EtherWAN

EX26262F PoE Managed Switch

User's Guide – Command Line Interface (CLI)

AUDIENCE

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

CONVENTIONS

The following conventions are used throughout this guide to show information:

NOTE: Emphasizes important information or calls your attention to related features or instructions.

WARNING: Alerts you to a potential hazard that could cause personal injury.

CAUTION: Alerts you to a potential hazard that could cause loss of data, or damage the system or equipment.

Revision History

Release	Date	Revision
Initial Release	**2017/05/22**	**A1**

CONTENTS

INTRODUCTION ..... - 5 -
CLI Management ..... - 6 -
AAA Commands ..... - 7 -
Access Management Commands ..... - 9 -
ACL Commands ..... - 10 -
Aggregation Commands ..... - 16 -
ARP-inspection Commands ..... - 18 -
Banner Commands ..... - 20 -
Clock Commands ..... - 21 -
Copy Commands ..... - 22 -
DHCP Commands ..... - 23 -
Diagnostic Commands ..... - 24 -
DNS Proxy ..... - 25 -
dot1x Commands ..... - 26 -
Enable / Disable ..... - 28 -
Event Notifications ..... - 29 -
Hostname ..... - 30 -
Green Ethernet ..... - 30 -
Mac Address Table ..... - 31 -
Firmware Commands ..... - 33 -
GVRP Commands ..... - 35 -
HTTP Commands ..... - 37 -
IGMP Commands ..... - 38 -
Interface Configuration Commands ..... - 42 -
IPMC Commands ..... - 44 -
IP Name Server ..... - 44 -
IP Route and Routing ..... - 45 -
IP Source Binding / Verify Source ..... - 45 -
IPv6 Commands ..... - 46 -
LACP Commands ..... - 47 -
LLDP Commands ..... - 48 -
Logging Commands ..... - 51 -
Loop Protect ..... - 51 -
Port Mirroring and Monitoring ..... - 52 -
MLD Commands ..... - 53 -
MVR Commands ..... - 54 -
Network Time Protocol ..... - 55 -
Power Over Ethernet ..... - 56 -
Port security Commands ..... - 58 -
Privilege level Commands ..... - 58 -
QoS Commands ..... - 59 -
Reload ..... - 64 -
RMON ..... - 64 -
SFlow Commands ..... - 66 -
SMTP Commands ..... - 68 -
SNMP Commands ..... - 68 -

SSH Commands ..... - 71 -
STP Commands..... - 72 -
Terminal Commands ..... - 76 -
UPnP Commands..... - 76 -
Username Commands..... - 77 -
VLAN Commands..... - 78 -
Voice VLAN Commands..... - 80 -
Web Commands..... - 81 -

INTRODUCTION

EtherWAN's EX26262F provides a 26-port switching platform with support for IEEE802.3at Power over Ethernet, high performance switching, and the advanced management features required for enterprise environments.

Equipped with 24 10/100/1000BASE-TX PoE ports, in combination with 2 100/1000 SFP Combo options, the EX26262F is feature-rich, with 9216 Bytes Jumbo Frame support, full wire speed Gigabit throughput, and QoS support.

The PoE ports provide up to 30 Watts per port, with a total power budget of 370 Watts, allowing the switch to operate a wide variety of Powered Devices with different bandwidth and power consumption requirements, such as IP cameras.

Robust management features include port security, IGMP snooping, VLANs, GARP protocols, and LACP, as well as SNMP & RMON interfaces. An intuitive GUI for web management simplifies switch configuration, status monitoring, and maintenance activities.

The EX26262F provides the following features:

- Supports IPv4/IPv6 dual stack management
- Supports SSH/SSL secured management
- Supports SNMP v1/v2c/v3
- Supports RMON groups 1,2,3,9
- Supports IGMP v1/v2/v3 Snooping
- Supports MLD v1/v2 Snooping
- Supports RADIUS and TACACS+ authentication
- Supports IP Source Guard
- Supports DHCP Relay (Option 82)
- Supports DHCP Snooping
- Supports ACL and QCL for traffic filtering
- Supports 802.1d(STP), 802.1w(RSTP) and 802.1s(MSTP)
- Supports LACP and static link aggregation
- Supports Q-in-Q double tag VLAN
- Supports GVRP dynamic VLAN

CLI Management

Initial Configuration

Connect to the switch console by connecting the RJ45 to DB9 console cable to the RJ45 console port of the switch and to the serial port of the computer running a terminal emulation application (such as HyperTerminal or Putty).

Configuration settings of the terminal-emulation program: Baud rate: 115,200bps, Data bits: 8, Parity: none, Stop bit: 1, Flow control: none.

The default login name is "root," no password.

Baud rate	115200
Stop bits	1
Data bits	8
Parity	N
Flow control	none

You can also use telnet to connect to the management VLAN of the switch: 192.168.1.10. Login is the sameL "root," no password.

Command Modes

The CLI is divided into several modes. If a user has privilege to run a particular command, the command must be run in the correct mode. To see the commands of the mode, enter a "?" at the system prompt. All commands will be listed in the screen. The command modes are listed bellow:

MODE	PROMPT	FUNCTIONS
exec	EX26262F#	Display current configuration, diagnostics, maintenance
config	EX26262F (config)#	Configuration commands
Config-if	EX26262F (config-interface)#	Configure ports
Config-if-vlan	EX26262F (config-if-vlan)#	Configure static vlan
Config-line	EX26262F (config-line)#	Line Configuration
Config-impc-profile	EX26262F (config-impc-profile)#	IPMC Profile
Config-snmp-host	EX26262F (config-snmp-host)#	SNMP Server Host
Config-stp-aggr	EX26262F (config-stp-aggr)#	STP Aggregation
Config-dhcp-pool	EX26262F (config-dhcp-pool)#	DHCP Pool Configuration
Config-rfc2544-profile	EX26262F (config-rfc2544-profile)#	RFC2544 Profile

AAA Commands

AAA

This section shows you to use an AAA (Authentication, Authorization, Accounting) server to provide access control to your network. The AAA server can be a TACACS+ or RADIUS server to create and manage objects that contain settings for using AAA servers.

radius-server:

Configure the RADIUS accounting server parameter.

Mode: **Global config**

Syntax:

[no] radius-server attribute 32 <line1-255>

[no] radius-server attribute 4 <ipv4_ucast>

[no] radius-server attribute 95 <ipv6_ucast>

[no] radius-server deadtime <1-1440>

[no] radius-server host { <word1-255> | <ipv4_ucast> | <ipv6_ucast> } [auth-port <0-65535>] [acct-port <0-65535>] [timeout <1-1000>] [retransmit <1-1000>] [key <line1-63>]

[no] radius-server key <line1-63>

[no] radius-server retransmit <1-1000>

[no] radius-server timeout <1-1000>

Parameter:

deadtime	Time to stop using a RADIUS server that doesn't respond
host	Specify a RADIUS server
key	Set RADIUS encryption key
retransmit	Specify the number of retries to active server
timeout	Time to wait for a RADIUS server to reply
<Minutes : 1-1440>	Time in minutes
<Host4 : ipv4_ucast>	IPv4 address
<Host6 : ipv6_ucast>	IPv6 address
<HostName : word1-255>	Hostname
acct-port	UDP port for RADIUS accounting server
auth-port	UDP port for RADIUS authentication server
key	Server specific key (overrides default)
retransmit	Specify the number of retries to active server (overrides default)
timeout	Time to wait for this RADIUS server to reply (overrides default)
<AuthPort : 0-65535>	UDP port number
<Seconds : 1-1000>	Wait time in seconds

EXAMPLE:

```
Switch(config)# radius-server host device key 12
```

aaa:

Configure aaa Authentication.

Mode **Global config**

Syntax: **aaa** authentication login { console | telnet | ssh | http } { { local | radius | tacacs } [{ local | radius | tacacs } [{ local | radius | tacacs }]] }

Parameter:

authentication	Authentication
login	Login
console	Configure Console
http	Configure HTTP
ssh	Configure SSH
telnet	Configure Telnet
local	Use local database for authentication
radius	Use RADIUS for authentication
tacacs	Use TACACS+ for authentication

EXAMPLE:

```
Switch(config)# aaa suthentication login telnet radius
```

tacacs-server:

Configure TACACS+

Mode: **Global config**

Syntax:

[no] tacacs-server deadtime <minutes>

[no] acacs-server host <host_name> [port <port>] [timeout <seconds>] [key <key>]

[no] tacacs-server key <key>

[no] tacacs-server timeout <seconds>

Parameter:

deadtime	Time to stop using a nonresponding TACACS+ server
host	Specify a TACACS+ server
key	Set TACACS+ encryption key
timeout	Time to wait for a TACACS+ server to reply
<Minutes : 1-1440>	Time in minutes
<Key: line1-63>	Shared key
<Seconds : 1-1000>	Wait time in seconds

EXAMPLE:

```
EX26262F(config)# tacacs-server deadtime 300
EX26262F(config)# tacacs-server host 192.168.1.2
EX26262F(config)# tacacs-server key 33
EX26262F(config)# tacacs-server timeout 300
EX26262F(config)#
```

Access Management Commands

Access

This section shows you to configure access management table of the Switch including HTTP/HTTPS, SNMP, and TELNET/SSH. You can manage the Switch over an Ethernet LAN, or over the Internet..

access management:

Access management configuration.

