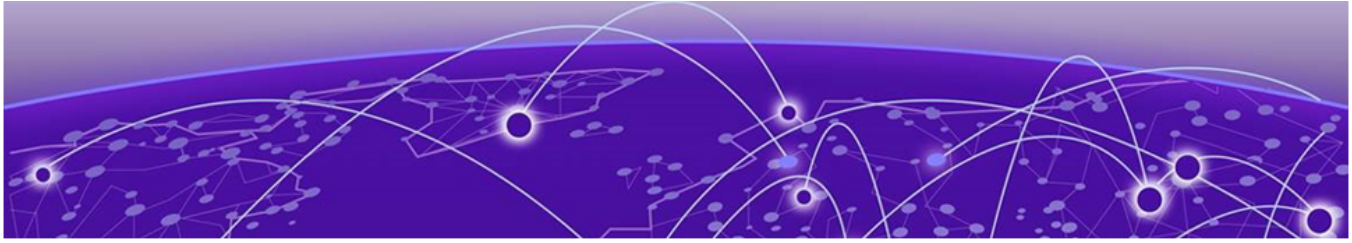
Access to Hardware Interface

Access to the hardware interface is by a terminal (or computer with terminal emulation software). Requirements for the terminal are:

- RS-232 ASCII port
- Selectable transmission baud rate
- Full alphanumeric capability
- Selectable odd/even or no parity check
- Connecting to ISW Ethernet port (RJ45 Ethernet port)
- Key-in the command under Telnet: **`telnet 192.0.2.1`**
- Login with default account and password:

  Username: `admin`

  Password: `[none]`



Getting Started with the ISW Switch

Connecting to the ISW Interface on page 17
Execution Modes on page 18
Using the CLI Help on page 19
Terminal Key Function on page 19
Notation Conventions on page 20

Access to the switch is protected by a logon security system. You can log on to the switch with the user name and password. After three failed logon attempts, the system refuses further attempts.

After you log on, the system monitors the interface for periods of inactivity. If the interface is inactive for too long, you are automatically logged off.

The CLI initial user name is (**admin**) and no password. You should change the password as soon as possible, because the initial password is known to anyone who reads this manual. You can also change the user name or add additional user names. Use the **account add** command to enter a new user identification, password, and authorization level.

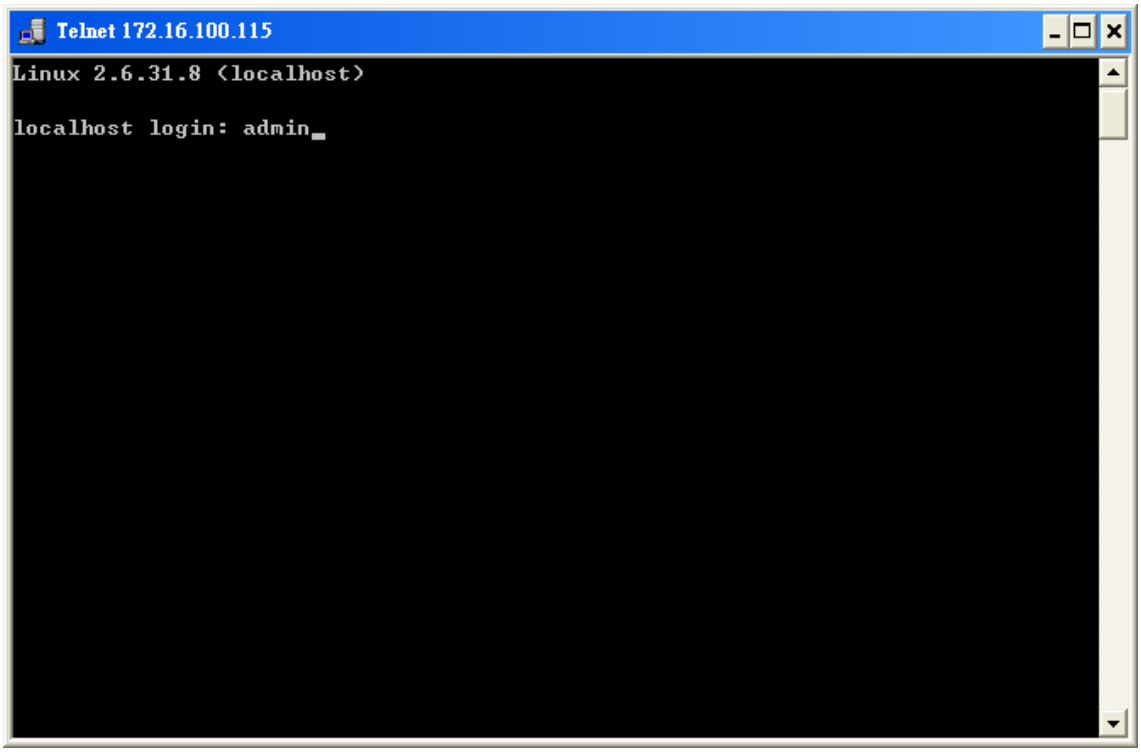
Connecting to the ISW Interface

Interface	Parameters
Console	Baud rate: 115200bps Data bit: 8 Parity: None. Stop bit: 1
Telnet	Port 23
SSH	Port 22 (In Windows, you can run terminal emulator such as PuTTY)

Connecting to ISW Ethernet port (RJ45 Ethernet port):

1. Key-in the command under Telnet: **telnet 192.0.2.1**

2. Log in with default account and password (`admin / [none]`).



Execution Modes

The CLI contains several execution modes. Users will see different set of commands under different execution modes. The following table lists all the execution modes and their purposes. When you enter a certain execution mode, the corresponding mode prompt will be displayed automatically on the screen. The mode prompts of all the execution modes are also listed in the following table.

Table 3: List of Execution Modes

Mode	Access Level	Prompt
Init Mode	Guest	>
Enable Mode	Guest	#
Config Mode	Guest	`(conf)#`
Alarm Profile Config Mode	Engineer	`(alarm-profile-conf)#`
Gigabit Interface Config Mode	Engineer	`(gigabit-intf-conf)#`
ACL (Access Control List) Profile Config Mode	Engineer	`(acl-profile-conf)#`
scheduler Profile Config Mode	Engineer	`(sch-profile-conf)#`
VLAN (Virtual LAN) Interface Config Mode	Engineer	`(vlan-intf-conf)#`
IGMP (Internet Group Management Protocol) MVR Profile Config Mode	Engineer	`(igmp-mvr-profile-conf)#`
IGMP ACL Profile Config Mode	Engineer	`(igmp-acl-profile-conf)#`

Table 3: List of Execution Modes (continued)

Mode	Access Level	Prompt
RingV2 Group Config Mode	Engineer	`(ring)#`
Trunk Group Config Mode	Engineer	`(trunk-group-conf)#`

Using the CLI Help

You can get help by entering a question mark (?) at each position in the command. The displayed result depends on the execution mode and previous input.

Terminal Key Function

Following is the list of all the terminal keys and their function.

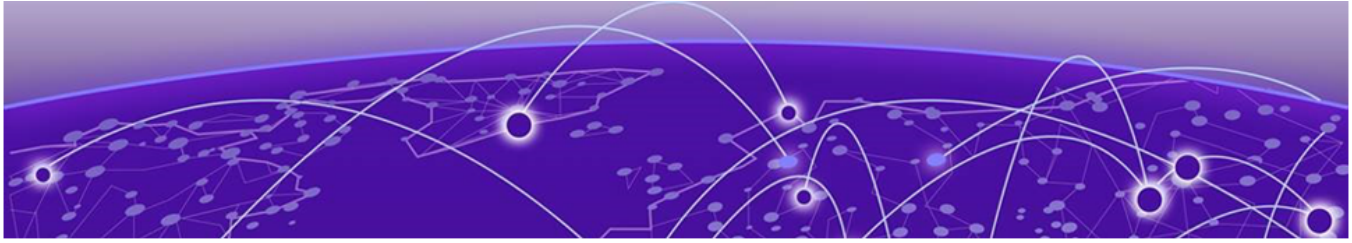
Table 4: List of Terminal Keys

[ENTER]	Run a CLI config script
[CTRL] + [M]	
[TAB]	Tab completion. If **[TAB]** is pressed after a non-whitespace character, complete the word before the Tab. If **[TAB]** is pressed after a whitespace character, complete the next word.
[CTRL] +[I]	
[?]	Display available commands. If ? is pressed after a non-whitespace character, show possible choices for *this* word. If ? is pressed after a whitespace character, show possible choices for the *next* word.
up arrow	Up history
[CTRL] + [P]	
down arrow	Down history
[CTRL] + [N]	
[Home]	Move the cursor to the beginning of the input line
[CTRL] + [A]	
[End]	Move the cursor to the end of the input line
[CTRL] + [E]	
left arrow	Move the cursor backward
[CTRL] + [B]	
right arrow	Move the cursor forward
[CTRL] + [F]	
[Backspace]	Erase the character before the cursor
[CTRL] + [H]	

Notation Conventions

The notation conventions for the parameter syntax of each CLI command are as follows:

- { }: Required parameters.
- [ ]: Optional parameters.
- |: Only one of the specified values can be used.



ISW Commands

Initialize Mode Commands on page 21
Enable Mode Commands on page 23
Configure Mode Commands on page 57
VLAN Mode Commands on page 88
Interface VLAN Mode Commands on page 93
RingV2 Group Mode Commands on page 97
Spanning Tree on page 99
sFlow Configure Command on page 105
SNMP Configure Command on page 108
QoS Function Command on page 114
IGMP Functional Commands on page 120
MVR Functional Commands on page 124
MLD Functional Commands on page 129
Authenticate Mode Commands on page 133
Loop-Protection Configure commands on page 141
LLDP Configure commands on page 142
RFC2544 Testing Configure Commands on page 145
GVRP Configure Commands on page 147
Voice VLAN Configure Commands on page 148
Profile Alarm Commands on page 150
PoE Commands on page 151
Configuring ERPS from the CLI on page 154

Initialize Mode Commands

The commands in this section (except the **enable** command) can be executed under all command modes. These are also global commands.

exit

Description

Exit current mode and quit CLI.

Syntax

`exit`

Parameters

None.

configure terminal

Description

Enter configuration mode.

Syntax

`configure terminal`

Parameters

None.

enable

Description

Enter enable mode.

Syntax

`enable`

Parameters

None.

show terminal

Description

Show CLI environment variables.

Syntax

`show terminal`

Parameters

None.

show history

Description

Show command history.

Note
Commands issued in one execution mode only appear in history of that execution mode.

Syntax

```
show history
```

Parameters

None.

show clock

Description

Show current time.

Syntax

```
show clock [detail]
```

Parameters

None.

Enable Mode Commands

All the show commands in this section can also be executed under any other command mode except Initialize Mode.

configure terminal

Description

Enter configuration mode.

Syntax

```
configure terminal
```

Parameters

None.

disable

Description

Enter init mode.

Syntax

`disable`

Parameters

None.

show aaa

Description

Show AAA.

Syntax

`show aaa`

Parameters

None.

show access management

Description

Access management configuration.

Syntax

`show access managemnet [`**`statistics`**` | `*`access_id_list`*`]`

Parameters

Name	Description
`statistics`	Statistics data.
`access_id_list`	ID of access management entry.

show access-list

Description

Access list.

Syntax

`show access-list [interface [(port_type [ v_port_type_list])]] [rate-limiter [rate_limiter_list]] [ace statistics [ace_list]]`

`show access-list ace-status [static] [link-oam] [loop-protect] [dhcp] [ptp] [upnp] [arp-inspection] [mep] [ipmc] [ip-source-guard] [ip-mgmt] [conflicts] [switch switch_list]`

Parameters

Name	Description
interface	Select an interface to configure
ace-status	The local ACEs status
port_type	GigabitEthernet,1 Gigabit Ethernet Port
v_port_type_list	Port list in 1/1 – 14
rate-limiter	Rate limiter
rate_limiter_list	Valid values are 1 – 16
ace	Access list entry
statistics	Traffic statistics
ace_list	<AceId : 1–256> ACE ID
static	The ACEs that are configured by users manually
loop-protect	The ACEs that are configured by Loop Protect module
ipmc	The ACEs that are configured by IPMC module
ip-source-guard	The ACEs that are configured by IP Source Guard module
dhcp	The ACEs that are configured by DHCP module
conflicts	The ACEs that did not get applied to the hardware due to hardware limitations
arp-inspection	The ACEs that are configured by ARP Inspection module

show account

Description

Show user account list.

Syntax

`show account`

Parameters

None.

show aggregation

Description

Aggregation.

Syntax

`show aggregation [mode]`

Parameters

mode	Traffic distribution mode.

show aging time

Description

Show aging time for MAC learning table (system-wide).

Syntax

`show aging time`

Parameters

None.

show alarm

Description

Alarm information.

Syntax

`show alarm [history | current]`

Parameters

current	Shows alarm current information.
history	Shows alarm history information.

show cpu-load

Description

CPU load.

Syntax

`show cpu-load`

Parameters

None.

show ddmi

Description

Show DDMI configuration.

Syntax

```
show ddmi
```

Parameters

None.

show dot1x

Description

Show dot1x information.

Syntax

```
show dot1x
```

Parameters

None.

show dot1x status

Description

Show dot1x stats.

Syntax

```
show dot1x status [interface port_type [port_type_list]] [brief]
```

Parameters

None.

show dot1x statistics

Description

Show dot1x statistics

Syntax

```
show dot1x statistics {eapol | radius | all} [interface (port_type
   [v_port_type_list])]
```

Parameters

Name	Description
eapol	Show EAPOL statistics
radius	Show Backend Server statistics
all	Show all dot1x statistics
port_type	GigabitEthernet, 1 Gigabit Ethernet Port
v_port_type_list	PORT_LIST, Port list in 1/1-14

show ext-tpid

Description

Show TPID for the *VLAN (Virtual LAN)* Tag

Syntax

```
show ext-tpid
```

Parameters

None.

show green-ethernet

Description

Green Ethernet.

Syntax

```
show green-ethernet [interface (port_type [port_list])]
show green-ethernet eee [interface (port_type [port_list])]
show green-ethernet energy-detect [interface (port_type [port_list])]
show green-ethernet short-reach [interface (port_type [port_list])]
```

Parameters

Name	Description
eee	Shows green ethernet EEE status for a specific port or ports.
energy-detect	Shows green ethernet energy-detect status for a specific port or ports.
short-reach	Shows green ethernet short-reach status for a specific port or ports.
interface	Shows green ethernet status for a specific port or ports.

Name	Description
port_type	GigabitEthernet, 1 Gigabit Ethernet Port.
port_list	Port list in 1/1 – 14.

show interface gigabit <portNo>

Description

Show interface gigaport information

Syntax

```
show interface gigabit portNo
```

Parameters

Name	Description
portNo	Gigabit port. Valid values: 1 – 10 Type: Mandatory

show interface gigabit <portNo> port-isolation

Description

Show isolation information per gigabit port.

Syntax

```
show pvlan isolation [interface portNo [port_type_list]]
```

Parameters

Name	Description
portNo	Valid values: 1 – 10 Type: Mandatory

show interface gigabit <portNo> storm-control

Description

Show storm control information per gigabit port.

Syntax

```
show interface gigabit portNo storm-control
```

Parameters

Name	Description
port_type	Port type in Fast, Giga or Tengiga Ethernet
portNo	Valid values: 1–10 Type: Mandatory

show interface gigabit <portNo> transceiver

Description

Show interface transceiver

Syntax

`show interface GigabitEthernet interface port_type_list transceiver`

Parameters

Name	Description
portNo	Valid values: 11 – 14 (for 14 port model) Type: Mandatory

show interface gigabit <portNo> vlan

Description

Show vlan information per port

Syntax

`show interface gigabit portNo vlan`

Parameters

Name	Description
portNo	Gigabit port. Valid values: 1 – 10 Type: Mandatory

show interface

Description

Show interface information per port.

Syntax

`show interface port_type [port_type_list] status`

Parameters

Name	Description
port_type	Port type in Fast, Giga or Tengiga Ethernet
portNo	Valid values: 1 – 10 Type: Mandatory

show interface priority

Description

Show *QoS (Quality of Service)* per gigabit port.

Syntax

`show interface port_type [port_type_list] statistics {priority [0-7] }`

Table 5: Parameters

Name	Description
priority [0-7]	Valid values:0 – 7 Type: Mandatory
port_type	Port type in Fast, Giga or Tengiga Ethernet
portNo	Valid values: 0 – 10 Type: Mandatory

show interface statistics

Description

Show Ethernet counter per gigabit port.