Mode: **Global config**

Syntax: **[no] access management** <access_id>

access management <access_id> <access_vid> <start_addr> [to <end_addr>] { [web] [snmp] [telnet] | all }

Parameter: **access_id:** Numerical ID of entry <1-16>

access_vid: VLAN ID <1-4095>

start_addr: Starting IP address of range in IPv4 or IPV6 format

end_addr: Ending IP address of range in IPv4 or IPV6 format

<all> All services

<snmp> SNMP services

<telnet> telnet services

<web> Web services

EXAMPLE:

```
EX26262F(config)# access management 10 3 192.168.1.1 all
```

ACL Commands

ACL

The switch access control lists are used for packet filtering and for selecting types of traffic to be analyzed, forwarded, or influenced in some way. The ACLs are divided into EtherTypes. IPv4, ARP protocol, MAC and VLAN parameters etc. Here we will just go over the standard and extended access lists for TCP/IP. As you create ACEs for ingress classification, you can assign a policy for each port, the policy number is 1-8, however, each policy can be applied to any port. This makes it very easy to determine what type of ACL policy you will be working with.

access-list ace:

Create or modify Access Control Entry.

Mode: **Global config**

Syntax: **access-list ace** { update<1-256> | <1-256> } [action< deny | filter | permit >]

access-list ace { update<1-256> | <1-256> } [dmac-type < any | broadcast | multicast | unicast >]

access-list ace { update<1-256> | <1-256> } [frametype < any | arp | etype | ipv4 | ipv4-icmp | ipv4-tcp | ipv4-udp | ipv6 | ipv6-icmp | ipv6-tcp | ipv6-udp >]

access-list ace { update<1-256> | <1-256> } [ingress] [ingress interface { <port_type> <port_type_id> | <port_type> <port_type_list> } | any }]

access-list ace { update<1-256> | <1-256> } [logging [disable]]

access-list ace { update<1-256> | <1-256> } [lookup [disable]]

access-list ace { update<1-256> | <1-256> } [mirror [disable]]

access-list ace { update<1-256> | <1-256> } [next { <1-256> | last }]

access-list ace { update<1-256> | <1-256> } [policy <0-255> [policy-bitmask <0x0-0xFF>]]

access-list ace { update<1-256> | <1-256> } [rate-limiter { <1-16> | disable }]

access-list ace { update<1-256> | <1-256> } [redirect | interface { <port_type> <port_type_id> | <port_type> <port_type_list> } | disable }]

access-list ace { update<1-256> | <1-256> } [shutdown]

access-list ace { update<1-256> | <1-256> } [tag { tagged | untagged | any }]

access-list ace { update<1-256> | <1-256> } [tag-priority { <0-7> | any }]

access-list ace { update<1-256> | <1-256> }[vid { <1-4095> | any }]

Parameter:

action	Access list action
dmac-type	The type of destination MAC address
frametype	Frame type
ingress	Ingress
logging	Logging frame information
lookup	Second lookup
mirror	Mirror frame to destination mirror port
next	insert the current ACE before the next ACE ID
policy	Policy
rate-limiter	Rate limiter
redirect	Redirect frame to specific port
shutdown	Shutdown incoming port
tag	Tag
tag-priority	Tag priority
vid	VID field
deny	Deny
filter	Filter
permit	Permit
any	Don't-care the type of destination MAC address
broadcast	Broadcast destination MAC address
multicast	Multicast destination MAC address
unicast	Unicast destination MAC address
any	Don't-care the frame type
arp	Frame type of ARP
etype	Frame type of etype
ipv4	Frame type of IPv4
ipv4-icmp	Frame type of IPv4 ICMP
ipv4-tcp	Frame type of IPv4 TCP
ipv4-udp	Frame type of IPv4 TCP
ipv6	Frame type of IPv4
ipv6-icmp	Frame type of IPv6 ICMP
ipv6-tcp	Frame type of IPv6 TCP
ipv6-udp	Frame type of IPv6 UDP
interface	Select an interface to configure
<port_type>	Gigabitethernet
*****	All switches or All ports
Gigabitethernet	1 Gigabit Ethernet port
<port_type_id>	Port ID in the format of switch-no/port-no ex, 1/1-26 for Gigabitethernet

<port_type>	* or Gigabitethernet
*****	All Switches or All ports
Gigabitethernet	1 Gigabit Ethernet Port
<port_type_list>	Port list in 1/1-26
any	Don't-care the ingress interface
<0-255>	Policy ID
policy-bitmask	The bitmask for policy ID
<0x0-0xFF>	The value of policy bitmask
<1-4095>	The value of VID field
<0-7>	The value of tag priority

EXAMPLE:

```
EX26262F(config)# access-list ace 10 action deny
```

access-list rate-limiter:

Configure ACL rate limiting

Mode: **Global config**

Syntax: **access-list rate-limiter** [<1~16>] { pps <0-3276700> | 100kbps <0-10000> }
[default] **access-list rate-limiter** [<1~16>]

Parameter:

100kbps	100k bits per second
<RateLimiterList : 1~16>	Rate limiter ID
<PpsRate : 0-3276700>	Rate value
<0-10000>	Rate value

EXAMPLE:

```
EX26262F(config)# access-list rate-limiter 100kbps 111
```

access-list action:

Configure ACL port default action

Mode: **Interface Config**

Syntax: **access-list action** < permit | deny >

Parameter: **deny:** Deny forwarding

permit: Permit forwarding

access-list logging:

Enable access list logging. Note: The logging feature only works when the packet length is less than 1518 (without VLAN tags) and the System Log memory size and logging rate is limited.

Mode: **Interface Config**

Syntax: **access-list logging**

Parameter: **none**

access-list mirror:

Mirror frames to a destination mirror port.

Mode: **Interface Config**

Syntax: **[no] access-list mirror**

Parameter: **none**

access-list policy:

Configure the access-list policy value. The access-list interface configuration will affect the received frames if it doesn't match any ACE.

Mode: **Interface Config**

Syntax: **access-list policy** <0-255>

Parameter: **<1-256>** ACE ID must be exist

<0-256> If the next ACE ID is non-zero, the ACE will be Placed before this ACE in the list. If the next ACE ID is zero, the ACE will be placed last in the list.

EXAMPLE:

```
EX26262F(config-if)# access-list policy 10
```

access-list port-state:

Enable access-list port state.

Mode: **Interface Config**

Syntax: **access-list port-state**

Parameter: **none**

access-list rate-limiter:

Set the access control rule with rate limiter on switch.

Mode: **Interface config**

Syntax: **access-list rate-limiter** [<1~16>] { pps <1, 2, 4, 8, 16, 32, 64, 128, 256, 512> | 100pps <1-32767> | kpps <1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1024> | 100kbps <0-10000> }

Parameter: **<1-16>** Rate limiter ID

kbps Kbits per second

pps Packets per second

<0-10000> Rate in 100Kbps

EXAMPLE:

```
EX26262F(config-if)#  access-list rate-limiter 1 kbps 100
```

access-list redirect:

Redirect frame to specific port

Mode: **Interface config**

Syntax: **[no] access-list redirect** interface { <port_type_id> | <port_type_list> }

Parameter: **none**

access-list shutdown:

Shutdown incoming port. The shutdown feature only works when the packet length is less than 1518 (without VLAN tags).

Mode: **Interface config**

Syntax: **[no] access-list shutdown**

Parameter: **none**

show access-list:

Show all access control entry setting or information of the switch.

Mode: **Privilged exec**

Syntax: **show access-list** [interface [* | Gigabitetherne <PORT_LIST>]] [rate-limiter [<RateLimiterList : 1~16>]] [ace statistics [<AceId : 1~256>]]

show access-list ace-status [static] [loop-protect] [dhcp] [upnp] [arp-inspection] [mep] [ipmc] [ip-source-guard] [ip-mgmt] [conflicts]

Parameter:

interface	Select an interface to configure
*****	All Switches or All Ports
Gigbitethernet	1 Gigabit Ethernet Port
<port_type_list>	Port list in 1/1-26
rate-limiter	Rate limiter
< RateLimiterList : 1~16>	Rate limiter ID
ace	Access list entry
statistics	Traffic statistics
<AceId : 1~256>	ACE ID
ace-status	The local ACEs status
static	The ACEs that are configured by users manually
loop-protect	The ACEs that are configured by Loop Protect module
dhcp	The ACEs that are configured by DHCP module
upnp	The ACEs that are configured by UPnP module
arp-inspection	The ACEs that are configured by ARP Inspection module
mep	The ACEs that are configured by MEP module
ipmc	The ACEs that are configured by IPMC module
ip-source-guard	The ACEs that are configured by IP Source Guard module
ip-mgmt	The ACEs that are configured by IP Mamagement module
conflicts	The conflicts ACEs that does not applied to the hardware due to hardware limitations

EXAMPLE:

```
EX26262F# show access-list ace statistics rate-limiter

Switch access-list ace number: 0

Switch access-list rate limiter ID 1 is 1 pps
```

Aggregation Commands

Aggregation

The Aggregation is used to configure the settings of Link Aggregation. You can bundle more than one port with the same speed, full duplex and the same MAC to be a single logical port, thus the logical port aggregates the bandwidth of these ports. This means you can apply your current Ethernet equipment's to build the bandwidth aggregation. For example, if there are three Fast Ethernet ports aggregated in a logical port, then this logical port has bandwidth three times as high as a single Fast Ethernet port has.

aggregation mode:

Set traffic distribution mode.

Mode: **Global config**

Syntax: **aggregation mode** { [smac] [dmac] [ip] [port] }

no aggregation mode

Parameter:

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

EXAMPLE:

```
EX26262F(config)# aggregation mode ip port dmac smac
```

aggregation group:

Configure the link aggregation group.

Monde: **Interface config**

Syntax: **aggregation group** <uint>

no aggregation group

Parameter: **<uint>** The Aggregation group id <1-14>.

EXAMPLE:

```
EX26262F(config-if)# aggregation group 10
```

show aggregation:

Display aggregation configurations on the switch.

Mode **Privileged exec**

Syntax: **show** aggregation [mode] [| {begin | exclude | include } <LINE>]

Parameter:

mode	Traffic distribution mode
|	Output modifiers
begin	Begin with the line that matches
exclude	Exclude lines that match
include	Include lines that match
<LINE>	String to match output lines

EXAMPLE:

```
EX26262F# show aggregation  Mode
Aggregation Mode:

SMAC  : Enabled
DMAC  : Disabled
IP    : Enabled
Port  : Enabled
```

ARP-inspection Commands

Arp inspection

The section describes to configure the ARP Inspection parameters of the switch. You could use the ARP Inspection configure to manage the ARP table.

ip arp inspection:

Add ARP inspection static entry.

Mode: **Global config**

Syntax:

[no] ip arp inspection

ip arp inspection entry interface <port_type> <in_port_type_id> <vlan_var> <mac_var> <ipv4_var>

ip arp inspection translate [interface <port_type> <in_port_type_id> <vlan_var> <mac_var> <ipv4_var>]

ip arp inspection vlan <in_vlan_list>

ip arp inspection vlan <in_vlan_list> logging { deny | permit | all }

Parameter:

inspection	ARP inspection
entry	arp inspection entry
interface	arp inspection entry interface config
<port_type>	Port type in Fast, Giga ethernet
<port_type_id>	Port ID in the format of switch-no/port-no
<vlan_id>	Select a VLAN id to configure
<mac_ucast>	Select a MAC address to configure
<ipv4_ucast>	Select an IP Address to configure
deny	log denied entries
permit	log permitted entries
all	log all entries
translate	arp inspection translate all entries
vlan	arp inspection vlan setting
<vlan_list>	arp inspection vlan list

show ip arp:

Display the ARP inspection configuration information.

Mode: **Privilged exec**

Syntax: **show ip arp**

show ip arp inspection [interface {<port_type> <port_type_list>} | vlan <vlan_list>]

show ip arp inspection entry [dhcp-snooping | static] [interface <port_type> <port_type_list>]

Parameter:

inspection	ARP inspection
interface	arp inspection entry interface config
<port_type>	Gigabitethernet
<port_type_list>	Port list in 1/1-26 for Gigabitethernet

EXAMPLE:

```
EX26262F# show ip arp
169.254.0.1 via VLAN1:00-e0-b3-3f-18-65
192.168.1.11 via VLAN1:00-e0-b3-3f-18-65
192.168.1.199 via VLAN1:30-65-ec-91-98-20
192.168.1.254 (Incomplete)
```

Banner Commands

banner:

Define a login banner

Mode: **Global config**

Syntax:

banner [motd] <banner>

banner exec <banner>

banner login <banner>

Parameter:

<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

Clock Commands

clock:

Configure time and clock settings

Mode: **Global config**

Syntax:

clock set <icliDate> <icliTime>

clock summer-time <word16> date [<start_month_var> <start_date_var> <start_year_var> <start_hour_var> <end_month_var> <end_date_var> <end_year_var> <end_hour_var> [<offset_var>]]

clock summer-time <word16> recurring [<start_week_var> <start_day_var> <start_month_var> <start_hour_var> <end_week_var> <end_day_var> <end_month_var> <end_hour_var> [<offset_var>]]

clock timezone <word_var> <hour_var> [<minute_var>]

Parameter:

set	set clock
summer-time	Configure summer (daylight savings) time
timezone	Configure time zone
<date>	yyyy/mm/dd
<time>	hh:mm:ss
<2000-2097>	Year to start
hh:mm	Time to start (hh:mm)
<1-12>	Month to end
<1-31>	Date to end
<2000-2097>	Year to end
hh:mm	Time to end (hh:mm)
<1-1440>	Offset to add in minutes
<1-5>	Week number to start
<1-7>	Weekday to start
<1-12>	Month to start

Copy Commands

copy

Copy from source to destination.

Mode: **Privilged exec**

Syntax: **copy** { startup-config | running-config | < flash:filename | tftp://server/path-and-filename > } { startup-config | running-config | < flash:filename | tftp://server/path-and-filename > } [syntax-check][| { begin | exclude | include }{ <LINE >}]

Parameter:

flash:filename | tftp://server/path-and-filename	File in FLASH or on TFTP server
running-config	Currently running configuration
startup-config	Startup configuration
|	Output modifiers
syntax-check	Perform syntax check on source configuration
begin	Begin with the line that matches
exclude	Exclude lines that match
include	Include lines that match
<LINE>	String to match output lines

DHCP Commands

DHCP

Dynamic Host Configuration Protocol (DHCP) automatically provides an Internet Protocol (IP) host with its IP address and other configuration information such as the subnet mask and default gateway.

ip dhcp (privileged exec):

Restart the DHCP query process

Mode: **Privilged exec**

Syntax: **ip dhcp** retry interface vlan <vlan_id>

Parameter:

dhcp	Dhcp commands
retry	Restart the DHCP query process
interface	Interface
vlan	Vlan interface
<vlan_id>	Vlan ID

ip dhcp (global):

DHCP settings and configuration.

Mode: **Global config**

Syntax:

[no] ip dhcp excluded-address <low_ip> [<high_ip>]

[no] ip dhcp pool <pool_name>

[no] ip dhcp relay

[no] ip dhcp relay information option

[no] ip dhcp relay information policy { drop | keep | replace }

[no] ip dhcp server

[no] ip dhcp snooping

ip helper-address <v_ipv4_ucast>

Parameter:

drop Drop the package when receive a DHCP message that already contains relay information

keep Keep the original relay information when receive a DHCP message that already contains it

replace Replace the original relay information when receive a DHCP message that already contains it.

show ip dhcp:

Display DHCP information.

Mode: **Privilged exec**

Syntax:

show ip dhcp relay [statistics]

show ip dhcp snooping [statistics] [interface <port_type> <port_type_list>]

show ip dhcp detailed statistics { server | client | snooping | relay | normal-forward | combined } [interface <port_type_list>]

Parameter:

interface	arp inspection entry interface config
<port_type>	Gigabitethernet
<port_type_list>	Port list in 1/1-26 for Gigabitethernet

Diagnostic Commands

ping:

Send ICMP echo messages

Syntax:

ping ip <word1-255> [repeat <Count : 1-60>] [size <Size : 2-1452>] [interval <Seconds : 0-30>]

ping ipv6 <ipv6_addr> [repeat <Count : 1-60>] [size <Size : 2-1452>] [interval <Seconds : 0-30>] [interface vlan <vlan_id>]

Parameter:

ip	IP (ICMP) echo
<word1-255>	ICMP destination address
repeat	Specify repeat count
<Count : 1-60>	1-60; Default is 5
size	Specify datagram size
<Size : 2-1452>	2-1452; Default is 56 (excluding MAC, IP and ICMP headers)
interval	Specify repeat interval
<Seconds : 0-30>	0-30; Default is 0
ipv6	IPv6 (ICMPv6) echo
<ipv6_addr>	ICMPv6 destination address
repeat	Specify repeat count
<1-60>	1-60; Default is 5
size	Specify datagram size
<2-1452>	2-1452; Default is 56 (excluding MAC, IP and ICMP headers)
interval	Specify repeat interval
<0-30>	0-30; Default is 0
interface	Select an interface to configure
vlan	VLAN Interface
<vlan_id>	VLAN identifier(s): VID

veriphy:

Run cable diagnostics

Mode: **Privileged exec**

Syntax: **show interface <port_type_list> veriphy**

Parameter: **<port-list>** Port list, available value is from 1 to 10B format:1,3-5

***** All ports

EXAMPLE:

```
EX26262F# show interface * veriphy
Starting VeriPHY - Please wait
Interface             Pair A  Length  Pair B, Length  Pair C  Length  Pair D  Length
---------------------  ------  ------  --------------  ------  ------  ------
-------
GigabitEthernet 1/1    Open    0       Open    0       Open    0       Open    0
GigabitEthernet 1/2    Open    0       Open    0       Open    0       Open    0
GigabitEthernet 1/3    OK      0       OK      0       OK      0       OK      0
GigabitEthernet 1/4    Open    0       Open    0       Open    0       Open    0
```

DNS Proxy

ip dns proxy:

Set dns proxy service

Mode: **Global config**

Syntax: **ip dns proxy**

Parameter: **none**

dot1x Commands

dot1x (privileged exec):

IEEE Standard for port-based Network Access Control.