Syntax

`show interface port_type [port_type_list] statistics`

Parameters

Name	Description
port_type	Port type in Fast, Giga or Tengiga Ethernet
portNo	Valid values: 1 – 10 Type: Mandatory
counter	Show Gigabit Ethernet counter

show interface vlan

Description

Show interface information of all or specific *VLAN*s.

Syntax

`show interface vlan {vlanid}`

Parameters

Name	Description
vlanid	VLAN ID. Valid values: 1 – 4094

show ip

Description

IP information.

Syntax

`show ip`

Parameters

Name	Description
arp	Address Resolution Protocol
dhcp	Dynamic Host Configuration Protocol
http	Hypertext Transfer Protocol
igmp	Internet Group Management Protocol
interface	IP interface status and configuration
name-server	Domain Name System
route	Display the current ip routing table
source	source command
ssh	Secure Shell
telnet	Telnet
statistics	Traffic statistics
verify	verify command

show ipmc

Description

IPMC information.

Syntax

`show ipmc profile [profile_name] [detail]`

`show ipmc range [entry_name]`

Parameters

Name	Description
profile	IPMC profile configuration.
range	A range of IPv4/IPv6 multicast addresses for the profile.
profile_name	Profile name in 16 characters.
detail	Detailed information of a profile.
entry_name	Range entry name in 16 characters.

show ipv6

Description

IPv6 information.

Syntax

`show ipv6`

Parameters

Name	Description
interface	Select an interface to configure.
mld	Multicasat Listener Discovery.
neighbor	IPv6 neighbors.
route	IPv6 routes.
statistics	Traffic statistics.

show lacp

Description

LACP information.

Syntax

`show lacp {internal | statistics | system-id | neighbour}`

Parameters

Name	Description
internal	Internal LACP configuration.
neighbour	Neighbour LACP status.
statistics	Internal LACP statistics.
system-id	LACP system ID.

show line

Description

Alive line information.

Syntax

`show line [alive]`

Parameters

Name	Description
alive	Display information about alive lines.

show logging

Description

Logging information.

Syntax

`show logging log_id [ switch switch_list]`

`show logging [info] [warning] [error] [switch switch_list]`

Parameters

Name	Description
log_id	Valid values are 1 – 4294967295
error	Error
info	Infomation
warning	Warning

show loop-protec

Description

Loop protect information.

Syntax

```
show loop-protect [interface (port_type [plist])]
```

Parameters

Name	Description
interface	Interface status and configuration.
port_type	GigabitEthernet, 1 Gigabit Ethernet Port.
plist	Port list in 1/1 – 14.

show system inventory

Description

Show system inventory.

Syntax

```
show system inventory
```

Parameters

None.

show mac address-table (learning)

Description

Show MAC learning table.

Syntax

```
show mac address-table [conf | static | aging-time | {{learning | count}
   [interface port_type [port_type_list]]} | {address mac_addr [vlan
   vlan_id ]} | vlan vlan_id | interface port_type [port_type_list]]
```

Parameters

None.

show mac address table learning

Description

Learn/disable/secure stat.

Syntax

```
show mac address-table [conf | static | aging-time | {{learning | count}
   [interface (port_type [v_port_type_list])]} | {address v_mac_addr
```

```
[vlan v_vlan_id]} | vlan v_vlan_id_1 | interface (port_type
[v_port_type_list_1])]
```

Parameters

None.

show mac-address-table (per gigabit port)

Description

Show static MAC forwarding table per gigabit port.

Syntax

```
show mac address-table {learning | count} [interface port_type
   [port_type_list]]
```

Parameters

Name	Description
port_type	Port type in Fast, Giga or Tengiga Ethernet
portNo	Valid values: 1 – 10 Type: Mandatory

show mac address-table (per VLAN index)

Description

Show static MAC forwarding table per *VLAN* index.

Syntax

```
show mac address-table {learning | count} vlan vlan_id
```

Parameters

Name	Description
vlan_id	Valid values: 1 – 4094 Type: Mandatory

show mac address-table conf

Description

User-added static MAC addresses.

Syntax

```
show mac address-table conf | static | aging-time | {{learning | count}
   [interface port_type [v_port_type_list]]} | {address v_mac_addr [vlan
```

```
v_vlan_id ]} | vlan v_vlan_id | interface port_type
[v_port_type_list]]
```

Parameters

None.

show mac address-table count

Description

Total number of MAC addresses.

Syntax

```
show mac address-table [conf | static | aging-time | {{learning | count}
   [interface (port_type [v_port_type_list])]} | {address v_mac_addr
   [vlan v_vlan_id]} | vlan v_vlan_id_1 | interface (port_type
   [v_port_type_list_1])]
```

Parameters

None.

show mac address-table interface

Description

Show MAC learning table per port.

Syntax

```
show mac address-table [interface (port_type [port_type_list]]
```

Parameters

Name	Description
port_no	Valid values: 1 – 10 Type: Mandatory

show mac address-table static

Description

Show all static MAC addresses.

Syntax

```
show mac address-table [conf | static | aging-time | {{learning | count}
   [interface (port_type [v_port_type_list])]} | {address v_mac_addr
   [vlan v_vlan_id]} | vlan v_vlan_id_1 | interface (port_type
   [v_port_type_list_1])]
```

Parameters

None.

show mac address-table vlan <vlanid>

Description

Show MAC learning table per *VLAN* index.

Syntax

```
show mac address-table {learning | count} vlan [vlan_id]]
```

Parameters

Name	Description
vlan_id	Valid values: 1 – 4094 Type: Mandatory

show multicast-fdb

Description

Show *IGMP (Internet Group Management Protocol)* group membership table

Syntax

```
show multicast-fdb
```

Parameters

None.

show mvr

Description

MVR information.

Syntax

```
show mvr vlan [v_vlan_list | name mvr_name] [group-database [interface
   (port_type [v_port_type_list])] [sfm-information]] [detail]
```

Parameters

Name	Description
vlan	Search by *VLAN*.
v_vlan_list	MVR multicast VLAN list.
name	Search by MVR name.

Name	Description
mvr_name	MVR multicast VLAN name.
group-database	Multicast group database from MVR.
interface	Search by port.
port_type	GigabitEthernet, 1 Gigabit Ethernet Port.
v_port_type_list	PORT_LIST, Port list in 1/1 – 14
sfm-information	Including source filter multicast information from MVR.
detail	Detail information/statistics of MVR group database.

show ntp

Description

Show *SNTP (Simple Network Time Protocol)* information.

Syntax

```
show sntp
```

Parameters

None.

show platform phy

Description

PHYs information.

Syntax

```
show platform phy [interface (port_type [v_port_type_list])]
show platform phy id [interface (port_type [v_port_type_list])]
show platform phy instance
show platform phy status [interface port_type [v_port_type_list])]
```

Parameters

Name	Description
id	ID
instance	PHY Instance Information
status	Status
interface	Interface
port_type	Gigabit Ethernet, 1 Gigabit Ethernet Port
v_port_type_list	Port list in 1/1 – 14

show poe

Description

Show *PoE (Power over Ethernet)* status and information for each port.

Syntax

```
show poe
show poe [interface (port_type [v_port_type_list])]
```

Parameters

Name	Description
poe	Power over Ethernet
port_type	Gigabit Ethernet, 1 Gigabit Ethernet Port
v_port_type_list	Port list in 1/1 – 14

show port-mirror

Description

Show port mirror information.

Syntax

```
show port-mirror
```

Parameters

None.

show port-security

Description

Port security.

Syntax

```
show port-security
```

Parameters

Name	Description
port	Show MAC Addresses learned by Port Security
switch	Show Port Security status
interface	Interface

Name	Description
port_type	Gigabit Ethernet, 1 Gigabit Ethernet Port
v_port_type_list	Port list in 1/1 – 14

show port-shaper

Description

Show port shaper information.

Syntax

`show port-shaper`

Parameters

None.

show profile alarm

Description

Profile alarm.

Syntax

`show profile alarm`

Parameters

None.

show protocol-vlan

Description

Show protocol based *VLAN* information for all entries.

Syntax

`show protocol-vlan`

Parameters

None.

show pvlan isolation [interface <port_type> [<port_type_list>]]

Description

Show all port isolation information.

Syntax

`show pvlan isolation [`**`interface`** *`port_type`* `[`*`port_type_list`*`]]`

Parameters

Name	Description
`port_type`	Port type in Fast, Giga or Tengiga Ethernet
`portNo`	Valid values: 1 – 10 Type: Mandatory

show pvlan [<pvlan_list>]

Description

PVLAN ID

Syntax

`show pvlan [`*`pvlan_list`*`]`

Parameters

Name	Description
`pvlan_list`	PVLAN ID to show configuration for

show qos

Description

QoS interface information

Syntax

`show qos [{`**`interface`** `[(`*`port_type`* `[`*`port`*`])]}`

Parameters

Name	Description
`interface`	Interface
`port_type`	GigabitEthernet, 1 Gigabit Ethernet Port
`port`	PORT_LIST, Port list in 1/1-14

show qos maps

Description

MAPS

Syntax

```
show qos maps {maps [dscp-cos] [dscp-ingress-translation] [dscp-
   classify] [cos-dscp] [dscp-egress-translation]}
```

Parameters

Name	Description
cos-dscp	Map for cos to dscp
dscp-classify	Map for dscp classify enable
dscp-cos	Map for dscp to cos
dscp-egress-translation	Map for dscp egress translation
dscp-ingress-translation	Map for dscp ingress translation

show qos maps (CoS queue mapping)

Description

Show *CoS (Class of Service)* queue mapping table.

Syntax

```
show qos maps
```

Parameters

None.

show qos qce

Description

QCE

Syntax

```
show qos {qce [qce]}
```

Parameters

Name	Description
qce	QCE ID. Valid values are 1 – 256.

show qos storm

Description

Show storm control information by *VLAN*.

Syntax

```
show vlan unknown-uc
show vlan unknown-mc
show vlan broadcast
```

Parameters

Name	Description
unknown-uc	Show unknown unicast storm control information by VLAN. Type: Mandatory
unknown-mc	Show unknown multicast storm control information by VLAN. Type: Mandatory
broadcast	Show broadcast storm control information by VLAN. Type: Mandatory

show que-scheduler profile

Description

Show scheduler profile table.

Syntax

```
show queue-scheduler profile
```

Parameters

None.

show queue-shaper

Description

Show queue shaper information.

Syntax

```
show queue-shaper
```

Parameters

None.

show radius-server [statistics]

Description

show radius-server statistics

Syntax

```
show radius-server [statistics]
```

Parameters

Name	Description
statistics	Count radius packet statistics

show rfc2544 profile

Description

Show rfc2544 profile name.

Syntax

```
show rfc2544 profile [word32]
```

Parameters

Name	Description
word32	rfc2544 profile name

show ringv2

Description

Show ring protect information

Syntax

```
show ring
```

Parameters

None.

show rmon

Description

Syntax

```
show rmon alarm [id_list]
show rmon event [id_list]
show rmon history [id_list]
show rmon statistics [id_list]
```

Parameters

Name	Description
alarm	Display the RMON alarm table
event	Display the RMON event table
history	Display the RMON history table
statistics	Display the RMON statistics table
id_list	Statistics entry list. Valid values are 1 – 65535

show running-cfg

Description

Show running configuration.

Syntax

`show running-cfg`

Parameters

None.

show running-config interface Gigabit

Description

Show port configuration.

Syntax

`show running-config interface (port_type [list]) [all-defaults]`

Parameters

Name	Description
list	Port list in 1/1 – 14.
all-defaults	Include most/all default values.

show running-config interface vlan

Description

Show default running configuration.

Syntax

`show running-config interface vlan vlan_list [all-defaults]`

Parameters

Name	Description
vlan_list	List of *VLAN* numbers.
all-defaults	Include most/all default values.

show running-config all-defautls

Description

Show all default settings.

Syntax

`show running-config [all-defaults]`

Parameters

Name	Description
all-defaults	Include all default values.

show running-config feature

Description

Show running configuration feature.

Syntax

`show running-config feature feature_name [all-defaults]`

Parameters

Name	Description
all-defaults	Include all default values.
feature_name	CWORD Valid values are : GVRP | access | access-list | aggregation | alm_profile | arp-inspection | auth | clock | dhcp | dhcp-snooping | dhcp_server | dns | dot1x | green-ethernet | http | icli | ip-igmp-snooping | ip-igmp-snooping-port | ip-igmp-snooping-vlan | ipmc-profile | ipmc-profile-range | ipv4 | ipv6 | ipv6-mld-snooping | ipv6-mld-snooping-port | ipv6-mld-snooping-vlan | lacp | lldp | logging | loop-protect | mac | monitor | mstp | mvr | mvr-port | ntp | phy | port | port-security | pvlan | qos | rmon | snmp | source-guard | ssh | tring_g1 | tring_g2 | tring_g3 | user | vlan | voice-vlan web-privilege-group-level
all-defaults	Include most/all default values

show running-config line

Description

Line information.

Syntax

`show running-config line {`**`console`** `| vty} list [`**`all-defaults`**`]`

Parameters

Name	Description
list	List of console/VTYs.
all-defaults	Include most/all default values

show running-config vlan

Description

VLAN information.

Syntax

`show running-config vlan list [`**`all-defaults`**`]`

Parameters

Name	Description
list	List of VLAN numbers.
all-defaults	Include most/all default values.

show sflow

Description

Sflow information

Syntax

`show sflow`

`show sflow statistics {`**`receiver`** `[rcvr_idx_list] | `**`samplers`** `[`**`interface`** `[samplers_list] (port_type [v_port_type_list])]}`

Parameters

Name	Description
receiver	Show statistics for receiver
samplers	Show statistics for samplers

Name	Description
interface	Interface
port_type	Gigabit Ethernet, 1 Gigabit Ethernet Port
v_port_type_list	Port list in 1/1 - 14

show snmp

Description

SNMP (Simple Network Management Protocol) information.

Syntax

```
show snmp
show snmp access [group_name {v1 | v2c | v3 | any} {auth | noauth |
   priv}]
show snmp community v3 [community]
show snmp host [conf_name] [system] [switch] [interface] [aaa]
show snmp mib context
show snmp mib ifmib ifIndex
show snmp security-to-group {v1 | v2c | v3} security_name]
show snmp user [username engineID]
show snmp view [view_name oid_subtree]
```

Parameters

Name	Description
access	access configuration
group_name	Group name
any	any security model
v1	v1 security model
v2c	v2c security model
v3	v3 security model
auth	authNoPriv Security Level
noauth	noAuthNoPriv Security Level
priv	authPriv Security Level
community	Community
community	Specify community name
host	Set SNMP host's configurations
conf_name	Name of the host configuration

Name	Description
aaa	AAA event group
interface	Interface event group
switch	Switch event group
system	System event group
mib	Management Information Base
context	MIB context
ifmib	IF-MIB
ifIndex	The IfIndex that is defined in IF-MIB
security-to-group	security-to-group configuration
security_name	Security group name
user	User
username	Security user name
engineID	Security Engine ID
view	MIB view configuration
view_name	MIB view name
oid_subtree	MIB view OID. Valid values are 1 – 255.

show spanning-tree

Description

System-wide Spanning Tree setting/status.

Syntax

```
show spanning-tree [summary | active | {interface (port_type
   [v_port_type_list])} | {detailed [interface port_type
   [v_port_type_list_1])]} | {mst [configuration | {instance [interface
   (port_type [v_port_type_list_2])]}]}]
```

Parameters

Name	Description
active	*STP (Spanning Tree Protocol)* active interfaces
detailed	STP statistics
interface	Choose port
mst	Configuration
summary	STP summary

show switchport forbidden

Description

Lookup *VLAN* Forbidden port entry

Syntax

```
show switchport forbidden [{vlan vid} | {name name}]
```

Parameters

Name	Description
vlan	Show forbidden access for specific VLAN id
vid	VLAN id
name	Show forbidden access for specific VLAN name
name	VLAN name

show tacacs-server

Description

TACACS+ configuration

Syntax

```
show tacacs server
```

Parameters

None.

NEW! show tech-support

Description

Display all details about the switch that would be useful to technical support – for example, system, version, current date and time, MAC addresses, IP addresses, switch configuration, switch log messages, hardware, software threads, and port statistics.

Syntax

```
show tech-support {|} {begin word | exclude word | include word}
```

Parameters

Note
In all of the following, *word* is case-sensitive.

Name	Description
begin *word*	Display output beginning with the first line containing *word*
exclude*word*	Display output, excluding lines containing *word*
include*word*	Display output, including only those lines containing *word*

Examples

```
ISW1# show tech | include address
ntp server 1 ip-address 10.8.255.160
ntp server 2 ip-address 10.8.255.159
mac address-table aging-time 3000
 ip address 192.0.2.1 255.255.255.0
 ip address 20.0.202.11 255.255.255.0
 ip address dhcp
 ipv6 address dhcp
```

show version

Description

Show firmware hardware and software status update status.