Syntax: **dot1x** initialize [interface (<port_type> [<plist>])]

Parameter:

initialize	Force re-authentication immediately
interface	Interface
*****	All switches or All ports
Gigabitethernet	1 GigabitEthernet port
<port_type_list>	Port list in 1/1-26 for Gigabitethernet

dot1x (global):

IEEE Standard for port-based Network Access Control.

Syntax:

[no] dot1x authentication timer inactivity <v_10_to_100000>

[no] dot1x authentication timer re-authenticate <v_1_to_3600>

[no] dot1x feature { [guest-vlan] [radius-qos] [radius-vlan] }*1

[no] dot1x guest-vlan <value>

[no] dot1x guest-vlan supplicante

[no] dot1x max-reauth-req <1-255>

[no] dot1x re-authentication

[no] dot1x system-auth-control

[no] dot1x timeout quiet-period <v_10_to_1000000>

[no] dot1x timeout tx-period <v_1_to_65535>

Parameter:

authentication	Authentication
feature	Globally enables/disables a dot1x feature functionality
guest-vlan	Guest VLAN
max-reauth-req	Guest VLAN ID used when entering the Guest VLAN.
re-authentication	Set Re-authentication state
system-auth-control	Set the global NAS state
timeout	timeout
timer	timer
inactivity	Time in seconds between check for activity on successfully authenticated MAC addresses.
re-authenticate	The period between re-authentication attempts in seconds
<10-1000000>	seconds

<1-3600> seconds

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.

<1-4095> The number of times a Request Identity EAPOL frame is sent without response before considering entering the Guest VLAN.

supplicant The switch remembers if an EAPOL frame has been received on the port for the life-time of the port. Once the switch considers whether to enter the Guest VLAN, it will first check if this option is enabled or disabled. If disabled (unchecked; default), the switch will only enter the Guest VLAN if an EAPOL frame has not been received on the port for the life-time of the port. If enabled (checked), the switch will consider entering the Guest VLAN even if an EAPOL frame has been received on the port for the life-time of the port.

<1-255> number of times

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

tx-period the time between EAPOL retransmissions.

<10-1000000> seconds

<1-65535> seconds

dot1x (interface):

IEEE Standard for port-based Network Access Control.

Syntax: **dot1x re-authenticate**

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

no dot1x port-control

dot1x guest-vlan

dot1x radius-qos

dot1x radius-vlan

Parameter: **none**

Enable / Disable

enable:

Modify password parameters

Mode: **Global config**

Syntax: **enable** password [<level> <1-15>] <WORD>

enable secret { 0 | 5 } [< level> <1-15>] <WORD>

Parameter:

password	Assign the privileged level clear password
secret	Assign the privileged level secret
WORD	The UNENCRYPTED (cleartext) password
level	Set exec level password
<1-15>	Level number
0	Specifies an UNENCRYPTED password will follow
5	Specifies an ENCRYPTED secret will follow

Example:

```
EX26262F(config)# enable password level 10 999
EX26262F(config)#
```

disable:

Turn off privileged commands

Mode: **Privilged exec**

Syntax: **disable** <0-15>

Parameter:

<0-15>	Privilege level

Event Notifications

event:

Set Trap event severity level.

Mode: **Global config**

Syntax: **event** group <group_name> { level <lvl> | syslog { enable | disable } | trap { enable | disable } | smtp { enable | disable } | ipush { enable | disable } }

Parameter:

Group Configure trap event severity level

<word32> ACL, ACL_Log, Access_Mgmt, Auth_Failed, Cold_Start, Config_Info, FAN_FAIL, Firmware_Upgrade, Import_Export, LACP, Link_Status, Login, Logout, Loop_Protect, Mgmt_IP_Change, Module_Change, NAS, Password_Change, Poe_Auto_Check, Port_Security, Temperature, VLAN, Voltage, Warm_Start

Example:

```
EX26262F(config)# event group VLAN trap enable
EX26262F(config)#
```

Hostname

hostname:

Set system's network name

Mode: **Global config**

Syntax: **hostname** < WORD >

Parameter: **none**

Green Ethernet

green-ethernet:

Set Green Ethernet (Power reduction)

Mode: **Global config**

Syntax: **green-ethernet** eee optimize-for-power

Parameter:

eee	Powering down of PHYs when there is no traffic.
optimize-for-power	Set if EEE shall be optimized for least power consumption (else optimized for least traffic latency).

Mac Address Table

aging-time:

Configure the aging-time of MAC address entries

Mode: **Global config**

Syntax: **[no] mac address-table** aging-time <0, 10-1000000>

[no] mac address-table static <mac_addr> vlan <vlan_id> interface <port_type> <port_type_list>

Parameter:

<0, 10-1000000>	Aging time in seconds, 0 disables aging
static	Static MAC address
<mac_addr>	48 bit MAC address: xx:xx:xx:xx:xx:xx
vlan	VLAN keyword
<vlan_id>	VLAN IDs 1-4095
interface	Select an interface to configure
<port_type>	Port type * or Gigabitethernet
*****	All switches or All ports
Gigabitethernet	1 Gigabit Ethernet port
<port_type_list>	Port list in 1/1-26 for Gigabitethernet

EXAMPLE:

```
EX26262F(config)# mac address-table aging-time 3333
```

show mac address-table:

Display the MAC Table or configuration information what set on the switch

Mode: **Privileged exec**

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>] [| {begin | exclude | include } <LINE>]

Parameter:

address-table	Mac Address Table
conf	User added static mac addresses

static	All static mac addresses
aging-time	Aging time
learning	Learn/disable/secure state
count	Total number of mac addresses
interface	Select an interface to configure
<port_type>	Gigabitethernet

mac address-table learning:

Enable learning on a port

Mode: **Intefrace config**

Syntax: **mac address-table learning** [secure]

Parameter:

secure	Port secure mode

Firmware Commands

firmware

This section describes how to upgrade Firmware. The Switch can be enhanced with more value-added functions by installing firmware upgrades.

show version:

Display the active and alternate firmware image version information

Mode: **Privileged exec**

Syntax: **show version**

Parameter: **none**

EXAMPLE:

```
EX26262F# show version

MEMORY          : Total=78337 KBytes, Free=53703 KBytes, Max=53536 KBytes
FLASH           : 0x40000000-0x41ffffff, 512 x 0x10000 blocks
MAC Address     : 00-e0-b3-3f-20-8e
Previous Restart : Cold

System Contact   :
System Name      : EX26262F
System Location  :
System Time      : 2011-01-02T07:01:13+00:00
System Uptime    : 1d 07:01:13

Active Image
------------
Image           : managed
Version         : EX26262F (standalone) v6.54.2173
Date            : 2016-08-29T15:32:24+08:00

Alternate Image
---------------
Image           : managed.bk
Version         :
Date            :
```

firmware swap:

Swap the active firmware image to alternate firmware image or reverse between them

Mode: **Privileged exec**

Syntax: **firmware swap**

Parameter: **none**

firmware upgrade:

Upgrade the system firmware to active or alternate division

Mode: **Privileged exec**

Syntax: **firmware upgrade** <ipv6-address> <word>

firmware upgrade <ip-hostname> <word>

Parameter: **<word>** Firmware image file name

NOTE: This page facilitates an update of the firmware controlling the switch. Uploading software will update all managed switches to the location of a software image and click. After the software image is uploaded, a page announces that the firmware update is initiated. After about a minute, the firmware is updated and all managed switches restart. the switch restarts.

WARNING: While the firmware is being updated, Web access appears to be defunct. The front LED flashes Green/Off with a frequency of 10 Hz while the firmware update is in progress. Do not restart or power off the device at this time or the switch may fail to function afterwards.

GVRP Commands

GVRP

GVRP is an application based on Generic Attribute Registration Protocol (GARP), mainly used to automatically and dynamically maintain group membership information of VLANs. GVRP provides VLAN registration service through a GARP application. It makes use of GARP Information Declaration (GID) to maintain the ports associated with their attribute database and GARP Information Propagation (GIP) to communicate among switches and end stations. With GID information and GIP, GVRP state machine maintain the contents of Dynamic VLAN Registration Entries for each VLAN and propagate these information to other GVRP-aware devices to setup and update their knowledge database, the set of VLANs associated with currently active members, and through which ports these members can be reached.

gvrp (global):

Enable or disable GVRP globally

Mode: **Global config**

Syntax: **gvrp**

Parameter: **none**

gvrp time:

Config GARP protocol timer parameters. IEEE 802.1D-2004, clause 12.11.

Mode: **Global config**

Syntax: **gvrp** time { [join-time <1-20>] [leave-time <60-300>] [leave-all-time <1000-5000>] }*1

Parameter: **time** config gvrp timer value in units of centi seconds [cs]

gvrp max-vlans:

Set the number of VLANs that GVRP can control

Mode: **Global config**

Syntax: **gvrp** max-vlans <1-4095>

Parameter: **none**

gvrp (interface):

Enable or disable GVRP on an interface

Mode:	**Interface config**
Syntax:	**gvrp**
Parameter:	**none**

gvrp join-request:

Send a Join-Request for test purposes.

Mode:	**Interface config**
Syntax:	**gvrp join-request** vlan <vlan_list>
Parameter:	**none**

gvrp leave-request:

Send a leave-Request for test purposes.

Mode:	**Interface config**
Syntax:	**gvrp leave-request** vlan <vlan_list>
Parameter:	**none**

HTTP Commands

show ip http:

display the secure HTTP web server status.

Mode:	**Privileged exec**
Syntax:	**show ip http** server secure status
Parameter:	**none**

ip http secure-server:

Enable secure HTTP web server

Mode:	**Global config**
Syntax:	**[no] ip http secure-server**
Parameter:	**none**

ip http secure-redirect:

Enable secure HTTP web redirection. When the secure HTTP web server is enabled, the feature automatically redirects non-secure HTTP web connections to secure connections.

Mode:	**Global config**
Syntax:	**[no] ip http secure-redirect**
Parameter:	**none**

IGMP Commands

ip igmp snooping:

Configure compatibility parameters on the switch

Mode: **Global config or Interface config**

Syntax: **[no] ip igmp snooping** [VLAN, vlan_id]

Parameter: **none**

ip igmp unknown-flooding:

Flooding unregistered IPv4 multicast traffic

Mode: **Global config**

Syntax: **ip igmp unknown-flooding**

Parameter: **none**

ip igmp host-proxy:

Configure IGMP proxy

Mode: **Global config**

Syntax: **ip igmp host-proxy** [leave-proxy]

Parameter: **none**

ip igmp ssm-range:

IPv4 address range of Source Specific Multicast

Mode: **Global config**

Syntax: **[no] ip igmp ssm-range** <ipv4_mcast> <4-32>

Parameter: **none**

ip igmp snooping querier:

Configure IGMP querier

Mode: **Config-if-vlan**

Syntax: **ip igmp snooping querier** { election | address <ipv4_ucast> }

no ip igmp snooping querier { election | address }

Parameter: **none**

ip igmp snooping compatibility:

Set IGMP compatibility

Mode: **Config-if-vlan**

Syntax: **ip igmp snooping compatibility** { auto | v1 | v2 | v3 }

no ip igmp snooping compatibility

Parameter: **none**

ip igmp snooping priority:

Set IGMP priority

Mode: **Config-if-vlan**

Syntax: **ip igmp snooping priority** <0-7>

no ip igmp snooping priority

Parameter: **none**

ip igmp snooping robustness-variable:

Set IGMP priority

Mode: **Config-if-vlan**

Syntax: **ip igmp snooping robustness-variable** <1-255>

no ip igmp snooping robustness-variable

Parameter: **none**

ip igmp snooping query-interval:

Set IGMP query interval

Mode: **Config-if-vlan**

Syntax: **ip igmp snooping query-interval** <1-31744>

no ip igmp snooping query-interval

Parameter: **<1-31744>** Interval in tenths of seconds

ip igmp snooping query-max-response-time:

Set maximum response time for IGMP query

Mode: **Config-if-vlan**

Syntax: **ip igmp snooping query-max-response-time** <0-31744>

no ip igmp snooping query-max-response-time

Parameter: **<1-31744>** Time in tenths of seconds

ip igmp snooping last-member-query-interval:

Set Last Member Query Interval in tenths of seconds

Mode: **Config-if-vlan**

Syntax: **ip igmp snooping last-member-query-interval** <0-31744>

no ip igmp snooping last-member-query-interval

Parameter: **<1-31744>** Time in tenths of seconds

ip igmp snooping unsolicited-report-interval:

Set Unsolicited Report Interval in seconds

Mode: **Config-if-vlan**

Syntax: **ip igmp snooping unsolicited-report-interval** <0-31744>

no ip igmp snooping unsolicited-report-interval

Parameter: **<1-31744>** Time in seconds

ip igmp snooping mrouter:

Multicast router port configuration

Mode: **Interface config**

Syntax: **ip igmp snooping mrouter**

Parameter: **none**

ip igmp snooping max-groups:

IGMP group throttling configuration

Mode:	**Interface config**
Syntax:	**ip igmp snooping max-groups** <1-10>
	no ip igmp snooping max-groups
Parameter:	**<1-10>** Maximum number of groups

ip igmp snooping filter:

Access control on IGMP multicast group registration

Mode:	**Interface config**
Syntax:	**ip igmp snooping filter** <word16>
	no ip igmp snooping filter
Parameter:	**<word16>** Profile name

Interface Configuration Commands

shutdown:

Shut down an interface

Mode: **Config-if**

Syntax: **[no] shutdown**

Parameter: **none**

speed:

Configures interface speed.

Mode: **Config-if**

Syntax: **speed** {2500 | 1000 | 100 | 10 | auto {[10] [100] [1000]} }

no speed

Parameter:

10	**10Mbps**
100	**100Mbps**
1000	**1Gbps**

duplex:

Configures interface speed.

Mode: **Config-if**

Syntax: **duplex** { half | full | auto [half | full] }

no duplex

Parameter: **none**

media-type:

Configure the interface media type.

Mode: **Config-if**

Syntax: **media-type** { rj45 | sfp | dual }

no media-type

Parameter: **none**

flowcontrol:

Configure flow control for the interface.

Mode: **Config-if**

Syntax: **flowcontrol** { on | off }

no flowcontrol

Parameter: **none**

excessive-restart:

Configure backoff algorithm in half duplex mode.

Mode: **Config-if**

Syntax: **[no] excessive-restart**

Parameter: **none**

mtu:

Specify maximum frame size (1518 - 9600 bytes).

Mode: **Config-if**

Syntax: **mtu <Max_frame>**

no mtu

Parameter: **Max_frame:** Number from 1518 to 9600

switchport:

Specify switching mode.

Mode: **Config-if**

Syntax: **switchport mode** {access | trunk | hybrid}

no switchport mode

switchport hybrid port-type { unaware | c-port | s-port | s-custom-port }

no switchport hybrid port-type

switchport hybrid ingress-filtering

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

no switchport hybrid acceptable-frame-type

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

no switchport hybrid egress-tag

Parameter: **none**

IPMC Commands

ipmc:

IPv4 / IPv6 multicast configuration

Mode: **Global config**

Syntax: **ipmc profile**

ipmc profile <profile_name>

ipmc range <entry_name> { <v_ipv4_mcast> [<v_ipv4_mcast_1>] | <v_ipv6_mcast> [<v_ipv6_mcast_1>] }

Parameter:

profile	IPMC profile configuration
range	A range of IPv4/IPv6 multicast addresses for the profile
< word16>	Range entry name in 16 char's
<ipv4_mcast>	Valid IPv4 multicast address
<ipv6_mcast>	Valid IPv6 multicast address

EXAMPLE:

```
EX26262F(config)# ipmc profile test
EX26262F(config-ipmc-profile)#
```

IP Name Server

ip name-server:

Configure DNS server information

Mode: **Global config**

Syntax: **[no] ip name-server** { <v_ipv4_addr> | dhcp [interface vlan <v_vlan_id>] }

Parameter:

dhcp	Dynamic Host Configuration Protocol
<v_vlan_id>	VLANID

IP Route and Routing

ip route:

Add new IP route

Mode: **Global config**

Syntax: **[no] ip route** <ipv4_addr> <ipv4_netmask> <ipv4_addr>

Parameter:

<ipv4_addr> IPV4 address of route

<ipv4_netmask> Mask in A.B.C.D format

<ipv4_addr> Gateway IP address

EXAMPLE:

```
EX26262F(config)# ip route 192.168.1.1 255.255.255.0 192.168.1.100
```

ip routing:

Enable IPv4 and IPv6 routing

Mode: **Global config**

Syntax: **[no] ip routing**

Parameter: **none**

IP Source Binding / Verify Source

ip source binding:

Configure IP source binding

Syntax: **[no] ip source binding interface** <port_type_id> <vlan_id> <ipv4_ucast> <mac_ucast>

[no] ip source binding interface <port_type_id> <vlan_id> <ipv4_ucast> <ipv4_netmask>

[no] ip source binding interface <port_type> <in_port_type_id> <vlan_var> <ipv4_var> <mac_var>

[no] ip verify source

[no] ip verify source limit <0-2>

[no] ip verify source translate

Parameter:

<port_type_id> Port ID in the format of switch-no/port-no, ex 1/1-26 for Gigabitethernet

<vlan_id> Select a VLAN id to configure

<ipv4_ucast>	Select an IP Address to configure
<ipv4_netmask>	Select a subnet mask to configure
<mac_ucast>	Select a MAC address to configure
translate	ip verify source translate all entries

IPv6 Commands

ipv6:

All IPV6 configuration comands.