Syntax

`show version`

Parameters

None.

show vlan

Description

Show bridge port memberset/status.

Syntax

`show vlan`

Parameters

None.

show vlan brief

Description

VLAN summary information

Syntax

`show vlan [id vlan_list | name name | brief]`

Parameters

Name	Description
id	VLAN status by VLAN ID.
vlan_list	VLAN ID. Valid values are 1 – 4095.
name	VLAN status by VLAN name.
name	A VLAN name up to 32 characters.
brief	VLAN summary information.

show vlan id

Description

Show bridge port memberset/status per *VLAN* index.

Syntax

`show vlan id vlan_id`

Parameters

Name	Description
vlan_id	Valid values: 1 – 4094 Type: Mandatory.

show vlan ip-subnet

Description

Show *VLAN* ip-subnet entries

Syntax

`show vlan ip-subnet [id subnet_id]`

Parameters

Name	Description
id	Show a specific IP-subnet entry
subnet_id	The specific IP-subnet to show. Valid values are 1 – 28.

show vlan mac

Description

Show *VLAN* MAC entries

Syntax

```
show vlan mac [address mac_addr]
```

Parameters

Name	Description
address	Show a specific MAC entry
mac_addr	<mac_ucast> The specific MAC entry to show

show vlan name

Description

Show bridge port memberset/status per *VLAN* name.

Syntax

```
show vlan name vword32
```

Parameters

Name	Description
vword32	Valid values: 32 words Type: Mandatory.

show vlan protocol

Description

Protocol-based *VLAN* status

Syntax

```
show vlan protocol [eth2 {etype | arp | ip | ipx | at}] [snap {oui |
   rfc-1042 | snap-8021h} pid] [llc dsap ssap]
```

Parameters

Name	Description
eth2	Ethernet protocol based VLAN status
etype	<0x600-0xffff> Ether Type (Range: 0x600 - 0xFFFF)
arp	Ether Type is ARP
ip	Ether Type is IP
ipx	Ether Type is IPX
at	Ether Type is AppleTalk
llc	LLC-based VLAN status
dsap	<0x0-0xff> DSAP (Range: 0x00 - 0xFF)
ssap	<0x0-0xff> SSAP (Range: 0x00 - 0xFF)
snap	SNAP-based VLAN status
oui	<0x0-0xffffff> SNAP OUI (Range 0x000000 - 0XFFFFFF)
rfc-1042	SNAP OUI is rfc-1042
snap-8021h	SNAP OUI is 8021h

show vlan status

Description

Show the *VLAN*s configured for each interface

Syntax

```
show vlan status [interface (port_type [plist])] [combined | admin | nas
   | mvr | voice-vlan | mstp | erps | vcl | evc | gvrp | all |
   conflicts]
```

Parameters

Name	Description
admin	Show the VLANs configured by administrator
all	Show all VLANs configured
combined	Show the VLANs configured by a combination
conflicts	Show VLANs configurations that has conflicts
gvrp	Show the VLANs configured by GVRP
interface	Show the VLANs configured for a specific interface(s)
mstp	Show the VLANs configured by *MSTP (Multiple Spanning Tree Protocol)*.
mvr	Show the VLANs configured by MVR
nas	Show the VLANs configured by NAS

Name	Description
vcl	Show the VLANs configured by VCL
voice-vlan	Show the VLANs configured by Voice VLAN

show vlan-trans

Description

Show *VLAN* translation table for all

Syntax

```
show vlan-trans
```

Parameters

None.

show voice

Description

Vlan for voice traffic

Syntax

```
show voice vlan [oui oui | interface (port_type [port_list])]
```

Parameters

Name	Description
vlan	*VLAN* for voice traffic
oui	OUI configuration
oui	OUI value
interface	Select an interface to configure
port_type	GigabitEthernet, 1 Gigabit Ethernet Port
port_list	Port list in 1/1-14

show web

Description

Web privilege

Syntax

```
show web privilege group [group_name] level
```

Parameters

Name	Description
privilege	Web privilege
group	Web privilege grou
group_name	CWORD Valid words are: Aggregation | DHCP | Debug | Dhcp_Client | Diagnostics | EEE | Green_Ethernet | IP2 | IPMC_Snooping | LACP | *LLDP (Link Layer Discovery Protocol)* | Loop_Protect | MAC_Table | MVR | Maintenance | Mirroring | NTP | Ports | Private_VLANs | *QoS* | RPC | Security | Spanning_Tree | System | Timer | VCL | VLANs | Voice_VLAN | XXRP | sFlow
level	Web privilege group level

Configure Mode Commands

Commands that can be executed under Configure Mode. To enter Configure Mode, type the command: `configure terminal`. The prompt will now show `(config)#`.

aaa

Description

Authentication

Syntax

```
aaa authentication
```

Parameters

Name	Description
authentication	Authentication

access

Description

Management configuration

Syntax

```
access management
```

Parameters

Name	Description
management	Access management configuration

access-list

Description

Enter *ACL (Access Control List)* Profile Config Mode

Syntax

```
profile acl
```

Parameters

None.

account add <username>

Description

Add an account.

Syntax

`username word31 **privilege** 0-15 **password encrypted** word4-44`

Parameters

Name	Description
word31	Valid values: 1 – 31 characters Type: Mandatory
0-15	Valid values: 0 – 15 Type: Mandatory
word4-44	Valid values: 4-44 characters debug Type: Mandatory

account delete <username>

Description

Delete an account.

Syntax

`no username word31`

Parameters

Name	Description
word31	Valid values: 1 – 31 characters Type: Mandatory

aggregation mode

Description

Traffic distribution mode

Syntax

```
aggregation mode {dmac | ip | port | smac}
```

Parameters

Name	Description
dmac	Destination MAC affects the distribution
ip	IP address affects the distribution
port	IP port affects the distribution
smac	Source MAC affects the distribution

alarm history clear

Description

Clear alarm history

Syntax

```
alarm history clear
```

Parameters

None.

banner

Description

Banner control

Syntax

```
banner {LINE | exec | login | motd}
```

Parameters

Name	Description
LINE	c banner-text c, where 'c' is a delimiting character
exec	Set EXEC process creation banner
login	Set login banner
motd	Set Message of the Day banner

clear ip igmp snooping statistics

Description

clear IP *IGMP* snooping statistics

Syntax

```
clear ip igmp snooping [vlan vlan_list] statistics
```

Parameters

Name	Description
vlan_list	*VLAN* list.

clear logging

Description

Clear logging

Syntax

```
clear logging [info] [warning] [error] [switch switch_list]
```

Parameters

Name	Description
info	Information
warning	Warning
error	Error
switch_list	List of switch ID, e.g., 1,3-5,6

clear mac address-table

Description

Clear MAC address-table

Syntax

```
clear mac address-table
```

Parameters

clock datetime

Description

Set device date and time.

Syntax

```
clock datetime 2000-2037 1-12 1-31 0-23 0-59 0-59
```

Parameters

Name	Description
2000-2037	year
1-12	month
1-31	Date
0-23	Hour
0-59	minute
0-59	Second

clock summer-time set [start-time] [end-time]

Description

Set date/time.

Syntax

```
clock summer-time word16 date [1-12 1-31 2000-2097 hhmm 1-12 1-31
   2000-2097 hhmm [1-1440]]
```

Parameters

Name	Description
word16	Valid values: please see 'list timezone' Type: Mandatory
day	Valid values: 1 – 31 Type: Mandatory
month	Valid values: 1 – 12 Type: Mandatory
year	Valid values: 2000 – 2097 Type: Mandatory
minute	Valid values: 0 – 59 Type: Mandatory
second	Valid values: 0 – 59 Type: Optional

clock timezone

Description

Set time zone.

Syntax

```
clock timezone word16 -23-23 [0-59]
```

Parameters

Name	Description
word16	Valid values: please see 'list timezone' Type: Mandatory

configuration save and replace

Description

Save and install configuration

Syntax

```
copy {startup-config | running-config | Filename} {startup-config |
   running-config | Filename} [syntax-check]
```

Parameters

Name	Description
running-config	Currently running configuration
startup-config	Startup configuration
syntax-check	Perform syntax check on source configuration
Filename	File in FLASH or on TFTP server

ddmi

Description

Enable DDMI function

Syntax

```
ddmi
```

Parameters

None.

debug

Description

Set prompt for testing

Syntax

```
debug prompt word
```

Parameters

Name	Description
word	Word for prompt in 32 characters.

default access-list rate-limiter

Description

Rate limiter

Syntax

```
default access-list rate-limiter [rate_limiter_list]
```

Parameters

Name	Description
RateLimiterId	Rate limiter ID. Valid values are 1 – 16.

delete

Description

Delete one file in flash: file system

Syntax

```
delete word
```

Parameters

Name	Description
word	Name of file to delete.

dir

Description

Directory of all files in flash: file system

Syntax

```
dir
```

Parameters

do

Description

To run exec commands in config mode

Syntax

```
do line
```

Parameters

Name	Description
line	Exec Command

duplex

Description

Set duplex mode

Syntax

```
duplex {half | full | auto [half | full]}
```

Parameters

Name	Description
half	Forced half duplex.
full	Forced full duplex.
auto	Auto negotiation of duplex mode.
half | full	Advertise half /full duplex.

editing

Description

Enable command line editing

Syntax

```
editing
```

Parameters

firmware

Description

Firmware swap and upgrade

Syntax

```
firmware {swap | upgrade}
```

Parameters

Name	Description
swap	Swap between Active and Alternate firmware image
upgrade	Firmware upgrade

flowcontrol

Description

Enable/Disable flow control.

Syntax

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

Parameters

Name	Description
on	Enable flow control.
off	Disable flow control.

flow-control {enable | disble}

Description

Enable/Disable flow-control.

Syntax

```
flow-control {enable | disble}
```

Parameters

Name	Description
enable	Enable flow-control.
disable	Disable flow-control.

frame-sizes

Description

Select the frame sizes that the enabled tests will loop through

Syntax

```
frame-sizes {[64] [128] [256] [512] [1024] [1280] [1518] [2000] [9600]}
```

Parameters

Name	Description
64	Enable testing with 64-byte TST PDUs
128	Enable testing with 128-byte TST PDUs
256	Enable testing with 256-byte TST PDUs
512	Enable testing with 512-byte TST PDUs
1024	Enable testing with 1024-byte TST PDUs
1280	Enable testing with 1280-byte TST PDUs
1518	Enable testing with 1518-byte TST PDUs
2000	Enable testing with 2000-byte TST PDUs
9600	Enable testing with 9600-byte TST PDUs

green-etherneteee

Description

Powering down of PHYs when there is no traffic.

Syntax

```
green-etherneteee
```

Parameters

green-etherneteee optimize-for-power

Description

Set if EEE shall be optimized for least power consumption (else optimized for least traffic latency).

Syntax

```
green-etherneteee optimize-for-power
```

Parameters

green-etherneteee urgent-queues

Description

Enables EEE urgent queue. An urgent queue means that latency is kept to a minimum for traffic going to that queue. Note: EEE power savings will be reduced.

Syntax

```
green-etherneteee urgent-queues [range_list]
```

Parameters

Name	Description
range_list	EEE Interface.

help

Description

Description of the interactive help system

Syntax

`help`

Parameters

interface gigabit <portNo>

Description

Enter gigabit interface mode.

Syntax

`interface gigabit portNo`

Parameters

Name	Description
portNo	Valid values: 1 – 10 Type: Mandatory

interface vlan <vlanid>

Description

Enter mode of interface *VLAN*.

Syntax

`interface vlan vlanid`

Parameters

Name	Description
vlanid	Valid values: 1 – 4094 Type: Mandatory

iparp inspection

Description

IPARP inspection

Syntax

```
iparp inspection
```

Parameters

ip arp inspection entry

Description

ARP inspection entry interface configuration

Syntax

```
ip arp inspection entry interface port_type in_port_type_id vlan_var
   mac_var ipv4_var
```

Parameters

Name	Description
port_type	Port type in Fast, Giga or Tengigaethernet
in_port_type_id	Port ID in the format of switch-no/port-no
vlan_var	Select a *VLAN* id to configure
mac_var	Select a MAC address to configure
ipv4_var	Select an IP Address to configure

ip arp inspection translate

Description

IP ARP inspection entry interface configuration

Syntax

```
ip arp inspection translate [interface port_type port_type_id vlan_id
   mac_ucast ipv4_ucast]
```

Parameters

Name	Description
port_type	Port type in Fast, Giga or Tengigaethernet
port_type_id	Port ID in the format of switch-no/port-no
vlan_id	Select a *VLAN* id to configure

Name	Description
mac_ucast	Select a MAC address to configure
ipv4_ucast	Select an IP Address to configure

ip arp inspection vlan

Description

IP ARP inspection vlan setting

Syntax

`ip arp inspection vlan vlan_list`

Parameters

Name	Description
vlan_list	ARP inspection *VLAN* list

ip dns proxy

Description

IP DNS proxy service

Syntax

`ipdns proxy`

Parameters

ip http secure-redirect

Description

IP http secure-redirect

Syntax

`ip http secure-redirect`

Parameters

ip http secure-server

Description

IP Secure HTTP web server

Syntax

```
ip http secure-server
```

Parameters

ip name-server

Description

IP name server

Syntax

```
ip name-server {v_ipv4_ucast | dhcp [interface vlan v_vlan_id]}
```

Parameters

Name	Description
v_ipv4_ucast	A valid IPv4 unicast address
dhcp	Dynamic Host Configuration Protocol
v_vlan_id	*VLAN* identifier(s): VID

ip route

Description

IP Route

Syntax

```
ip route v_ipv4_addr v_ipv4_netmask v_ipv4_gw
```

Parameters

Name	Description
v_ipv4_addr	Network
v_ipv4_netmask	Netmask
v_ipv4_gw	Gateway

ip routing

Description

IP routing

Syntax

```
ip routing
```

Parameters

ip source binding interface

Description

IP source binding entry interface configuration

Syntax

```
ip source binding interface port_type port_type_id vlan_id ipv4_ucast
   mac_ucast
```

Parameters

Name	Description
port_type	Port type in Fast, Giga or Tengigaethernet
port_type_id	Port ID in the format of switch-no/port-no
vlan_id	Select a *VLAN* id to configure
ipv4_ucast	Select an IP Address to configure
mac_ucast	Select a MAC address to configure

ip ssh

Description

IP Secure Shell

Syntax

```
ip ssh
```

Parameters

None

NEW! ip telnet

Description

IP telnet

Syntax

```
ip telnet
```

Parameters

None

ip verify

Description

IP verify

Syntax

```
ip verify [source] [translate]
```

Parameters

Name	Description
source	verify source
translate	ip verify source translate all entries

ipmc profile

Description

IPMC profile configuration

Syntax

```
ipmc profile
```

Parameters

ipmc range

Description

A range of IPv4/IPv6 multicast addresses for the profile

Syntax

```
ipmc range word16 {ipv4_mcast [ipv4_mcast] | ipv6_mcast [ipv6_mcast]}
```

Parameters

Name	Description
word16	Range entry name in 16 char's
ipv4_mcast	Valid IPv4 multicast address
ipv4_mcast	Valid IPv4 multicast address that is not less than start address
ipv6_mcast	Valid IPv6 multicast address
ipv6_mcast	Valid IPv6 multicast address that is not less than start address

lacp

Description

LACP system priority

Syntax

```
lacp system-priority v_1_to_65535
```

Parameters

Name	Description
system-priority	System priority
v_1_to_65535	Priority value, lower means higher priority

line

Description

Console terminal control

Syntax

```
line {0-16 | console 0 | vty 0-15}
```

Parameters

Name	Description
<0-16>	List of line numbers
console	Console terminal line
vty	Virtual terminal

login host

Description

Domain name and IP address

Syntax

```
logging hostname {v_ipv4_ucast | v_word45}
```

Parameters

Name	Description
hostname	Domain name of the log server
ipv4_ucast	IP address of the log server

login level

Description

Log level

Syntax

```
logging level {info | warning | error}
```

Parameters

Name	Description
error	Error
info	Information
warning	Warning

login on

Description

Log on

Syntax

```
logging on
```

Parameters

logout

Description

System logout

Syntax

```
logout
```

Parameters

mac address-table aging-time

Description

MAC table entries/configuration

Syntax

```
mac address-table aging-time v_0_10_to_1000000
```

Parameters

Name	Description
<v_0_10_to_1000000>	Aging time in seconds, 0 disables aging

mac address-table aging-time <time>

Description

Configure aging time for a bridge port.