Mode: **Global config**

Syntax:

ipv6 mld host-proxy [leave-proxy]

ipv6 mld snooping

ipv6 mld snooping vlan <v_vlan_list>

ipv6 mld ssm-range <v_ipv6_mcast> <ipv6_prefix_length>

ipv6 mld unknown-flooding

ipv6 route <v_ipv6_subnet> { <v_ipv6_ucast> | interface vlan <v_vlan_id> <v_ipv6_addr> }

Parameter:

mld	Multicasat Listener Discovery
route	Configure static routes
host-proxy	MLD proxy configuration
snooping	Snooping MLD
ssm-range	IPv6 address range of Source Specific Multicast
unknown-flooding	Flooding unregistered IPv6 multicast traffic
leave-proxy	MLD proxy for leave configuration
vlan	MLD VLAN
<vlan_list>	VLAN identifier(s): VID
<ipv6_mcast>	Valid IPv6 multicast address
X:X:X:X::X/<0-128>	IPv6 prefix x:x::y/z

EXAMPLE:

```
EX26262F(config)# ipv6 mld host-proxy leave-proxy
EX26262F(config)# ipv6 mld snooping vlan 1
EX26262F(config)#
```

LACP Commands

lacp:

Configure the LACP key.

Mode: **Global config**

Syntax: **lacp system-priority** <1-65535>

Parameter: **<1-65535>:** LACP key

lacp (interface):

Configure LACP mode.

Mode: **Config-if-vlan**

Syntax: **lacp**

lacp key { <1-65535> | auto }

lacp role { active | passive }

lacp timeout { fast | slow }

lacp port-priority <1-65535>

Parameter: **<1-65535>** Priority value, lower means higher priority

LLDP Commands

lldp:

Configure LLDP

Mode: **Global config**

Syntax:

lldp holdtime <2-10>

lldp med datum { wgs84 | nad83_navd88 | nad83_mllw }

lldp med fast <1-10>

lldp med location-tlv altitude { meters | floors } <word11>

lldp med location-tlv civic-addr { country | state | county | city | district | block | street | leading-street-direction | trailing-street-suffix | street-suffix | house-no | house-no-suffix | landmark | additional-info | name | zip-code | building | apartment | floor | room-number | place-type | postal-community-name | p-o-box | additional-code } <string250>

lldp med location-tlv elin-addr <dword25>

lldp med location-tlv latitude { north | south } <word8>

lldp med location-tlv longitude { west | east } <word9>

lldp med media-vlan policy-list <range_list>

lldp med media-vlan-policy <0-31> { voice | voice-signaling | guest-voice-signaling | guest-voice | softphone-voice | video-conferencing | streaming-video | video-signaling } { tagged <vlan_id> | untagged } [l2-priority <0-7>] [dscp <0-63>]

lldp reinit <1-10>

lldp timer <5-32768>

lldp transmission-delay <1-8192>

Parameter:

holdtime	Sets LLDP hold time
med	Media Endpoint Discovery.
reinit	LLDP tx reinitialization delay in seconds.
timer	Sets LLDP TX interval
transmission-delay	Sets LLDP transmision-delay.
<2-10>	2-10 seconds.
<1-10>	1-10 seconds.
<5-32768>	5-32768 seconds.
<1-8192>	1-8192 seconds.
datum	Datum (geodetic system) type.
fast	Number of times to repeat LLDP frame transmission at fast start.

location-tlv LLDP-MED Location Type Length Value parameter.

media-vlan-policy Use the media-vlan-policy to create a policy, which can be assigned to an interface.

nad83_mllw Mean lower low water datum 1983

nad83_navd88 North American vertical datum 1983

wgs84 World Geodetic System 1984

altitude **Altitude parameter**

meter **Altitude value**

floors **Altitude value**

civic-addr Civic address information and postal information

country The two-letter ISO 3166 country code in capital ASCII chars

state National subdivisions (state, canton, region, province, prefecture).

county County, parish, gun (Japan), district.

city City, township, shi (Japan) - Example: Copenhagen.

district City division, borough, city district, ward, chou (Japan).

block Neighbourhood, block.

street Street - Example: Poppelvej.

leading-street-direction Leading street direction - Example: N.

trailing-street-suffix Trailing street suffix - Example: SW.

street-suffix Street suffix - Example: Ave, Platz.

house-no House number - Example: 21.

house-no-suffix House number suffix - Example: A, 1/2.

landmark Landmark or vanity address - Example: Columbia University.

additional-info Additional location info - Example: South Wing.

name Name (residence and office occupant)

zip-code Postal/zip code - Example: 2791.

building Building (structure) - Example: Low Library.

apartment Unit (Apartment, suite) - Example: Apt 42.

floor Floor - Example: 4.

room-number Room number - Example: 450F.

place-type Place type - Example: Office.

postal-community-name Postal community name - Example: Leonia.

p-o-box Post office box (P.O. BOX) - Example: 12345.

additional-code Additional code - Example: 1320300003.

<string250> Value for the corresponding selected civic address.

elin-addr Emergency Location Identification Number,

<dword25> ELIN value

north Setting latitude direction to north.

south Setting latitude direction to south.

<word8>	Latitude degrees (0.0000-90.0000).
policy-list	Assignment of policies.
<range_list>	Policies to assign to the interface.
<0-31>	Policy id for the policy which is created.
voice	Create a voice policy.
voice-signaling	Create a voice signaling policy.
guest-voice-signaling	Create a guest voice signaling policy.
guest-voice	Create a guest voice policy.
softphone-voice	Create a softphone voice policy.
video-conferencing	Create a video conferencing policy.
streaming-video	Create a streaming video policy.
video-signaling	Create a video signaling policy.
tagged	The policy uses tagged frames.
<vlan_id>	The VLAN the policy uses tagged frames.
untagged	The policy uses un-tagged frames.
l2-priority	Layer 2 priority.
<0-7>	Priority 0-7
dscp	Differentiated Services Code Point.
<0-63>	DSCP value 0-63.

Logging Commands

logging:

Configure syslog.

Mode	**Global config**	
Syntax:	**logging host** { <ipv4_ucast> | <hostname> }	
	logging level { info | warning | error }	
	logging on	
Parameter:	**host**	host
	<ipv4_ucast>	IP address of the log server
	<hostname>	Domain name of the log server
	level	level
	info	Information
	warning	Warning
	error	Error
	on	Enable syslog server

Loop Protect

loop-protect (global):

Loop protection configuration.

Mode	**Global config**	
Syntax:	**loop-protect**	
	loop-protect shutdown-time <0-604800>	
	loop-protect transmit-time <1-10>	
Parameter:	**shutdown-time**	Loop protection shutdown time interval
	<0-604800>	Shutdown time in second
	transmit-time	Loop protection transmit time interval
	<1-10>	Transmit time in second

loop-protect (interface):

Loop protection configuration.

Mode **Config-if**

Syntax:

loop-protect

loop-protect action { [shutdown] [log] }*1

no loop-protect action

loop-protect tx-mode

Parameter: **none**

Port Mirroring and Monitoring

monitor:

Set mirroring and monitoring configurations

Mode: **Global config**

Syntax:

monitor destination interface <port_type> <port_type_id>

monitor source { interface <port_type> <port_type_list> | cpu } { both | rx | tx }

Parameter:

destination	The destination port.
interface	Interface to mirror traffic to.
source	The source port.
interface	Mirrort interface traffic.
<port_type>	1 Gigabit Ethernet port
*****	All switches or all ports
<port_type_list>	Port list in 1/1-26.
cpu	Mirrot CPU traffic.
both	Mirror both ingress and egress traffic.
rx	Setting source port to rx will mirror bothingress traffic.
tx	Setting source port to tx will mirror both egress traffic.
<port_type>	Port type in Gigabitethernet
<port_type_list>	Port list in 1/1-26 for Gigabitethernet

MLD Commands

ipv6 mld:

Set Version of MLD Operating on Hosts and Routers.