Syntax

```
mac address-table aging-time time
```

Parameters

Name	Description
time	Valid values: 10 – 1000000 (seconds), 0: disable aging Type: Mandatory

mac address-table static

Description

MAC table entries/configuration

Syntax

```
mac address-table static v_mac_addr vlan v_vlan_id interface (port_type
   [v_port_type_list])
```

Parameters

Name	Description
v_mac_addr	48 bit MAC address
v_vlan_id	*VLAN* IDs 1-4095
port_type	Select an interface to configure
v_port_type_list	Port list

media-type

Description

Configure media-type

Syntax

```
media-type {rj45 | sfp | dual}
```

Parameters

Name	Description
rj45	rj45 interface (copper interface).
sfp	sfp interface (fiber interface).
dual	Dual media interface (cu & fiber interface).

monitor destination interface

Description

The destination port. That is the port that trafficked should be mirrored to.

Syntax

```
monitor destination interface port_type port_type_id
```

Parameters

Name	Description
port_type	Port type
port_type_id	Port Number

monitor source cpu

Description

Mirror Interface traffic

Syntax

```
monitor source {cpu [cpu_switch_range]} {both | rx | tx}
```

Parameters

Name	Description
both	Setting source port to both will mirror both ingress and egress traffic
rx	Setting source port to rx will mirror ingress traffic
tx	Setting source port to tx will mirror egress traffic

monitor source interface

Description

Mirror Interface traffic

Syntax

```
monitor source {{interface (port_type [v_port_type_list])}
```

Parameters

Name	Description
port_type	1 Gigabit Ethernet Port
v_port_type_lis	Port list

more

Description

File in FLASH or on TFTP server

Syntax

`more Path`

Parameters

mtu <value>

Description

MTU size.

Syntax

`mtu value`

Parameters

Name	Description
value	Range. Valid values: 1536 – 9000 (bytes) Type: Mandatory

no

Description

Function disable

Syntax

`no {debug | port-securit | terminal}`

Parameters

Name	Description
debug	Debugging functions
port-securit	Port security (PSEC limit)
terminal	Set terminal line parameters

ntp server <1-5> ip-address <ip>

Description

Set NTP server address.

Syntax

`ntp server 1-5 ip-address {ipv4_ucast | ipv6_ucast | hostname}`

Parameters

Name	Description
1-5	index number
ipv4 <ipv6 >	Type: Mandatory
hostname	Server name

ping

Description

The ping function

Syntax

`ping {ip | ipv6}`

Parameters

Name	Description
ip	IP (*ICMP (Internet Control Message Protocol)*) echo
ipv6	IPv6 (ICMPv6) echo

port-security

Description

Port security

Syntax

`port-security [aging] [time v_10_to_10000000]`

Parameters

Name	Description
aging	Enable/disable port security aging
time	Time in seconds between check for activity on learned MAC addresses
v_10_to_10000000	10 - 10000000 seconds

port {enable/disable}

Description

Set interface gigabit port enable or disable.

Syntax

```
port {enable | disable}
```

Parameters

Name	Description
enable	Turn off gigabit port.
disable	Turn off gigabit port.

privilege

Syntax

```
privilege {exec |configure|config-vlan |line |interface | if-vlan |ipmc-
   profile |snmps-host |stp-aggr |dhcp-pool |rfc2544-profile} level
   privilege cmd
```

Parameters

Name	Description
config-vlan	*VLAN* Configuration Mode
configure	Global configuration mod
dhcp-pool	DHCP Pool Configuration Mode
exec	Exec mode
if-vlan	VLAN Interface Mode
interface	Port List Interface Mode
ipmc-profile	IPMC Profile Mode
line	Line configuration mode
rfc2544-profile	RFC2544 Profile Mode
snmps-host	*SNMP* Server Host Mode
stp-aggr	*STP* Aggregation Mode

profile sch

Description

Enter Scheduling Profile Config Mode

Syntax

```
profile sch
```

Parameters

None.

reload

Description

System or configuration reset

Syntax

```
reload {cold | default}
```

Parameters

Name	Description
cold	Reload cold
defaults	Reload defaults without rebooting

rmon

Description

RMON

Syntax

```
rmon {alarm | event}
```

Parameters

Name	Description
alarm	Configure an RMON alarm
event	Configure an RMON event

rmon alarm

Description

RMON Alarm

Syntax

```
rmon alarm id oid_str interval {absolute | delta} rising-threshold
   rising_threshold [rising_event_id] falling-threshold
   falling_threshold [falling_event_id] {[rising | falling | both ] }
```

Parameters

Name	Description
id	Alarm entry ID

interval	Sample interval
absolute	Test each sample directly
delta	Test delta between samples
rising_threshold	<-2147483648-2147483647> rising threshold value
rising_event_id	<0-65535> Event to fire on rising threshold crossing
falling_threshold	<-2147483648-2147483647> falling threshold value
falling_event_id	<0-65535> Event to fire on falling threshold crossing
rising	Trigger alarm when the first value is larger than the rising threshold
falling	rigger alarm when the first value is less than the falling threshold
both	Trigger alarm when the first value is larger than the rising threshold or less than the falling threshold (default)

rmon event

Description

RMON Event

Syntax

`rmon event` *`id`* [**`log`**] [**`trap`** *`community`*] {[**`description`** *`description`*]}

Parameters

Name	Description
`description`	Specify a description of the event
`log`	Generate RMON log when the event fires
`trap`	Generate SNMP trap when the event fires

speed (Ethernet)

Description

Configure gigabit Ethernet speed and Copper/SFP for gigabit port 7–8.

Note
Ports 1–6 Only support copper. They do not support SFP. Ports 9 and 10 only support **`auto`**.

Syntax

`speed {`**`auto`** | **`full-1000mbps`** | **`full-100mbps`** | **`full-10mbps`** | **`half-100mbps`** | **`half-10mbps`**`}`

Parameters

Name	Description
auto	Auto negotiation.
full-1000mbps	Set 1000 Mbps full duplexing.
full-100mbps	Set 100 Mbps full duplexing.
full-10mbps	Set 10 Mbps full duplexing.
half-100mbps	Set 100 Mbps half duplexing.
half-10mbps	Set 10 Mbps half duplexing.

speed (interface)

Description

Configure interface speed. If you use **10**, **100**, or **1000** keywords with the **auto** keyword the port will only advertise the specified speeds.

Syntax

`speed {10g | 2500 | 1000 | 100 | 10 | auto {[10] [100] [1000]}}`

Parameters

Name	Description
10g	10 Gbps
2500	25 Gbps
1000	1 Gbps
100	100 Mbps
auto	Auto-negotiation
10	10 Mbps
100	100 Mbps
1000	1000 Mbps (1 Gbps)

syslog {enable | disable}

Description

Disable or enable Syslog service.

Syntax

```
logging on
no logging on
```

Parameters

None.

tacacs-server host

Description

Configure TACACS+ server

Syntax

```
tacacs-server host word1-255 [ port 0-65535] [timeout 1-1000] [key
   line1-63]
```

Parameters

Name	Description
word1-255	Hostname or IP address
0-65535	TCP port number
1-1000	Wait time in seconds
line1-63	The shared key

tacacs-server key

Description

Configure TACACS+ encryption key

Syntax

```
tacacs-server key line1-63
```

Parameters

Name	Description
line1-63	The shared key

tacacs-server timeout

Description

Time to wait for a TACACS+ server to reply

Syntax

```
tacacs-server timeout <1-1000>
```

Parameters

Name	Description
1-1000	Wait time in seconds

terminal

Description

Terminal control.

Syntax

`terminal {editing |exec-timeout |help |history |length |width}`

Parameters

Name	Description
editing	Enable command line editing
exec-timeout	Set the EXEC timeout
help	Description of the interactive help system
history	Control the command history function
length	Set number of lines on a screen
width	Set width of the display terminal

traps

Description

trap event configuration

Syntax

`traps [aaa authentication ] [system [coldstart] [warmstart]] [switch [stp] [rmon]]`

Parameters

Name	Description
aaa authentication	AAA authentication fail event
coldstart	Cold start event
warmstart	Warm start event
stp	*STP* event
rmon	RMON event

upnp

Description

Set UPnP's configurations

Syntax

`upnp`

Parameters

upnp advertising-duration

Description

Set UPnP's advertising duration

Syntax

`upnp advertising-duration` *`100-86400`*

Parameters

Name	Description
`100-86400`	advertising duration

upnp ttl

Description

Set UPnP's TTL value

Syntax

`upnp ttl` *`1-255`*

Parameters

Name	Description
`1-255`	TTL value

username

Description

User account

Syntax

`username` *`username`* **`privilege`** *`priv`* **`password encrypted`** *`encry_password`*

`username` *`username`* **`privilege`** *`priv`* **`password none`**

`username` *`username`* **`privilege`** *`priv`* **`password unencrypted`** *`password`*

Parameters

Name	Description
username	<Username : word31> User name allows letters, numbers and underscores
privilege	Set user privilege level
priv	User privilege level
password	Specify the password for the user
encrypted	Specifies an ENCRYPTED password will follow
none	NULL password
unencrypted	Specifies an UNENCRYPTED password will follow

vlan <vlanid>

Description

Configure *VLAN*.

Syntax

`vlan` *`vlanid`*

Parameters

Name	Description
`vlanid`	Create an empty VLAN index. Valid values: 1 – 4094 Type: Mandatory

vlan <vlanid> <name>

Description

Configure *VLAN*'s name.

Syntax

vlan *`vlanid name`*

Parameters

Name	Description
vlanid	Create an empty VLAN index. Valid values: 1 – 4094 Type: Mandatory
name	VLAN Name (0–31) String Size:0–31 Type: Mandatory

vlan disable <vlanid>

Description

Delete *VLAN* memberset/setting.

Syntax

```
vlan disable vlanid
```

Parameters

Name	Description
vlanid	Valid values: 1 – 4094 Type: Mandatory

web

Description

Configure web privilege group names and levels.

Syntax

```
web privilege group group_namelevel {[crocro] [crwcrw] [srosro]
   [srwsrw]}*1
```

Parameters

Name	Description
privilege	Web privilege
group	Web privilege group
group_name	Valid words are Aggregation | DHCP | Debug | Dhcp_Client | Diagnostics | EEE | Green_Ethernet | IP2 | IPMC_Snooping | LACP | *LLDP* | Loop_Protect | MAC_Table | MVR | Maintenance | Mirroring | NTP | Ports | Private_VLANs | *QoS* | RPC | Security | Spanning_Tree | System | Timer | VCL | VLANs | Voice_VLAN | XXRP | sFlow
level	Web privilege group level
cro	Configuration Read-only level

Name	Description
crw	Configuration Read-write level
sro	Status/Statistics Read-only level
srw	Status/Statistics Read-write level
cro	<Cro : 0-15>
crw	<Crw : 0-15>
sro	<Sro : 0-15>
srw	<Srw : 0-15>

VLAN Mode Commands

vlan

Description

VLAN commands

Syntax

`vlan vlan_list`

Parameters

Name	Description
vlan_list	ISL VLAN IDs 1–4095

vlan ethertype s-custom-port

Description

Vlan Ether type for custom S-ports configuration

Syntax

`vlan ethertype s-custom-port 0x0600-0xffff`

Parameters

Name	Description
0x0600-0xffff	Ethertype range

vlan protocol

Description

Syntax

Syntax

```
vlan protocol {{eth2 {0x600-0xffff | arp | ip | ipx | at}} | {snap
   {0x0-0xffffff | rfc_1042 | snap_8021h} 0x0-0xffff} | {llc 0x0-0xff
   0x0-0xff}} group word16
```

Parameters

Name	Description
0x600-0xffff	Ether Type range
arp	Ether Type is ARP
ip	Ether Type is IP
ipx	Ether Type is IPX
at	Ether Type is AppleTalk
0x0-0xffffff	SNAP OUI range
rfc_1042	SNAP OUI is rfc_1042
snap_8021h	SNAP OUI is 8021h
0x0-0xffff	PID range
0x0-0xff	DSAP range
0x0-0xff	SSAP range
word16	Group Name. Valid values are 1 – 16 characters

vlan-trunking

Description

Change whether trunking of unknown VLANs is enabled

Syntax

```
vlan-trunking
```

Parameters

switchport access vlan

Description

Set switch access mode of the interface

Syntax

```
switchport access vlan vlan_id
```

Parameters

Name	Description
vlan_id	*VLAN* ID of the VLAN when this port is in access mode

switchport forbidden vlan

Description

Adds or removes forbidden *VLAN*s from the current list of forbidden VLANs

Syntax

```
switchport forbidden vlan {add | remove} vlan_list
```

Parameters

Name	Description
add	Add to existing list.
remove	Remove from existing list.
vlan_list	VLAN IDs

switchport hybrid acceptable-frame-type

Description

Set acceptable frame type on a port

Syntax

```
switchport hybrid acceptable-frame-type {all | tagged | untagged}
```

Parameters

Name	Description
all	Allow all frames
tagged	Allow only tagged frames
untagged	Allow only untagged frames

switchport hybrid allowed vlan

Description

Set allowed *VLAN* characteristics when interface is in hybrid mode

Syntax

```
switchport hybrid allowed vlan {all | none | [add | remove | except]
   vlan_list}
```

Parameters

Name	Description
all	All VLANs
none	No VLANs
add	Add VLANs to the current list
remove	Remove VLANs from the current list
except	All VLANs except the following
vlan_list	VLAN IDs of the allowed VLANs when this port is in hybrid mode

switchport hybrid egress-tag

Description

Egress *VLAN* tagging configuration

Syntax

```
switchport hybrid egress-tag {none | all [except-native]}
```

Parameters

Name	Description
none	No egress tagging
all	Tag all frames
except-native	Tag all frames except frames classified to native VLAN of the hybrid port

switchport hybrid ingress-filtering

Description

VLAN Ingress filter configuration

Syntax

```
switchport hybrid ingress-filtering
```

Parameters

switchport mode

Description

Set switching mode

Syntax

```
switchport mode {access | trunk | hybrid}
```

Parameters

Name	Description
access	Set mode to ACCESS unconditionally
trunk	Set mode to TRUNK unconditionally
hybrid	Set mode to HYBRID unconditionall

switchport trunk allowed vlan

Description

Set allowed *VLAN* characteristics when interface is in trunk mode

Syntax

```
switchport trunk allowed vlan {all | none | [add | remove | except]
   vlan_list}
```

Parameters

Name	Description
all	All VLANs
none	No VLANs
add	Add VLANs to the current list
remove	Remove VLANs from the current list
except	All VLANs except the following
vlan_list	VLAN IDs of the allowed VLANs when this port is in trunk mode

switchport vlan protocol group

Description

Protocol-based *VLAN* group commands

Syntax

```
switchport vlan protocol group word16 vlan vlan_id
```

Parameters

Name	Description
word16	Group Name (Range: 1 - 16 characters)
vlan_id	VLAN ID required for the group to VLAN mapping (Range: 1-4095)

Interface VLAN Mode Commands

interface

Description

Interface configuration

Syntax

`interface` **`port_type`** [*port_type_list*]

Parameters

Name	Description
port_type	Port type in Fast, Giga or Tengigaethernet
port_type_list	List of Port ID, ex, 1/1,3-5;2/2-4,6

interface vlan

Description

VLAN interface configurations

Syntax

`interface vlan` *vlan_list*

Parameters

Name	Description
vlan_list	List of VLAN interface numbers, range is 1 – 4095

ip address

Description

IPv4 address configurations

Syntax

`ip address {{`*ipv4_addr ipv4_netmask*`} | {`**`dhcp`** [**`fallback`** *ipv4_addr ipv4_netmask* [**`timeout`** *uint*]]}}

Parameters

Name	Description
ipv4_addr	IP address
ipv4_netmask	IP netmask

Name	Description
dhcp	Enable DHCP
fallback	DHCP fallback settings
ipv4_addr	DHCP fallback address (default is 192.0.2.1)
ipv4_netmask	DHCP fallback netmask
timeout	DHCP fallback timeout
uint	DHCP fallback timeout in seconds

ip dhcp excluded-address

Description

Prevent DHCP from assigning certain addresses

Syntax

```
ip dhcp excluded-address low_ip [high_ip]
```

Parameters

Name	Description
low_ip	Low IP address
high_ip	High IP addres

ip dhcp pool

Description

Pool name in 32 characters

Syntax

```
ip dhcp pool <pool_name>
```

Parameters

None.

ip dhcp relay

Description

DHCP relay agent configuration

Syntax

```
ipdhcp relay
```

Parameters

None.

ip dhcp relay information option

Description

IP DHCP relay information option(Option 82)

Syntax

```
ipdhcp relay information option
```

Parameters

None.

ip dhcp retry interface vlan

Description

Restart the DHCP query process

Syntax

```
ipdhcp retry interface vlan vlan_id
```

Parameters

Name	Description
vlan_id	Vlan ID

ip dhcp server

Description

DHCP Server

Syntax

```
ip dhcp server
```

Parameters

None.

ip dhcp snooping

Description

IP DHCP snooping

Syntax

```
ipdhcp snooping
```

Parameters

None.

ip helper-address

Description

DHCP relay server

Syntax

```
ip helper-address <v_ipv4_ucast>
```

Parameters

Name	Description
v_ipv4_ucast	IP address of the DHCP relay server

ip name-server

Description

Interface Internet Protocol config commands Domain Name System

Syntax

```
ip name-server {ipv4_ucast | dhcp [interface vlan vlan_id]}
```

Parameters

Name	Description
ipv4_ucast	A valid IPv4 unicast address
vlan_id	*VLAN* identifier(s): VID

ipv6 address

Description

Configure the IPv6 address of an interface

Syntax

```
ipv6 address ipv6_subnet
```

Parameters

Name	Description
ipv6_subnet	IPv6 prefix x:x::y/z

ipv6mtu

Description

IPv6 Maximum transmission unit

Syntax

`ipv6 mtu 1280-1500`

Parameters

Name	Description
1280-1500	MTU value in bytes

RingV2 Group Mode Commands

ringv2 protect

Description

To configure ring protection.

Syntax

`ring protect`

Parameters

Name	Description
group1	Configure ring protection v2 group1 (Ring)
group2	Configure ring protection v2 group2 (Ring)
group3	Configure ring protection v2 group3 (Chain)

guard-time

Description

Set guard time

Syntax

`guard-time {ringGuardTimerDef}`

Parameters

Name	Description
ringGuardTimerDef	<10-3600>, unit: secound. Default is 10 seconds

mode

Description

Enable/Disable ring group

Syntax

`mode {disable | enable}`

Parameters

Name	Description
disable	Set the specified Ring group to Disabled
enable	Set the specified Ring group to Enabled

node1 interface GigabitEthernet <portNo>}

Description

Set interface of ring protection node

Syntax

`node1 interface GigabitEthernet portNo`

Parameters

Name	Description
portNo	Valid values: 1-max port index.

node2 interface GigabitEthernet <portNo>}

Description

Set interface of ring protection node

Syntax

`Node2 interface GigabitEthernet portNo`

Parameters

Name	Description
portNo	Valid values: 1-max port index.

role

Description

Set role for group

Syntax

```
role {ring-master | ring-slave | coupling-primary | coupling-backup |
   dual-homing | chain-head | chain-tail | chain-member | b-chain-
   terminal-1 | b-chain-terminal-2 | b-chain-central-block | b-chain-
   member}
```

Parameters

Name	Description
ring-master	Set role to ring master
ring-slave	Set role to ring slave
coupling-primary	Set role to coupling primary
coupling-backup	Set role to coupling backup
dual-homing	Set role to dual homing
chain-head	Set role to chain head
chain-member	Set role to chain member
chain-tail	Set role to chain tail
b-chain-central-block	Set role to balancing chain central block
b-chain-member	Set role to balancing chain member
b-chain-terminal-1	Set role to balancing chain terminal 1
b-chain-terminal-2	Set role to balancing chain terminal 2

Spanning Tree

spanning-tree

Description

Enabe/disable *STP* on this interface

Syntax

```
spanning-tree
```

Parameters

None.

spanning-tree aggregation

Description

Spanning Tree protocol

Syntax

```
spanning-tree aggregation
```

Parameters

None.

spanning-tree auto-edge

Description

Auto detect edge status

Syntax

```
spanning-tree auto-edge
```

Parameters

None.

spanning-tree bpdu-guard

Description

Enable/disable BPDU guard

Syntax

```
spanning-tree bpdu-guard
```

Parameters

None.

spanning-tree edge

Description

Edge port

spanning-tree

STP Bridge

Syntax

```
spanning-tree edge
```

Parameters

None.

spanning-tree edge bpdu-filter

Description

Enable BPDU filter (stop BPDU tx/rx)

Syntax

```
spanning-tree edge bpdu-filter
```

Parameters

None.

spanning-tree mode

Description

Spanning Tree mode

STP protocol mode

stp

802.1D Spanning Tree

rstp

Rabid Spanning Tree (802.1w)

mstp

Multiple Spanning Tree (802.1s)

Syntax

```
spanning-tree mode {stp | rstp | mstp}
```

Parameters

Name	Description
stp	802.1D Spanning Tree
rstp	Rabid Spanning Tree (802.1w)
mstp	Multiple Spanning Tree (802.1s)

spanning-tree mst cost

Description

STP bridge instance

STP Cost of this port

Syntax

```
spanning-tree mst 0-7 cost {1-200000000 | auto}
```

Parameters

Name	Description
0-7	instance 0-7 (CIST=0, MST2=1...)
1-200000000	STP Cost of this port

spanning-tree mst port-priority

Description

port-priority

Syntax

```
spanning-tree mst 0-7 port-priority 0-240
```

Parameters

Name	Description
0-7	instance 0-7 (CIST=0, MST2=1...)
0-240	*STP* priority of this port

spanning-tree mst priority

Description

Priority of the instance. Range in seconds.

Syntax

```
spanning-tree mst 0-7 priority 0-61440
```

Parameters

Name	Description
0-7	instance 0-7 (CIST=0, MST2=1...)
0-61440	Priority of the instance

spanning-tree mst vlan

Description

VLAN keyword

Syntax

```
spanning-tree mst 0-7 vlan vlan_list
```

Parameters

Name	Description
0-7	instance 0-7 (CIST=0, MST2=1...)
vlan_list	Range of VLANs

spanning-tree mst forward-time

Description

forward-time

Delay between port states

Syntax

```
spanning-tree mst forward-time 4-30
```

Parameters

Name	Description
4-30	Delay between port states

spanning-tree mst max-age

Description

Max bridge age before timeout.

Syntax

```
spanning-tree mst max-age 6-40 [forward-time 4-30 ]
```

Parameters

Name	Description
6-40	Max bridge age before timeout
4-30	forward-time

spanning-tree mst max-hops

Description

MSTP bridge max hop count

Syntax

```
spanning-tree mst max-hops 6-40
```

Parameters

Name	Description
6-40	MSTP bridge max hop count

spanning-tree mst name

Description

Name of the bridge

Revision

Revision keyword

Syntax

spanning-tree mst name *word32* revision *0-65535*

Parameters

Name	Description
word32	Name of the bridge
0-65535	Revision keyword

spanning-tree mst <instance>

Description

instance 0-7 (CIST=0, MST2=1...)

Syntax

spanning-tree mst *instance* **priority** *prio*

spanning-tree mst *instance* **vlan** *v_vlan_list*

Parameters

Name	Description
instance	<Instance : 0-7> instance 0-7 (CIST=0, MST2=1...)
priority	Priority of the instance
vlan	*VLAN* keyword
prio	<Prio : 0-61440> Range in seconds
v_vlan_list	<vlan_list> Range of VLANs

spanning-tree recovery

Description

Recovery

Syntax

```
spanning-tree recovery interval interval
```

Parameters

Name	Description
interval	The interval
interval;	Interval : 30-86400 seconds

spanning-tree transmit

Description

Transmit

Syntax

```
spanning-tree transmit hold-count holdcount
```

Parameters

Name	Description
hold-count	Max number of transmit BPDUs per sec
holdcount	<Holdcount : 1-10> 1-10 per sec, 6 is default

sFlow Configure Command

sflow

Description

Enables/disables flow sampling on this port.

Syntax

```
sflow [range_list]
```

Parameters

Name	Description
range_list	Sampler instance

sflow agent-ip

Description

The agent IP address used as agent-address in UDP datagrams. Defaults to IPv4 loopback address.

Syntax

```
sflow agent-ip {ipv4 ipv4_addr | ipv6 ipv6_addr}
```

Parameters

Name	Description
ipv4_addr	IPv4 address
ipv6_addr	IPv6 address

sflow collector-address

Description

Sflow runtime, see sflow_icli_functions

Syntax

```
sflow collector-address [receiver range_list] [word]
```

Parameters

Name	Description
range_list	Sampler instance

sflow max-datagram-size

Description

Statistics flow Maximum datagram size.

Syntax

```
sflow max-datagram-size [receiver range_list] 200-1468
```

Parameters

Name	Description
range_list	receiver list
200-1468	packet byte

sflow max-sampling-size

Description

Specifies the maximum number of bytes to transmit per flow sample.

Syntax

```
sflow max-sampling-size [sampler range_list] [14-200]
```

Parameters

Name	Description
range_list	Sampler instance
200-1468	packet byte

sflow collector-port

Description

Collector UDP port

Syntax

```
sflow collector-port [receiver rcvr_idx_list] collector_port
```

Parameters

Name	Description
collector_port	<Collector Port : 1-65535> Port number

sflow sampling-rate

Description

Specifies the statistical sampling rate. The sample rate is specified as N to sample 1/Nth of the packets n the monitored flows. There are no restrictions on the value, but the switch will adjust it to the closest possible sampling rate.

Syntax

```
sflow sampling-rate [sampler range_list] [1-4294967295]
```

Parameters

Name	Description
range_list	Sampler instance
1-4294967295	Sampling rate

sflow timeout

Description

Receiver timeout measured in seconds. The switch decrements the timeout once per second, and as long as it is non-zero, the receiver receives samples. Once the timeout reaches 0, the receiver and all its configuration is reset to defaults.

Syntax

```
sflow timeout [receiver range_list] 0-2147483647
```

Parameters

Name	Description
range_list	Sampler instance
0-2147483647	Number of seconds.

SNMP Configure Command

snmp-server

Description

Enable *SNMP* server

Syntax

```
snmp-server
```

Parameters

None.

snmp-server access

Description

snmp-server access configuration

Syntax

```
snmp-server access group name model {v1 | v2c | v3 | any} level {auth |
   noauth | priv} [read word255] [write word255]
```

Parameters

Name	Description
group name	32 words
v1 | v2c | v3 | any	V1-v3 security model
level	security level
auth | noauth | priv	authNoPriv Security Level noAuthNoPriv Security Level authPriv Security Level

Name	Description
read	specify a read view for the group
word255	read view name

snmp-server community v2c

Description

Set the *SNMP* v2c community

Syntax

```
snmp-server community v2c word127 [ro | rw]
```

Parameters

Name	Description
word127	Community word
ro	Read only
rw	Read write

snmp-server community v3

Description

S Set the *SNMP* v3 community

Syntax

```
snmp-server community v3 word127 [ipv4_addr ipv4_netmask]
```

Parameters

Name	Description
word127	Community word
ipv4_addr	IPv4 address
ipv4_netmask	IPv4 netmask

snmp-server host

Description

Set *SNMP* server's configurations

Syntax

```
snmp-server host word32
```

Parameters

Name	Description
word32	Name of the host configuration

snmp-server host traps

Description

Set *SNMP* host's configurations

Syntax

```
snmp-server host Name of the host configuration traps [linkup]
   [linkdown] [lldp]
```

Parameters

Name	Description
Name of the host configuration	Name of the host configuration
linkup	Link up event
linkdown	Link down event
lldp	*LLDP* event

snmp-server trap

Description

Set *SNMP* server's configurations

Syntax

```
snmp-server trap
```

Parameters

None.

snmp-server user

Description

Set the SNMPv3 user's configurations

Syntax

```
snmp-server user Username engine-id Engine ID octet string [{md5
   word8-32 | sha word8-40} [priv {des | aes} word8-32]]
```

Parameters

Name	Description
Username	32 words
Engine ID octet string	word10-32
md5	Set *MD5 (Message-Digest algorithm 5)* protocol
sha	Set SHA protocol
word8-40	SHA password
priv	Set Privacy
des | aes	Set DES/AES protocol
word8-32	Set privacy password

snmp-server version

Description

Set the *SNMP* server's version

Syntax

```
snmp-server version {v1 | v2c | v3}
```

Parameters

Name	Description
v1 | v2c | v3	SNMP v1,v2c,v3

snmp-server view

Description

Snmp MIB view configuration

Syntax

```
snmp-server view word32 word255 {include | exclude}
```

Parameters

Name	Description
word32	MIB view name
word255	MIB view OID
include | exclude	Included/Excluded type from the view

SNMP trap receive ipv6 host

Description

host configuration

Syntax

`host ipv6_ucast [1-65535] [traps | informs]`

Parameters

Name	Description
ipv6_ucast	IP address of *SNMP* trap host
1-65535	UDP port of the trap messges
traps	Send Trap messages to this host
informs	Send Inform messages to this host

snmp-server contact

Description

SNMP server contact

Syntax

`snmp-server contact v_line255`

Parameters

Name	Description
v_line255	Contact string

snmp-server engine-id

Description

SNMP server engine ID

Syntax

`snmp-server engine-id local engineID`

Parameters

Name	Description
local	Set SNMP local engine ID
engineID	<Engineid : word10-32> local engine ID

snmp-server location

Description

SNMP server loation

Syntax

```
snmp-server location v_line255
```

Parameters

Name	Description
v_line255	<line255> location string

snmp-server security-to-group

Description

SNMP server security

Syntax

```
snmp-server security-to-group model {v1 | v2c | v3} name
   security_namegroupgroup_name
```

Parameters

Name	Description
model	security model
v1	v1 security model
v2c	v2c security model
v3	v3 security model
name	security user
security_name	<SecurityName : word32> security user name
group	security group
group_name	<GroupName : word32> security group name

SNMP trap receive ipv4 host

Description

Host configuration

Syntax

```
host {ipv4_ucast | hostname} [1-65535 ] [traps | informs]
```

Parameters

Name	Description
ipv4_ucast	IP address of *SNMP* trap host
hostname	hostname of SNMP trap host
1-65535	UDP port of the trap messges
traps	Send Trap messages to this host
informs	Send Inform messages to this host

QoS Function Command

qos qce

Description

QCE setting

Syntax

```
qos qce {Id : 1-256 | refresh | update }
```

Parameters

Name	Description
Id : 1-256	QCE ID
refresh	Refresh QCE tables in hardware
update	Update an existing QCE

qos storm

Description

QoS storm

Syntax

```
qos storm {unicast | multicast | broadcast} {{rate [kfps]} | {1024
   kfps}}
```

Parameters

Name	Description
broadcast	Police broadcast frames
multicast	Police multicast frames

Name	Description
unicast	Police unicast frames
rate	1024, Rate is 1024 kfps <Rate : 1,2,4,8,16,32,64,128,256,512> Policer rate (default fps)

qos cos

Description

Class of service configuration

Syntax

```
qos cos 0-7
```

Parameters

Name	Description
0-7	Specific class of service

qos dscp-classify

Description

Set qos dscp-classify.

Syntax

```
qos dscp-classify {zero | selected | any}
```

Parameters

None.

qos dscp-remark

Description

Set qos dscp-remark

Syntax

```
qos dscp-remark { rewrite | remap | remap-dp }
```

Parameters

None.

qos dscp-translate

Description

Enable Qos DSCP-translate mode

Syntax

```
qos dscp-translate
```

Parameters

None.

qos map cos-dscp

Description

Configure cos mapping to dscptable

Syntax

```
qos map cos-dscp 0-7 dpl 0-1 dscp {0-63 | {be | af11 | af12 | af13 |
   af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 |
   cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va}}
```

Parameters

Name	Description
0-7	Cos level
0-1	Specific drop precedence level
0-63	Dscp level
be	Default PHB(DSCP 0) for best effort traffic
af11-13	Assured Forwarding PHB 11-13(DSCP 10,12,14)
af22-23	Assured Forwarding PHB 22-23(DSCP 20,22)
af31-33	Assured Forwarding PHB 31-33(DSCP 26,28,30)
Af41-43	Assured Forwarding PHB 41-43(DSCP 34,36,38)
cs1-7	Class Selector PHB CS1-7 precedence 1-7(DSCP 8*(cs value))
ef	Expedited Forwarding PHB(DSCP 46)
va	Voice Admit PHB(DSCP 44)

qos map dscp-cos

Description

Configure dscp mapping to cos table

Syntax

```
qos map dscp-cos {0-63 | {be | af11 | af12 | af13 | af21 | af22 | af23 |
   af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5
   | cs6 | cs7 | ef | va}} cos 0-7 dpl dpl
```

Parameters

Name	Description
0-7	Cos level
0-63	Dscp level
be	Default PHB(DSCP 0) for best effort traffic
af11-13	Assured Forwarding PHB 11-13(DSCP 10,12,14)
af22-23	Assured Forwarding PHB 22-23(DSCP 20,22)
af31-33	Assured Forwarding PHB 31-33(DSCP 26,28,30)
af41-43	Assured Forwarding PHB 41-43(DSCP 34,36,38)
cs1-7	Class Selector PHB CS1-7 precedence 1-7(DSCP 8*(cs value))
ef	Expedited Forwarding PHB(DSCP 46)
va	Voice Admit PHB(DSCP 44)
0-1	Specific drop precedence level

qos map dscp-egress-translation

Description

Configure dscp egress-translation

Syntax

```
qos map dscp-egress-translation {0-63 | {be | af11 | af12 | af13 | af21
   | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 |
   cs3 | cs4 | cs5 | cs6 | cs7 | ef | va}} 0-1 to {0-63 | {be | af11 |
   af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 |
   af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va}}
```

Parameters

Name	Description
0-7	Cos level
0-63	Dscp level
be	Default PHB(DSCP 0) for best effort traffic
af11-13	Assured Forwarding PHB 11-13(DSCP 10,12,14)
af22-23	Assured Forwarding PHB 22-23(DSCP 20,22)
af31-33	Assured Forwarding PHB 31-33(DSCP 26,28,30)
af41-43	Assured Forwarding PHB 41-43(DSCP 34,36,38)

Name	Description
cs1–7	Class Selector PHB CS1–7 precedence 1–7(DSCP 8*(cs value))
ef	Expedited Forwarding PHB(DSCP 46)
va	Voice Admit PHB(DSCP 44)
0–1	Specific drop precedence level

qos map dscp-ingress-translation

Description

Configure dscp ingress-translation

Syntax

```
qos map dscp-ingress-translation {0–63 | {be | af11 | af12 | af13 | af21
   | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 |
   cs3 | cs4 | cs5 | cs6 | cs7 | ef | va}} to {0–63 | {be | af11 | af12
   | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43
   | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va}}
```

Parameters

Name	Description
0–7	CoS level
0–63	DSCP level
be	Default PHB(DSCP 0) for best effort traffic
af11–13	Assured Forwarding PHB 11–13(DSCP 10,12,14)
af22–23	Assured Forwarding PHB 22–23(DSCP 20,22)
af31–33	Assured Forwarding PHB 31–33(DSCP 26,28,30)
af41–43	Assured Forwarding PHB 41–43(DSCP 34,36,38)
cs1–7	Class Selector PHB CS1–7 precedence 1–7(DSCP 8*(cs value))
ef	Expedited Forwarding PHB(DSCP 46)
va	Voice Admit PHB(DSCP 44)
0–1	Specific drop precedence level

qos policer

Description

Configure qos policer

Syntax

```
qos policer unit [fps] [flowcontrol]
```

Parameters

Name	Description
unit	Traffic meter
fps	Frame rate
flowcontrol	Enable flowcontrol mode

qos wrr

Description

Specifies qos wrr mode

Syntax

`qos wrr 1-100 1-100 1-100 1-100 1-100 1-100`

Parameters

Name	Description
1-100	every level proportion

qos queue-shaper

Description

Configure queue-shaper command

Syntax

`qos queue-shaper queue 0-7 unit [excess]`

Parameters

Name	Description
1-100	every level proportion
unit	Traffic meter
excess	Agree the shaper could be excess or not

qos queue-policer

Description

Configure queue-policer command

Syntax

`qos queue-policer queue 0-7 unit`

Parameters

Name	Description
0–7	Queue number
unit	Traffic meter

qos shaper <unit>

Description

Configure *QoS* shaper command

Syntax

```
qos shaper unit
```

Parameters

Name	Description
1–100	every level proportion
unit	Traffic meter

IGMP Functional Commands

ip igmp host-proxy [leave-proxy]

Description

IGMP proxy for leave configuration

Syntax

```
ip igmp host-proxy [leave-proxy]
```

Parameters

Name	Description
leave-proxy	IGMP proxy for leave

ip igmp snooping

Description

Snooping *IGMP*

Syntax

```
ip igmp snooping
```

Parameters

None.

ip imp snooping immediate-leave

Description

IP *IGMP* snooping immediate leave configuration

Syntax

```
ip igmp snooping immediate-leave
```

Parameters

None.

ip igmp snooping last-member-query-interval

Description

IP *IGMP* snooping Last Member Query Interval in tenths of seconds

Syntax

```
ip igmp snooping last-member-query-interval 0-31744
```

Parameters

Name	Description
0-31744	0 - 31744 tenths of seconds

ip igmp snooping max-groups

Description

IGMP group throttling configuration

Syntax

```
ip igmp snooping max-groups 1-10
```

Parameters

Name	Description
1-10	Maximum number of IGMP group registration

ip igmp snooping mrouter

Description

IP *IGMP* snooping Multicast router port configuration

Syntax

```
ip igmp snooping mrouter
```

Parameters

None.

ip igmp snooping querier

Description

IP *IGMP* querier configuration

Syntax

```
ip igmp snooping querier {election | address ipv4_ucast}
```

Parameters

Name	Description
election	Act as an IGMP Querier to join Querier-Election
address	IGMP Querier address configuration
ipv4_ucast	A valid IPv4 unicast address

ip igmp snooping query-interval

Description

IP *IGMP* snooping Query-Interval in seconds

Syntax

```
ip igmp snooping query-interval 1-31744
```

Parameters

Name	Description
1-317	1 - 31744 seconds

ip igmp snooping vlan

Description

IP *IGMP* snooping vlan IDs

Syntax

```
ip igmp snooping vlan vlan_list
```

Parameters

Name	Description
vlan_list	*VLAN* identifier(s): VID

ip igmp ssm-range

Description

SSM range

Syntax

```
ip igmp ssm-range v_ipv4_mcast ipv4_prefix_length
```

Parameters

Name	Description
v_ipv4_mcast	Valid IPv4 multicast address
ipv4_prefix_length	Length

ip igmp unknown-flooding

Description

IP *IGMP* flooding unregistered IPv4 multicast traffic

Syntax

```
ip igmp unknown-flooding
```

Parameters

None.

clear ip igmp snooping statistics

Description

Clear IP *IGMP* snooping statistics

Syntax

```
clear ip igmp snooping [vlan vlan_list] statistics
```

Parameters

Name	Description
vlan_list	*VLAN* list.

MVR Functional Commands

mvr

Description

Multicast *VLAN* Registration configuration

Syntax

```
mvr
```

Parameters

None.

mvr immediate-leave

Description

MVR immediate leave configuration

Syntax

```
mvr immediate-leave
```

Parameters

None.

mvr name channel

Description

Multicast *VLAN* name and channel configuration

Syntax

```
mvr name word16 channel word16
```

Parameters

Name	Description
name	MVR multicast VLAN name
channel <*word16*>	Profile name in 16 char's

mvr frame priority

Description

Multicast *VLAN* interface *CoS* priority

Syntax

```
mvr name word16 frame priority 0-7
```

Parameters

Name	Description
name	MVR multicast VLAN name
0-7	CoS priority ranges from 0 to 7

mvr name <word16> frame tagged

Description

MVR control frame in TX, Tagged *IGMP*/MLD frames will be sent

Syntax

```
mvr name word16 frame tagged
```

Parameters

Name	Description
name	MVR multicast *VLAN* name

mvr name <word16> igmp-address <ipv4_ucast>

Description

MVR address configuration used in *IGMP*

Syntax

```
mvr name word16 igmp-address ipv4_ucast
```

Parameters

Name	Description
name	MVR multicast *VLAN* name
ipv4_ucast	A valid IPv4 unicast address

mvr name <word16> last-member-query-interval <0-31744>

Description

Configure last Member Query Interval in tenths of seconds

Syntax

```
mvr name word16 last-member-query-interval 0-31744
```

Parameters

Name	Description
name	MVR multicast *VLAN* name
0–31744	0 - 31744 tenths of seconds

mvr name <word16> mode

Description

Dynamic MVR operation mode

Syntax

`mvr name word16 mode {dynamic | compatible}`

Parameters

Name	Description
dynamic	Dynamic MVR operation mode
compatible	Compatible MVR operation mode

mvr name <word16> type

Description

MVR port role configuration

Syntax

`mvr name word16 type {source | receiver}`

Parameters

Name	Description
source	MVR source port
receiver	MVR receiver port

mvr vlan

Description

Multicast *VLAN* Registration configuration

Syntax

`mvr vlan vlan_list [name word16]`

Parameters

Name	Description
vlan_list	MVR multicast VLAN list
word16	MVR multicast VLAN name in 16 char's

mvr vlan <vlan_list> channel

Description

MVR channel configuration

Syntax

`mvr vlan vlan_list channel word16`

Parameters

Name	Description
vlan_list	MVR multicast *VLAN* list
word16	MVR multicast channel name in 16 char's

mvr vlan <vlan_list> frame priority

Description

Interface *CoS* priority

Syntax

`mvr vlan vlan_list frame priority 0-7`

Parameters

Name	Description
vlan_list	MVR multicast *VLAN* list
0-7	CoS priority ranges from 0 to 7

mvr vlan <vlan_list> frame tagged

Description

Set tagged *IGMP*/MLD frames will be sent

Syntax

`mvr vlan vlan_list frame tagged`

Parameters

Name	Description
vlan_list	MVR multicast *VLAN* list

mvr vlan <vlan_list> igmp-address

Description

Set tagged *IGMP*/MLD frames will be sent

Syntax

```
mvr vlan vlan_list igmp-address ipv4_ucast
```

Parameters

Name	Description
< vlan_list >	MVR multicast *VLAN* list
<ipv4_ucast>	A valid IPv4 unicast address for IGMP

mvr vlan <vlan_list> mode

Description

Dynamic MVR vlan operation mode

Syntax

```
mvr vlan vlan_list mode {dynamic | compatible}
```

Parameters

Name	Description
vlan_list	MVR multicast *VLAN* list
dynamic	Dynamic MVR operation mode
compatible	Compatible MVR operation mode

mvr vlan <vlan_list> type

Description

MVR vlan role configuration

Syntax

```
mvr vlan vlan_list type {source | receiver}
```

Parameters

Name	Description
vlan_list	MVR multicast *VLAN* list
source	MVR source port
receiver	MVR receiver port

MLD Functional Commands

ipv6 mld host-proxy

Description

IPv6 MLD proxy configuration

Syntax

```
ipv6 mld host-proxy [leave-proxy]
```

Parameters

Name	Description
leave-proxy	MLD proxy for leave configuration

ipv6 mld snooping

Description

IPv6 MLD snooping

Syntax

```
ipv6 mld snooping
```

Parameters

None.

ipv6 mld snooping compatibility

Description

IPv6 MLD snooping compatibility configuration

Syntax

```
ipv6 mld snooping compatibility {auto | v1 | v2}
```

Parameters

Name	Description
auto	Compatible with MLDv1/MLDv2
v1	Forced MLDv1
v2	Forced MLDv2

ipv6 mld snooping immediate-leave

Description

IPv6 MLD snooping immediate-leave configuration

Syntax

```
ipv6 mld snooping immediate-leave
```

Parameters

None.

ipv6 mld snooping last-member-query-interval

Description

IPv6 MLD snooping last member query interval in tenths of seconds

Syntax

```
ipv6 mld snooping last-member-query-interval 0-31744
```

Parameters

Name	Description
0-31744	0 - 31744 tenths of seconds

ipv6 mld snooping max-groups

Description

IPv6 MLD group throttling configuration

Syntax

```
ipv6 mld snooping max-groups 1-10
```

Parameters

Name	Description
1-10	Maximum number of MLD group registration

ipv6 mld snooping mrouter

Description

IPv6 MLD snooping multicast router port configuration

Syntax

```
ipv6 mld snooping mrouter
```

Parameters

None.

ipv6 mld snooping query-interval

Description

IPv6 MLD snooping query interval in seconds

Syntax

```
ipv6 mld snooping query-interval 1-31744
```

Parameters

Name	Description
1-31744	1 - 31744 seconds

ipv6 mld snooping query-max-response-time

Description

IPv6 MLD snooping querymaxresponse interval in tenths of seconds

Syntax

```
ipv6 mld snooping query-max-response-time 0-31744
```

Parameters

Name	Description
0-31744	0 - 31744 tenths of seconds

ipv6 mld snooping vlan

Description

IPv6 MLD snooping vlan

Syntax

```
ipv6 mld snooping vlan vlan_list
```

Parameters

Name	Description
vlan_list	*VLAN* identifier(s): VID

ipv6 mld ssm-range

Description

SSM range

Syntax

```
ipv6 mld ssm-range v_ipv6_mcast ipv6_prefix_length
```

Parameters

Name	Description
v_ipv6_mcast	Valid IPv6 multicast address
ipv6_prefix_length	length

ipv6 mld unknown-flooding

Description

Flooding unregistered IPv6 multicast traffic

Syntax

```
ipv6 mld unknown-flooding
```

Parameters

None.

ipv6 route

Description

IPv6 Route

Syntax

```
ipv6 route v_ipv6_subnet {v_ipv6_ucast | interface vlan v_vlan_id
   v_ipv6_addr}
```

Parameters

Name	Description
v_ipv6_subnet	IPv6 prefix x:x::y/z
v_ipv6_ucast	IP address of the DHCP relay server
v_vlan_id	*VLAN* ID
v_ipv6_addr	IP address

Authenticate Mode Commands

radius-server attribute 32

Description

Configure radius-server attribute

Syntax

```
radius-server attribute 32 id
```

Parameters

Name	Description
id	Id : line 1-253

radius-server attribute 4

Description

Configure radius-server attribute

Syntax

```
radius-server attribute 4 ipv4_ucast
```

Parameters

Name	Description
ipv4_ucast	ipv4_ucast address

radius-server attribute 95

Description

Configure radius-server attribute

Syntax

```
radius-server attribute 95 ipv6_ucast
```

Parameters

Name	Description
ipv6_ucast	ipv6_ucast address

radius-server deadtime

Description

Configure *RADIUS (Remote Authentication Dial In User Service)*-server deadtime

Syntax

```
radius-server deadtime 1-1440
```

Parameters

Name	Description
1-1440	Time in minutes

radius-server host [auth-port] [acct-port] [timeout] [retransmit] [key]

Description

Configure *RADIUS*-server host behavior

Syntax

```
radius-server host word1-255 [auth-port 0-65535] [acct-port 0-65535]
   [timeout 1-1000] [retransmit 1-1000] [key line1-63]
```

Parameters

Name	Description
word1-255	Hostname or IP address
0-65535	UDP port number for RADIUS authentication server
0-65535	UDP port number for RADIUS accounting server
1-1000	Wait time in seconds for this RADIUS server to reply (overrides default)

radius -server key

Description

RADIUS-server key

Syntax

```
radius-server key key
```

Parameters

Name	Description
key	<Key : line1-63> The shared key

radius-server retransmit

Description

RADIUS server retransmit

Syntax

```
radius-server retransmit retries
```

Parameters

Name	Description
retries	<Retries : 1-1000> Number of retries for a transaction

radius-server timeout

Description

RADIUS-server timeout

Syntax

```
radius-server timeout seconds
```

Parameters

Name	Description
seconds	<Seconds : 1-1000> Wait time in second

tacacs-server deadtime <1-1440>

Description

Time to stop using a TACACS+ server that doesn't respond

Syntax

```
tacacs-server deadtime 1-1440
```

Parameters

Name	Description
1-1440	Time in minutes

tacacs-server host

Description

Configure TACACS+ server host behavior

Syntax

```
tacacs-server host [auth-port] [timeout] [key]
```

dot1x authentication timer

Description

dot1x authentication timer

Syntax

```
dot1x authentication timer {inactivity v_10_to_100000} | {re-
   authenticate v_1_to_3600}
```

Parameters

Name	Description
inactivity	Time in seconds between check for activity on successfully authenticated MAC addresses
re-authenticate	The period between re-authentication attempts in seconds

dot1x feature

Description

Globally enables/disables a dot1x feature functionality

Syntax

```
dot1x feature {[guest-vlan] [radius-qos] [radius-vlan]}
```

Parameters

Name	Description
guest-vlan	Globally enables/disables state of guest-vlan
radius-qos	Globally enables/disables state of *RADIUS*-assigned *QoS*.
radius-vlan	Globally enables/disables state of RADIUS-assigned *VLAN*.

dot1x guest-vlan

Description

G Enables/disables Guest *VLAN* globally or on one or more ports

Syntax

```
dot1x guest-vlan
dot1x guest-vlan 1-4095
```

Parameters

Name	Description
1-4095	Guest VLAN ID used when entering the Guest VLAN.

dot1x initialize

Description

Forces a re-initialization of the clients on the port and thereby an immediate reauthentication

Syntax

```
dot1x initialize [interface port_type [port_type_list]]
```

Parameters

Name	Description
port_type	Port type in Fast, Giga or Tengigaethernet
port_type_list	List of Port ID, ex, 1/1,3-5;2/2-4,6

dot1x max-reauth-req

Description

Max value of authentication request

Syntax

```
dot1x max-reauth-req 1-255
```

Parameters

Name	Description
<1-255>	number of times

dot1x port-control

Description

Sets the port security state.

Syntax

```
dot1x port-control {force-authorized | force-unauthorized | auto |
   single | multi | mac-based | sense}
```

Parameters

Name	Description
force-authorized	Port access is allowed
force-unauthorized	Port access is not allowed
auto	Port-based 802.1x authentication
single	Single Host 802.1x authentication
multi	Multiple Host 802.1x authentication
mac-based	Switch authenticates on behalf of the client
sense	Sense whether the port received EAP/EAPOL packets after the port was connected (used to determine whether 802.1x is enabled on the client)

dot1x radius-vlan

Description

Enables/disables per-port state of *RADIUS*-assigned *VLAN*.

Syntax

```
dot1x radius-vlan
```

Parameters

None.

dot1x re-authentication

Description

re-authentication

Syntax

```
dot1x re-authentication
```

Parameters

None.

dot1x system-auth-controln

Description

System authentication control

Syntax

```
dot1x system-auth-control
```

Parameters

None.

dot1x timeout

Description

Timeout control

Syntax

```
dot1x timeout {quiet-period v_10_to_1000000} | {sense-period
   v_10_to_255} | {tx-period v_1_to_65535}
```

Parameters

Name	Description
quiet-period	Time in seconds before a MAC-address that failed authentication gets a new authentication chance.
sense-period	Time in seconds for sensing whether the port received EAP/EAPOL packets after the port was connected. Used to determine whether 802.1x is enabled on the client. Valid values are between 10 and 255 seconds. The default is 10 seconds.
tx-period	Time in seconds between EAPOL retransmissions.

show radius-server [statistics]

Description

Show *RADIUS*-server statistics

Syntax

```
show radius-server [statistics]
```

Parameters

Name	Description
statistics	Count RADIUS packet statistics

enable

Description

Privilege level control

Syntax

```
Enable {password [level priv] password} | {secret {0 | 5} [level priv]
   password}
```

Parameters

Name	Description
password	Assign the privileged level clear password
secret	Assign the privileged level secret

end

Description

Level exit

Syntax

```
end
```

Parameters

None.

exit

Description

Level exit

Syntax

```
end
```

Parameters

None.

hostname

Description

This system's network name

Syntax

```
hostname hostname
```

Parameters

None.

Loop-Protection Configure commands

loop-protect

Description

Loop protection configuration on port

Syntax

```
loop-protect
```

Parameters

None.

loop-protect action

Description

Loop protection configuration on port

Syntax

```
loop-protect action {[shutdown] [log]
```

Parameters

Name	Description
shutdown	Shutdown port
log	Generate log

loop-protect shutdown-time

Description

Loop protection shutdown time interval

Syntax

```
loop-protect shutdown-time 0-604800
```

Parameters

Name	Description
0-604800	Shutdown time in second

loop-protect transmit-time

Description

Loop protection transmit time interval

Syntax

```
loop-protect transmit-time 1-10
```

Parameters

None.

loop-protect tx-mode

Description

Loop protection actively generate PDUs

Syntax

```
loop-protect tx-mode
```

Parameters

None.

LLDP Configure commands

lldp holdtime

Description

Sets *LLDP* hold time (The neighbor switch will discarded the LLDP information after \"hold time\" multiplied with \"timer\" seconds).

Syntax

```
lldp holdtime 2-10
```

Parameters

Name	Description
2-10	Holdtime 2-10 seconds

lldp med

Description

LLDP MED

Syntax

See parameters.

Parameters

Name	Description
datum	Datum (geodetic system) type • nad83-mllw: Mean lower low water datum 1983 • nad83-navd88: North American vertical datum 1983 • wgs84: World Geodetic System 1984
fast	Number of times to repeat LLDP frame transmission at fast start <v_1_to_10> : <1-10>
location-tlv	LLDP-MED Location Type Length Value parameter • altitude: Altitude parameter • elin-addr: Emergency Location Identification Number (e.g., E911 and others), as defined by TIA or NENA. • Latitude: Latitude parameter • Longitude parameter
media-vlan-policy	Use the media-vlan-policy to create a policy, which can be assigned to an interface <Index : 0-31> : Policy id for the policy which is created

lldp receive

Description

Enable/Disable decoding of received *LLDP* frames.

Syntax

```
lldp receive
```

lldp reinit <1-10>

Description

LLDP TX reinitialization delay in seconds.

Syntax

```
lldp reinit 1-10
```

Parameters

Name	Description
1-10	Reinitialization delay time

lldp timer <5-32768>

Description

Sets *LLDP* TX interval (the time between each LLDP frame transmitted in seconds).

Syntax

```
lldp timer 5-32768
```

Parameters

Name	Description
5-32768	5-32768 seconds.

lldp tlv-select

Description

Which optional TLVs to transmit.

Syntax

```
lldp tlv-select {management-address | port-description | system-
   capabilities | system-description | system-name}
```

Parameters

Name	Description
management-address	Enable/Disable transmission of management address
port-description	Enable/Disable transmission of port description
system-capabilities	Enable/Disable transmission of system capabilities
system-description	Enable/Disable transmission of system description
system-name	Enable/Disable transmission of system name.

lldp transmission-delay

Description

Sets *LLDP* transmision-delay. LLDP transmission delay (the amount of time that the transmission of LLDP frames will delayed after LLDP configuration has changed) in seconds.)

Syntax

```
lldp transmission-delay 1-8192
```

Parameters

Name	Description
1-8192	transmission-delay seconds

lldp transmit

Description

Enable/Disabled transmission of *LLDP* frames.

Syntax

```
lldp transmit
```

Parameters

None.

RFC2544 Testing Configure Commands

rfc2544 profile <word32>

Description

RFC2544 profile configuration

Syntax

```
rfc2544 profile word32
```

Parameters

Name	Description
word32	Profile name up to 32 characters long

rfc2544 rename profile

Description

Rename an existing profile

Syntax

```
rfc2544 rename profile word32 word32
```

Parameters

Name	Description
profile <word32>	Old profile name
word32	New profile name

rfc2544 save <word32> <word>

Description

Save a report to a file on a TFTP server

Syntax

`rfc2544 save word32 word`

Parameters

Name	Description
<word32>	Name of existing report to save
<word>	TFTP server URL on the form tftp://server[:port]/path-to-file

rfc2544 start <word32> profile <word32> [desc <line128>]

Description

Start execution of a pre-configured profile

Syntax

`rfc2544 start word32 profile word32 [desc line128]`

Parameters

Name	Description
start *word32*	Unique name of resulting report
profile *word32*	Name of existing profile to execute
line128	Description that will appear in the report

rfc2544 stop <word32>

Description

Stop execution of an ongoing test

Syntax

`rfc2544 stop word32`

Parameters

Name	Description
word32	Report name to stop execution of

show rfc2544 profile [<word32>]

Description

show rfc2544 profile name

Syntax

```
show rfc2544 profile [word32]
```

Parameters

Name	Description
word32	rfc2544 profile name

GVRP Configure Commands

gvrp

Description

Enable GVRP on port(s)

Syntax

```
gvrp
```

Parameters

None.

gvrpjoin request vlan

Description

Emit a Join-Request for test purpose

Syntax

```
gvrp join-request vlan vlan_list
```

Parameters

Name	Description
vlan_list	List of VLANs

gvrpleave request vlan

Description

Emit a leave-Request for test purpose

Syntax

```
gvrp leave-request vlan vlan_list
```

Parameters

Name	Description
vlan_list	List of VLANs

gvrp max-vlans

Description

GVRP maximum number of VLANs

Syntax

```
gvrp max-vlans 1-4095
```

Parameters

Name	Description
<1-4095>	A valid range is from 1-4095.

gvrp time { [join-time <1-20>] [leave-time <60-300>] [leave-all-time <1000-50>]

Description

Set GVRP time

Syntax

```
gvrp time {[join-time 1-20] [leave-time 60-300] [leave-all-time
   1000-5000]}
```

Parameters

Name	Description
1-20	join timer, range is 1 - 20
60-300	leave timer, range is 60 - 300
1000-5000	leave all timer, range is 1000 - 5000

Voice VLAN Configure Commands

voice vlan

Description

Vlan for Voice appliance attributes

Syntax

```
voice vlan
```

Parameters

None.

voice vlan aging-time

Description

Set secure learning aging time for voice traffic

Syntax

`voice vlan aging-time` *`10-10000000`*

Parameters

Name	Description
`10-10000000`	Aging time, 10-10000000 seconds

voice vlan class

Description

Set voice traffic class

Syntax

`voice vlan class {`*`0-7`* `|` **`low`** `|` **`normal`** `|` **`medium`** `|` **`high`**`}`

Parameters

Name	Description
`0-7`	Traffic class value
`low`	Traffic class low (0)
`normal`	Traffic class normal (1)
`medium`	Traffic class medium (2)
`high`	Traffic class high (3)

voice vlan oui

Description

Set voice traffic OUI configuration

Syntax

`voice vlan oui` *`oui`* `[`**`description`** *`line32`*`]`

Parameters

Name	Description
oui	OUI value
description	Set description for the OUI
line32	Description line

voice vlan vid

Description

Set voice *VLAN* ID

Syntax

```
voice vlan vid vlan_id
```

Parameters

Name	Description
vlan_id	VLAN ID, 1 - 4095

Profile Alarm Commands

profile alarm

Description

Profile alarm

Syntax

```
profile alarm
```

Parameters

None.

alarm

Description

Set alarm content

Syntax

```
alarm alarmId {mask | unmask | major | minor}
```

Parameters

101–114: GE-1–14 Port link down (for 14 port model)

Name	Description
alarmId	151: set Power alarm
mask	Set alarm as mask, it means event will not be send notify
unmask	Set alarm as un-mask, it means event will be send notify
major	Set alarm level as major
minor	Set alarm level as minor

PoE Commands

poe management mode

Description

Use management mode to configure *PoE* power management method.

Syntax

```
poe management mode mode
```

Parameters

Name	Description
allocation-consumption	Max. port power determined by allocated, and power is managed according to power consumption.
allocation-reserved-power	Max. port power determined by allocated, and power is managed according to reserved power.
class-consumption	Max. port power determined by class, and power is managed according to power consumption.
class-reserved-power	Max. port power determined by class, and power is managed according to reserved power.
lldp-consumption	Max. port power determined by *LLDP* Media protocol, and power is managed according to power consumption.
lldp-reserved-power	Max. port power determined by LLDP Media protocol, and power is managed according to reserved power.

Parameters

poe supply

Description

Use *PoE* supply to specify the maximum power the power supply can deliver.

Syntax

```
poe supply power
```

Parameters

Name	Description
power	Maximum power the power supply can deliver. Valid values are: 1 – 240.

poe mode

Description

Set *PoE* mode.

Syntax

```
poe mode mode
```

Parameters

Name	Description
disable	Set PoE to disable
enable	Set PoE to enable always
schedule	Set PoE to enable by scheduling

poe operation

Description

Set *PoE* operation mode.

Syntax

```
poe operation af/at
```

Parameters

Name	Description
af	Set operation mode to 802.3af(Maximum power 15.4W)
at	Set operation mode to 802.3at(Maximum power 30.0 W)

poe power

Description

Set maximum power for port in allocation mode.

Syntax

```
poe power limit power
```

Parameters

Name	Description
power	Maximum power for the interface (0-15.4 Watt for *PoE* standard mode, 0-30.0 Watt for PoE plus mode)

poe priority

Description

Set *PoE* port priority

Syntax

```
poe priority [critical | high | low]
```

Parameters

None.

poe reset

Description

Set *PoE* power reset time.

Syntax

```
poe reset hour minute range_list
```

Parameters

Name	Description
hour	0-23
minute	0-59
range_list	Day(s): • 1: Sunday • 2: Monday • 3: Tuesday • 4: Wednesday • 5: Thursday • 6: Friday • 7: Saturday

poe schedule

Description

Set *PoE* power scheduling during the week.

Syntax

```
poe schedule day range_list
```

Parameters

Name	Description
day	fri mon sat sun thu tue wed
range_list	There are 48 time interval one day. Each interval has 30 minutes. • [1]<00:00-00:29> • [2]<00:30-00:59> • [3]<01:00-01:29> • ... • [47]<23:00-23:29> • [48]<23:30-23:59>

Configuring ERPS from the CLI

Although RingV2 cannot be used concurrently with Ethernet Ring Protection Switching (ERPS), you might need to configure ERPS if your ISW ring will interact with rings on other platforms. ExtremeXOS (EXOS) switches can run with ERPS, for example, and so can some switches from other manufacturers.

When configuring a RingV2 ISW switch to interact with an EXOS switch running ERPS, keep the following principles in mind:

- The key to connecting RingV2 rings with ERPS rings is ensuring that configuration parameters align in both systems.
- ISW default values for some timings (associated with recovery of the ring) do not match EXOS defaults.
- Some ISW variables have a different accepted variable length than the equivalent variables in EXOS.
- Carefully test your configuration, using logs and other troubleshooting tools to understand ways in which the settings interact with each other.

The following examples provide guidance for configuring ERPS.

Initial Switch Configuration

The following commands disable *STP* and *LLDP*. They also enable C-Port on Port 1 and 2 on all switches.

```
#configure port 1-2
interface GigabitEthernet 1/1-2
#set C-Port
switchport hybrid port-type c-port
switchport mode hybrid
#disable LLDP
no lldp receive
no lldp transmit
#disable Spanning Tree Protocol
no spanning-tree

#disable Loop Protection
no loop-protect
```

Configuring MEP and ERPS on Switch 1 (RPL Owner)

```
#create mep 1 on port 1
mep 1 down domain port level 0 interface GigabitEthernet 1/1
#set vlan for MEP traffic
mep 1 vid 3001
#set id of peer mep
mep 1 peer-mep-id 5
#enable ccm; frames are to use priority 7, at a rate of 10pps
mep 1 cc 7 fr10s
#enable RAPS; frames are to use priority 7
mep 1 aps 7 raps
mep 2 down domain port level 0 interface GigabitEthernet 1/2
mep 2 mep-id 2
mep 2 vid 3001
mep 2 peer-mep-id 3
mep 2 cc 7 fr10s
mep 2 aps 7 raps
#create erps on port 1 and port 2
erps 1 major port0 interface GigabitEthernet 1/1 port1 interface GigabitEthernet 1/2
#set MEP ID for the corresponding port
erps 1 mep port0 sf 1 aps 1 port1 sf 2 aps 2
#set the RPL owner
erps 1 rpl owner port1
#configure protected VLAN
erps 1 vlan 1
```

Configuring MEP and ERPS on Switch 2 (RPL Neighbor)

```
mep 3 down domain port level 0 interface GigabitEthernet 1/1
mep 3 mep-id 3
mep 3 vid 3001
mep 3 peer-mep-id 2
mep 3 cc 7 fr10s
mep 3 aps 7 raps
mep 4 down domain port level 0 interface GigabitEthernet 1/2
mep 4 mep-id 4
mep 4 vid 3001
mep 4 peer-mep-id 6
mep 4 cc 7 fr10s
mep 4 aps 7 raps
erps 1 major port0 interface GigabitEthernet 1/1 port1 interface GigabitEthernet 1/2
erps 1 mep port0 sf 3 aps 3 port1 sf 4 aps 4
#set the RPL neighbor
erps 1 rpl neighbor port0
erps 1 vlan 1
```

Configuring MEP and ERPS on Switch 3

```
mep os-tlv oui 0xC sub-type 0x1 value 0x2
mep 5 down domain port level 0 interface GigabitEthernet 1/1\
mep 5 mep-id 5
mep 5 vid 3001
mep 5 peer-mep-id 1 mac D8-84-66-56-FB-E4
mep 5 cc 7 fr10s
mep 5 aps 7 raps
mep 6 down domain port level 0 interface GigabitEthernet 1/2
mep 6 mep-id 6
mep 6 vid 3001
mep 6 peer-mep-id 4 mac D8-84-66-56-FE-2E
mep 6 cc 7 fr10s
```

```
mep 6 aps 7 raps
erps 1 major port0 interface GigabitEthernet 1/1 port1 interface GigabitEthernet 1/2
erps 1 mep port0 sf 5 aps 5 port1 sf 6 aps 6
erps 1 vlan 1
```

You can check the *ERPS (Ethernet Ring Protection Switching)* status with the `show erps` command. Below is the output from Switch 1 as configured in this example:

```
Sw1# show erps
(L=Link Up/Down; B=Blocked/Unblocked)      Maj RPL  RPL   RPL  FSM   R-APS
Gr Typ V Rev Port 0     L B Port 1     L B Grp Role Port  Blck State TX RX FOP
--+---+-+---+----------+-+-+----------+-+-+---+----+-----+----+-----+--+--+---
 1 Maj 2 Rev Gi 1/1     U U Gi 1/2     U B -   Ownr Port1 Y    IDLE  Y     N
```

Regulatory and Compliance Information

Federal Communications Commission (FCC) Notice

This device complies with Part 15 of the FCC rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Note

This equipment has been tested and found to comply with the limits for a class A digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment uses, generates, and can radiate radio frequency energy and if not installed in accordance with the operator's manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause interference in which case the user will be required to correct the interference at his own expense.

Warning

Changes or modifications made to this device which are not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Industry Canada NoticeCAN ICES-3 (A)/NMB-3(A)

This digital apparatus does not exceed the class A limits for radio noise emissions from digital apparatus set out in the Radio Interference Regulations of the Canadian Department of Communications.

Le present appareil numerique n'emet pas de bruits radioelectriques depassant les limites applicables aux appareils numeriques de la class A prescrites dans le Reglement sur le brouillage radioelectrique edicte par le ministere des Communications du Canada.

Product Safety

This product complies with the following international safety standards:

- UL 60950-1 2nd edition, A2:2014
- CAN/CSA-C22.2 No.60950-1-07 2nd Ed. 2014-10
- IEC 60950-1:2005 2nd+A1:2009+A2:2013
- EN 60950-1:2006+A11+A1+A12+A2
- 2014/35/EU (2006/95/EC will invalid by 20 April 2016)

Electromagnetic Compatibility (EMC)

This product complies with the following:

FCC 47 CFR Part 15 Subpart B Class A (US), ICES-003 (Canada)
EN 55022 (ITE Emissions), EN 55024 (ITE Immunity)
2014/30/EU (EMC Directive), EN 50121-1: 2017, EN 50121-4: 2016, EN 55011(ISM)
EN 61000-6-2 (Ind. Immunity), EN61000-6-4 Ind. Emissions)
EN 61000-3-2: 2014, EN 61000-3-3: 2013
RCM (Australia), MSIP KCC (Korea), BSMI (Taiwan)

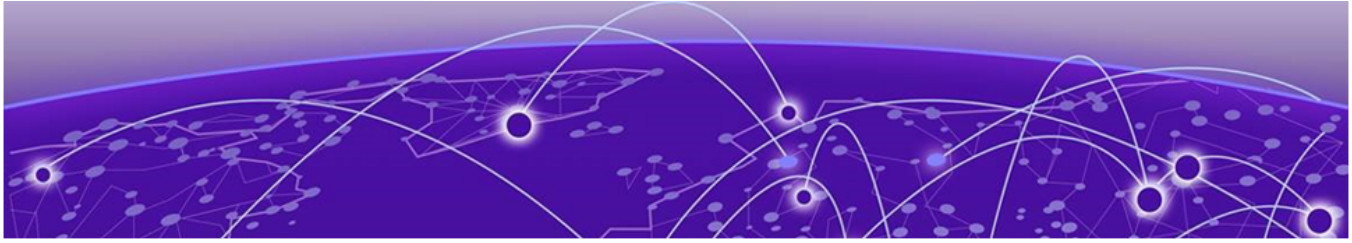
Korea EMC Statement (KCC)

이 기기는 업무용(A급) 전자파적합기기로서 판매자
또는 사용자는 이 점을 주의 하시기 바라며, 가정
외의 지역에서 사용하는 것을 목적으로 합니다.

BSMI EMC Statement - Taiwan

This is a Class A product. In a domestic environemnt this product may cause radio interference in which case the user may be required to take adequate measurers.

警告使用者：
此為甲類資訊技術設備，於居住環境中使用時，可能會造成射頻擾動，在此種情況下，使用者會被要求採取某些適當的對策。



Glossary

ACL

An Access Control List is a mechanism for filtering packets at the hardware level. Packets can be classified by characteristics such as the source or destination MAC, IP address, IP type, or QoS queue. Once classified, the packets can be forwarded, counted, queued, or dropped.

ad hoc mode

An 802.11 networking framework in which devices or stations communicate directly with each other, without the use of an AP.

ARP

Address Resolution Protocol is part of the TCP/IP suite used to dynamically associate a device's physical address (MAC address) with its logical address (IP address). The system broadcasts an ARP request, containing the IP address, and the device with that IP address sends back its MAC address so that traffic can be transmitted.

ATM

Asynchronous Transmission Mode is a start/stop transmission in which each character is preceded by a start signal and followed by one or more stop signals. A variable time interval can exist between characters. ATM is the preferred technology for the transfer of images.

BSS

Basic Service Set is a wireless topology consisting of one access point connected to a wired network and a set of wireless devices. Also called an infrastructure network. See also *IBSS (Independent Basic Service Set)*.

Chalet

Chalet is a web-based user interface for setting up and viewing information about a switch, removing the need to enter common commands individually in the CLI.

CHAP

Challenge-Handshake Authentication Protocol is one of the two main authentication protocols used to verify a user's name and password for PPP Internet connections. CHAP is more secure because it performs a three-way handshake during the initial link establishment between the home and remote machines. It can also repeat the authentication anytime after the link has been established.

CLI

Command Line Interface. The CLI provides an environment to issue commands to monitor and manage switches and wireless appliances.

CoS

Class of Service specifies the service level for the classified traffic type.

Data Center Connect

DCC, formerly known as DCM (Data Center Manager), is a data center fabric management and automation tool that improves the efficiency of managing a large virtual and physical network. DCC provides an integrated view of the server, storage, and networking operations, removing the need to use multiple tools and management systems. DCC automates VM assignment, allocates appropriate network resources, and applies individual policies to various data objects in the switching fabric (reducing VM sprawl). Learn more about DCC at http://www.extremenetworks.com/product/data-center-connect/.

DoS attack

Denial of Service attacks occur when a critical network or computing resource is overwhelmed so that legitimate requests for service cannot succeed. In its simplest form, a DoS attack is indistinguishable from normal heavy traffic. ExtremeXOS software has configurable parameters that allow you to defeat DoS attacks.

DSSS

Direct-Sequence Spread Spectrum is a transmission technology used in Local Area Wireless Network (LAWN) transmissions where a data signal at the sending station is combined with a higher data rate bit sequence, or chipping code, that divides the user data according to a spreading ratio. The chipping code is a redundant bit pattern for each bit that is transmitted, which increases the signal's resistance to interference. If one or more bits in the pattern are damaged during transmission, the original data can be recovered due to the redundancy of the transmission. (Compare with *FHSS (Frequency-Hopping Spread Spectrum)*.)

EAP-TLS/EAP-TTLS

EAP-TLS Extensible Authentication Protocol - Transport Layer Security. A general protocol for authentication that also supports multiple authentication methods, such as token cards, Kerberos, one-time passwords, certificates, public key authentication and smart cards.

IEEE 802.1x specifies how EAP should be encapsulated in LAN frames.
In wireless communications using EAP, a user requests connection to a WLAN through an access point, which then requests the identity of the user and transmits that identity to an authentication server such as RADIUS The server asks the access point for proof of identity, which the access point gets from the user and then sends back to the server to complete the authentication.

EAP-TLS provides for certificate-based and mutual authentication of the client and the network. It relies on client-side and server-side certificates to perform authentication and can be used to dynamically generate user-based and session-based WEP keys.

EAP-TTLS (Tunneled Transport Layer Security) is an extension of EAP-TLS to provide certificate-based, mutual authentication of the client and network through an encrypted tunnel, as well as to generate dynamic, per-user, per-session WEP keys. Unlike EAP-TLS, EAP-TTLS requires only server-side certificates.
(See also *PEAP (Protected Extensible Authentication Protocol)*.)

ERPS

Ethernet Ring Protection Switching provides fast protection and recovery switching for Ethernet traffic in a ring topology. It also ensures that the Ethernet layer remains loop-free. It is defined in ITU/T G.8032.

ESRP

Extreme Standby Router Protocol is an Extreme Networks-proprietary protocol that provides redundant Layer 2 and routing services to users.

Extreme Access Control

EAC, formerly NAC™, featuring both physical and virtual appliances, is a pre- and post-connect solution for wired and wireless LAN and VPN users. Using Identity and Access appliances and/or Identity and Access Virtual Appliance with the *Extreme Management Center* software, you can ensure only the right users have access to the right information from the right place at the right time. EAC is tightly integrated with the Intrusion Prevention System (IPS) and Security Information and Event Manager (SIEM) to deliver best-in-class post-connect access control. Learn more about EAC at http://www.extremenetworks.com/product/extreme-access-control/.

Extreme Application Analytics

EAA, formerly Purview™, is a network powered application analytics and optimization solution that captures and analyzes context-based application traffic to deliver meaningful intelligence about applications, users, locations, and devices. EAA provides data to show how applications are being used. This can be used to better understand customer behavior on the network, identify the level of user engagement, and assure business application delivery to optimize the user experience. The software also provides visibility into network and application performance allowing IT to pinpoint and resolve performance issues in the infrastructure whether they are caused by the network, application, or server. Learn more about EAA at http://www.extremenetworks.com/product/extremeanalytics/.

Extreme Management Center

Extreme Management Center (Management Center), formerly Netsight™, is a web-based control interface that provides centralized visibility into your network. Management Center reaches beyond ports, VLANs, and SSIDs and provides detailed control of individual users, applications, and protocols. When coupled with wireless and Identity & Access Management products, Management Center becomes the central location for monitoring and managing all the components in the infrastructure. Learn more about Management Center at http://www.extremenetworks.com/product/management-center/.

ExtremeCloud

ExtremeCloud is a cloud-based network management Software as a Service (SaaS) tool. ExtremeCloud allows you to manage users, wired and wireless devices, and applications on corporate and guest networks. You can control the user experience with smarter edges – including managing QoS, call admission control, secure access policies, rate limiting, multicast, filtering, and traffic forwarding, all from an intuitive web interface. Learn more about ExtremeCloud at http://www.extremenetworks.com/product/extremecloud/.

ExtremeSwitching

ExtremeSwitching is the family of products comprising different switch types: Modular (X8 and 8000 series [formerly BlackDiamond] and S and K series switches); Stackable (X-series and A, B, C, and 7100 series switches); Standalone (SSA, X430, and D, 200, 800, and ISW series); and Mobile Backhaul (E4G). Learn more about ExtremeSwitching at http://www.extremenetworks.com/products/switching-routing/.

ExtremeWireless

ExtremeWireless products and solutions offer high-density WiFi access, connecting your organization with employees, partners, and customers everywhere they go. The family of wireless products and

solutions includes APs, wireless appliances, and software. Learn more about ExtremeWireless at http://www.extremenetworks.com/products/wireless/.

ExtremeXOS

ExtremeXOS, a modular switch operating system, is designed from the ground up to meet the needs of large cloud and private data centers, service providers, converged enterprise edge networks, and everything in between. Based on a resilient architecture and protocols, ExtremeXOS supports network virtualization and standards-based SDN capabilities like VXLAN gateway, OpenFlow, and OpenStack Cloud orchestration. ExtremeXOS also supports comprehensive role-based policy. Learn more about ExtremeXOS at http://www.extremenetworks.com/product/extremexos-network-operating-system/.

FHSS

Frequency-Hopping Spread Spectrum is a transmission technology used in Local Area Wireless Network (LAWN) transmissions where the data signal is modulated with a narrowband carrier signal that 'hops' in a random but predictable sequence from frequency to frequency as a function of time over a wide band of frequencies. This technique reduces interference. If synchronized properly, a single logical channel is maintained. (Compare with *DSSS (Direct-Sequence Spread Spectrum)*.)

IBSS

An IBSS is the 802.11 term for an ad hoc network. See *ad hoc mode*.

ICMP

Internet Control Message Protocol is the part of the TCP/IP protocol that allows generation of error messages, test packets, and operating messages. For example, the ping command allows you to send ICMP echo messages to a remote IP device to test for connectivity. ICMP also supports traceroute, which identifies intermediate hops between a given source and destination.

IGMP

Hosts use Internet Group Management Protocol to inform local routers of their membership in multicast groups. Multicasting allows one computer on the Internet to send content to multiple other computers that have identified themselves as interested in receiving the originating computer's content. When all hosts leave a group, the router no longer forwards packets that arrive for the multicast group.

LLDP

Link Layer Discovery Protocol conforms to IEEE 802.1ab and is a neighbor discovery protocol. Each LLDP-enabled device transmits information to its neighbors, including chassis and port identification, system name and description, VLAN names, and other selected networking information. The protocol also specifies timing intervals in order to ensure current information is being transmitted and received.

MD5

Message-Digest algorithm is a hash function that is commonly used to generate 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.

MIC

Message Integrity Check (or Code), also called 'Michael', is part of WPA and TKIP. The MIC is an additional 8-byte code inserted before the standard 4-byte ICV appended in by standard WEP to the 802.11 message. This greatly increases the difficulty in carrying out forgery attacks.
Both integrity check mechanisms are calculated by the receiver and compared against the values sent

by the sender in the frame. If the values match, there is assurance that the message has not been tampered with.

MSTP

Multiple Spanning Tree Protocol, based on IEEE 802.1Q-2003 (formerly known as IEEE 892.1s), allows you to bundle multiple VLANs into one STP topology, which also provides enhanced loop protection and better scaling. MSTP uses RSTP as the converging algorithm and is compatible with legacy STP protocols.

netmask

A netmask is a string of 0s and 1s that mask, or screen out, the network part of an IP address, so that only the host computer part of the address remains. A frequently-used netmask is 255.255.255.0, used for a Class C subnet (one with up to 255 host computers). The ".0" in the netmask allows the specific host computer address to be visible.

PEAP

Protected Extensible Authentication Protocol is an IETF draft standard to authenticate wireless LAN clients without requiring them to have certificates. In PEAP authentication, first the user authenticates the authentication server, then the authentication server authenticates the user. If the first phase is successful, the user is then authenticated over the SSL tunnel created in phase one using EAP-Generic Token Card (EAP-GTC) or Microsoft Challenged Handshake Protocol Version 2 (MSCHAP V2). (See also *EAP-TLS/EAP-TTLS*.)

PoE

The Power over Ethernet standard (IEEE 802.3af) defines how power can be provided to network devices over existing Ethernet connections, eliminating the need for additional external power supplies.

QoS

Quality of Service is a technique that is used to manage network resources and 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.

RADIUS

RADIUS is a client/server protocol and software that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service. RADIUS allows a company to maintain user profiles in a central database that all remote servers can share. It provides better security, allowing a company to set up a policy that can be applied at a single administered network point. With RADIUS, you can track usage for billing and for keeping network statistics.

SNMP

Simple Network Management Protocol is a standard that uses a common software agent to remotely monitor and set network configuration and runtime parameters. SNMP operates in a multivendor environment, and the agent uses MIBs, which define what information is available from any manageable network device. You can also set traps using SNMP, which send notifications of network events to the system log.

SNTP

Simple Network Time Protocol is used to synchronize the system clocks throughout the network. An extension of NTP, SNTP can usually operate with a single server and allows for IPv6 addressing.

SSL

Secure Socket Layer is a protocol for transmitting private documents using the Internet. SSL works by using a public key to encrypt data that is transferred over the SSL connection. SSL uses the public-and-private key encryption system, which includes the use of a digital certificate. SSL is used for other applications than SSH, for example, OpenFlow.

STP

Spanning Tree Protocol, defined in IEEE 802.1d, used to eliminate redundant data paths and to increase network efficiency. STP allows a network to have a topology that contains physical loops; it operates in bridges and switches. STP opens certain paths to create a tree topology, thereby preventing packets from looping endlessly on the network. To establish path redundancy, STP creates a tree that spans all of the switches in an extended network, forcing redundant paths into a standby, or blocked, state.

STP allows only one active path at a time between any two network devices (this prevents the loops) but establishes the redundant links as a backup if the initial link should fail. If STP costs change, or if one network segment in the STP becomes unreachable, the spanning tree algorithm reconfigures the STP topology and re-establishes the link by activating the standby path.

syslog

A protocol used for the transmission of event notification messages across networks, originally developed on the University of California Berkeley Software Distribution (BSD) TCP/IP system implementations, and now embedded in many other operating systems and networked devices. A device generates a messages, a relay receives and forwards the messages, and a collector (a syslog server) receives the messages without relaying them.
syslog uses the UDP as its underlying transport layer mechanism. The UDP port that has been assigned to syslog is 514. (RFC 3164)

VLAN

The term VLAN is used to refer to a collection of devices that communicate as if they are on the same physical LAN. Any set of ports (including all ports on the switch) is considered a VLAN. LAN segments are not restricted by the hardware that physically connects them. The segments are defined by flexible user groups you create with the CLI.