Syntax:

ipv6 mld snooping
ipv6 mld unknown-flooding
ipv6 mld host-proxy [leave-proxy]
ipv6 mld ssm-range <ipv6_mcast> <8-128>
no ipv6 mld ssm-range
ipv6 mld snooping vlan <vlan_list>
no ipv6 mld snooping vlan [<vlan_list>]
ipv6 mld snooping immediate-leave
ipv6 mld snooping mrouter
ipv6 mld snooping max-groups <1-10>
no ipv6 mld snooping max-groups
ipv6 mld snooping filter <word16>
no ipv6 mld snooping filter
ipv6 mld snooping
ipv6 mld snooping querier election
ipv6 mld snooping compatibility { auto | v1 | v2 }
no ipv6 mld snooping compatibility
ipv6 mld snooping priority <0-7>
no ipv6 mld snooping priority
ipv6 mld snooping robustness-variable <1-255>
no ipv6 mld snooping robustness-variable
ipv6 mld snooping query-interval <1-31744>
no ipv6 mld snooping query-interval
ipv6 mld snooping query-max-response-time <0-31744>
no ipv6 mld snooping query-max-response-time
ipv6 mld snooping last-member-query-interval <0-31744>
no ipv6 mld snooping last-member-query-interval
ipv6 mld snooping unsolicited-report-interval <0-31744>
no ipv6 mld snooping unsolicited-report-interval

Parameter:

<vlan-list>: VLAN list, available value is from 1 to 4094 format: 1,3-5
Forced-MLDv1: Set MLDv1 of MLD operating on hosts and routers

Forced-MLDv2: Set MLDv2 of MLD operating on hosts and routers

MLD-Auto: Set auto mode of MLD operating on hosts and routers

<0-31744>: Range:0~31744 tenths of sec, default:100 tenths of sec.

MVR Commands

MVR

The MVR feature enables multicast traffic forwarding on the Multicast VLAN. In a multicast television application, a PC or a television with a set-top box can receive the multicast stream. Multiple set-top boxes or PCs can be connected to one subscriber port, which is a switch port configured as an MVR receiver port. When a subscriber selects a channel, the set-top box or PC sends an IGMP join message to Switch A to join the appropriate multicast. Uplink ports that send and receive multicast data to and from the multicast VLAN are called MVR source ports.

mvr:

Configure MVR

Mode: **Global config**

Syntax:

[no] mvr

[no] mvr name <mvr_name> channel <profile_name>

[no] mvr name <mvr_name> frame priority <cos_priority>

[no] mvr name <mvr_name> frame tagged

[no] mvr name <mvr_name> igmp-address <v_ipv4_ucast>

[no] mvr name <mvr_name> last-member-query-interval <ipmc_lmqi>

[no] mvr name <mvr_name> mode { dynamic | compatible }

[no] mvr vlan <v_vlan_list> [name <mvr_name>]

[no] mvr vlan <v_vlan_list> channel <profile_name>

[no] mvr vlan <v_vlan_list> frame priority <cos_priority>

[no] mvr vlan <v_vlan_list> frame tagged

[no] mvr vlan <v_vlan_list> igmp-address <v_ipv4_ucast>

[no] mvr vlan <v_vlan_list> last-member-query-interval <ipmc_lmqi>

[no] mvr vlan <v_vlan_list> mode { dynamic | compatible }

Parameter:

name	MVR multicast name
<word16>	MVR multicast VLAN name
channel	MVR channel configuration
<word16>	Profile name in 16 char's
frame	MVR control frame in TX
priority	Interface CoS priority
<0-7>	CoS priority ranges from 0 to 7
tagged	Tagged IGMP/MLD frames will be sent
igmp-address	MVR address configuration used in IGMP
<ipv4_ucast>	A valid IPv4 unicast address MVR multicast VLAN name
last-member-query-interval	Last Member Query Interval in tenths of seconds
<0-31744>	0 - 31744 tenths of seconds
mode	MVR mode of operation
dynamic	Dynamic MVR operation mode
compatible	Compatible MVR operation mode
vlan	MVR multicast vlan
<vlan_list>	MVR multicast VLAN list
channel	MVR channel configuration
<word16>	Profile name in 16 char's
frame	MVR control frame in TX
priority	Interface CoS priority
<0-7>	CoS priority ranges from 0 to 7
igmp-address	MVR address configuration used in IGMP
<ipv4_ucast>	A valid IPv4 unicast address
<vlan_list>	MVR multicast VLAN list
last-member-query-interval	Last Member Query Interval in tenths of seconds
<0-31744>	0 - 31744 tenths of seconds
compatible	Compatible MVR operation mode

Network Time Protocol

ntp:

Configure NTP

Mode: **Global config**

Syntax: **ntp**

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

ntp server <1-5> ip-address <ipv4_ucast>

ntp server <1-5> ip-address <ipv6_ucast>

Parameter:

server	Configure NTP server
<1-5>	index number
ip-address	ip address
<ipv4_ucast>	ipv4 address
<ipv6_ucast>	ipv6 address
<hostname>	domain name

Power Over Ethernet

poe (global):

Configure power over Ethernet

Syntax:

poe management mode { class-consumption | class-reserved-power | allocation-consumption | allocation-reserved-power | lldp-consumption | lldp-reserved-power }

no poe management mode

poe ping-check { enable | disable }

poe select-all <port_list>

poe supply sid <1~16> <1-2000>

no poe supply [sid <1~16>]

no poe schedule-all <range_list>

poe delay-mode <range_list>

no poe delay-mode <range_list>

poe delay-time <range_list> <0-300>

Parameter:

management	Use management mode to configure PoE power management method.
select-all	Configure PoE Schedule mode.
Ping-check	Enable/Disable POE Ping Check.
Mode	PoE Power Management Mode
allocation-consumption	Max. port power determined by allocation, and

power is managed according to power consumption.
allocation-reserved-power Max. port power determined by alocated, 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.

poe (interface):

Configure power over Ethernet

Syntax:

poe mode { standard | plus }

no poe mode

poe priority { low | high | critical }

no poe priority

poe power limit { <fword2.1> }

no poe power limit

[no] poe schedule-mode

[no] poe hour <0-23>

[no] poe Sun

[no] poe Mon

[no] poe Tue

[no] poe Wed

[no] poe Thr

[no] poe Fri

[no] poe Sat

Parameter:

management Use management mode to configure PoE power management method.
select-all Configure PoE Schedule mode.
Ping-check Enable/Disable POE Ping Check.
Mode PoE Power Management Mode
allocation-consumption Max. port power determined by allocation, and power is managed according to power consumption.
allocation-reserved-power Max. port power determined by alocated, 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.

Port security Commands

Port security

This section shows you to to configure the Port Security settings of the Switch. You can use the Port Security feature to restrict input to an interface by limiting and identifying MAC addresses.

port-security:

Configure the action involved with exceeding a limit

Syntax:

port-security

port-security aging

port-security aging time <v_10_to_10000000>

Parameter:

aging	Time in seconds between check for activity on learned MAC addresses.
time	Time in seconds between check for activity on learned MAC addresses.
<10-10000000>	seconds

Privilege level Commands

group:

Configure a privilege level group

Mode: **Global config**

Syntax:

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

Parameter:

config-vlan	VLAN Configuration Mode
configure	Global configuration mode
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
level	Set privilege level of command
<LINE>	Initial valid words and literals of the command to modify, in 128 char's

QoS Commands

QoS

The switch support four QoS queues per port with strict or weighted fair queuing scheduling. It supports QoS Control Lists (QCL) for advance programmable QoS classification, based on IEEE 802.1p, Ethertype, VID, IPv4/IPv6 DSCP and UDP/TCP ports and ranges.

qos map:

Configure global QOS map/table

Mode: **Global config**

Syntax:

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

qos map dscp-classify { <dscpNum : 0~63> | { be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va } }

qos map dscp-cos { < dscpNum : 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 <Cos : 0-7> dpl <dpl>

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

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

Parameter:

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
dpl	Specify drop precedence level
<Dpl : 0~1>	Specific drop precedence level or range
dscp	Specify DSCP
<DscpNum : 0-63>	Specific DSCP
cos	Specify class of QoS
<Cos : 0-7>	Specific class of QoS
af11	Assured Forwarding PHB AF11(DSCP 10)
af12	Assured Forwarding PHB AF12(DSCP 12)
af13	Assured Forwarding PHB AF13(DSCP 14)
af21	Assured Forwarding PHB AF21(DSCP 18)
af22	Assured Forwarding PHB AF22(DSCP 20)
af23	Assured Forwarding PHB AF23(DSCP 22)
af31	Assured Forwarding PHB AF31(DSCP 26)
af32	Assured Forwarding PHB AF32(DSCP 28)
af33	Assured Forwarding PHB AF33(DSCP 30)
af41	Assured Forwarding PHB AF41(DSCP 34)
af42	Assured Forwarding PHB AF42(DSCP 36)
af43	Assured Forwarding PHB AF43(DSCP 38)
be	Default PHB(DSCP 0) for best effort traffic
cs1	Class Selector PHB CS1 precedence 1(DSCP 8)
cs2	Class Selector PHB CS2 precedence 2(DSCP 16)
cs3	Class Selector PHB CS3 precedence 3(DSCP 24)
cs4	Class Selector PHB CS4 precedence 4(DSCP 32)
cs5	Class Selector PHB CS5 precedence 5(DSCP 40)
cs6	Class Selector PHB CS6 precedence 6(DSCP 48)
cs7	Class Selector PHB CS7 precedence 7(DSCP 56)
ef	Expedited Forwarding PHB(DSCP 46)
va	Voice Admit PHB(DSCP 44)

qos qce:

Configure QOS control entries

Mode: **Global config**

Syntax:

qos qce refresh

qos qce { [update] } <Id : 1-256> [{ next <Id : 1-256> } | last] [ingress interface *|Gigabitethernet <PORT_LIST>] [tag { tagged | untagged | any }] [vid { <vlan_list> | any }] [pcp { <pcp> | any }] [dei { <Dpl : 0-1> | any }] [smac { <mac_addr> | <oui> | any }] [dmac-type { unicast | multicast | broadcast | any }] [frametype { any | { etype [{ <0x600-0x7ff,0x801-0x86dc,0x86de-0xffff> | any }] } | { llc [dsap { <0-0xff> | any }] [ssap { <0-0xff> | any }] [control { <0-0xff> |

any }] } | { snap [{ <0-0xffff> | any }] } | { ipv4 [proto { <0-255> | tcp | udp | any }] [sip { <ipv4_subnet> | any }] [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 } | any }] [frag { yes | no | any }] [sport { <0~65535> | any }] [dport { <0~65535> | any }] } | { ipv6 [proto { <0-255> | tcp | udp | any }] [sip { <ipv4_subnet> | any }] [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 } | any }] [sport { <0~65535> | any }] [dport { <0~65535> | any }] } }] [action { [cos { <0-7> | default }] [dpl { <0-1> | default }] [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 } | default }] }]

Parameter:

<Id : 1-256>	QCE ID
refresh	Refresh QCE tables in hardware
update	Update an existing QCE
action	Specify action
dei	Specify DEI (Drop Eligible Indicator)
dmac-type	Specify DMAC type
frametype	Specify frame type
ingress	Ingress interfaces
last	Place QCE at the end
next	Place QCE before the next QCE ID
pcp	Specify PCP (Priority Code Point)
smac	Specify SMAC. If 'qos qce dmac-dip' is set, this parameter specifies the DMAC
tag	Specify tag options
vid	Specify VLAN ID
cos	Specify class of service
dpl	Specify drop precedence level
dscp	Specify DSCP
cos	Specify class of service
<Cos : 0-7>	Specific class of service
default	Keep default class of service
<Dpl : 0-1>	Specific drop precedence level
default	Keep default drop precedence level
<Dscp : 0-63>	Specific DSCP
af11	Assured Forwarding PHB AF11(DSCP 10)
af12	Assured Forwarding PHB AF12(DSCP 12)
af13	Assured Forwarding PHB AF13(DSCP 14)
af21	Assured Forwarding PHB AF21(DSCP 18)
af22	Assured Forwarding PHB AF22(DSCP 20)
af23	Assured Forwarding PHB AF23(DSCP 22)
af31	Assured Forwarding PHB AF31(DSCP 26)
af32	Assured Forwarding PHB AF32(DSCP 28)
af33	Assured Forwarding PHB AF33(DSCP 30)

af41	Assured Forwarding PHB AF41(DSCP 34)
af42	Assured Forwarding PHB AF42(DSCP 36)
af43	Assured Forwarding PHB AF43(DSCP 38)
be	Default PHB(DSCP 0) for best effort traffic
cs1	Class Selector PHB CS1 precedence 1(DSCP 8)
cs2	Class Selector PHB CS2 precedence 2(DSCP 16)
cs3	Class Selector PHB CS3 precedence 3(DSCP 24)
cs4	Class Selector PHB CS4 precedence 4(DSCP 32)
cs5	Class Selector PHB CS5 precedence 5(DSCP 40)
cs6	Class Selector PHB CS6 precedence 6(DSCP 48)
cs7	Class Selector PHB CS7 precedence 7(DSCP 56)
default	Keep default DSCP
ef	Expedited Forwarding PHB(DSCP 46)
va	Voice Admit PHB(DSCP 44)
any	Any
broadcast	Broadcast
multicast	Multicast
unicast	Unicast
etype	Ethernet frames
ipv4	IPv4 frames
ipv6	IPv6 frames
llc	LLC frames
snap	SNAP frames
<Etype : 0x600-0x7ff,0x801-0x86dc,0x86de-0xffff>	Specific EtherType
interface	Interfaces
<Next : 1-256>	The next QCE ID
<Pcp : pcp>	Specific PCP (0-7) or range (0-1, 2-3, 4-5, 6-7, 0-3 or 4-7)
<Smac : mac_addr>	Specific SMAC (XX-XX-XX-XX-XX-XX)
tagged	Tagged frames only
untagged	Untagges frames only
<Vid : vlan_list>	Specific VLAN ID or range
interface	Interfaces
Gigabitethernet	1 Gigabit Ethernet Port
<PORT_LIST>	Port list in 1/1-26 for Gigabitethernet

qos storm:

Configure storm policer

Mode: **Global config**

Syntax: **qos** storm { unicast | multicast | broadcast } <Rate : 1,2,4,8,16,32,64,128,256,512,1024> [kfps]

Parameter:

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

qos (interface commands):

Configure QOS on a port

Mode: **Config-if**

Syntax:
qos dpl <dpl>
no qos dpl
qos pcp <0-7>
no qos pcp
qos dei <0-1>
no qos dei
qos trust tag
qos trust dscp
qos map tag-cos pcp <0~7> dei <0~1> cos <0-7> dpl <dpl>
no qos map tag-cos pcp <0~7> dei <0~1>
qos policer <uint> [fps] [flowcontrol]
no qos policer
qos queue-policer queue <0~7> <uint>
no qos queue-policer queue <0~7>
qos wrr <1-100> <1-100> <1-100> <1-100> <1-100> <1-100>
no qos wrr
qos shaper <uint>
no qos shaper
qos queue-shaper queue <0~7> <uint> [excess]
no qos queue-shaper queue <0~7>
qos tag-remark { pcp <0-7> dei <0-1> | mapped }
no qos tag-remark
qos map cos-tag cos <0~7> dpl <0~1> pcp <0-7> dei <0-1>
no qos map cos-tag cos <0~7> dpl <0~1>
qos dscp-translate
qos dscp-classify { zero | selected | any }
no qos dscp-classify
qos dscp-remark { rewrite | remap | remap-dp }
no qos dscp-remark
qos storm { unicast | broadcast | unknown } <100-13200000> [fps]
no qos storm { unicast | broadcast | unknown }
qos qce { [addr { source | destination }] [key { double-tag | normal | ip-addr | mac-ip-addr }] }*1
no qos qce { [addr] [key] }*1
debug qos shaper cir { <100-3300000> [cbs <4096-258048>] } { [eir <100-3300000> [ebs <4096-258048>]] }
no debug qos shaper
debug qos queue-shaper queue <0~7> { cir <100-3300000> [cbs <4096-258048>] } { [eir <100-3300000> [ebs <4096-258048>]] } [excess]
no debug qos queue-shaper queue <0~7>

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

Reload

reload:

Reboot the switch

Mode: **Privilegd exec**

Syntax: **reload { { cold [sid <usid>] } | { defaults [keep-ip] } }**

Parameter:	**cold**	Reload cold, i.e. reboot.
	defaults	Reload defaults without rebooting.
	keep-ip	Attempt to keep VLAN1 IP setup.r

RMON

rmon:

Configure Remote Monitoring

Mode: **Global config**

Syntax: **rmon** alarm <1-65535> <WORD> <1-2147483647> { absolute | delta } rising-threshold <-2147483648-2147483647> [<0-65535>] falling-threshold <-2147483648-2147483647> [<0-65535>] { [rising | falling | both] }

rmon alarm <1-65535> { ifInOctets | ifInUcastPkts | ifInNUcastPkts | ifInDiscards | ifInErrors | ifInUnknownProtos | ifOutOctets | ifOutUcastPkts | ifOutNUcastPkts | ifOutDiscards | ifOutErrors } <uint> <1-2147483647> { absolute | delta } rising-threshold <-2147483648-2147483647> [<0-65535>] falling-threshold <-2147483648-2147483647> [<0-65535>] { [rising | falling | both] }

rmon event <1-65535> [log] [trap <word127>] { [description <line127>] }

no rmon alarm <1-65535>

no rmon event <1-65535>

Parameter:	**alarm**	Configure an RMON alarm
	event	Configure an RMON event
	<1-65535>	Alarm entry ID
	<WORD>	MIB object to monitor
	<1-2147483647>	Sample interval

absolute Test each sample directly

delta Test delta between samples

rising-threshold Configure the rising threshold

<-2147483648-2147483647> rising threshold value

<0-65535> Event to fire on rising threshold crossing

falling-threshold Configure the falling threshold

<-2147483648-2147483647> falling threshold value

rising Trigger alarm when the first value is larger than the rising threshold

falling Trigger alarm when the first value is less than the falling threshold

both Trigger alarm when the first value is larger than the rising threshold or less than the falling threshold (default)

ifInOctets The total number of octets received on the interface, including framing characters

ifInUcastPkts The number of uni-cast packets delivered to a higher-layer protocol

ifInNUcastPkts The number of broad-cast and multi-cast packets delivered to a higher-layer protocol

ifInDiscards The number of inbound packets that are discarded even the packets are normal

ifInErrors The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol

ifInUnknownProtos The number of the inbound packets that were discarded because of the unknown or un-support protocol

ifOutOctets The number of octets transmitted out of the interface , including framing characters

ifOutUcastPkts The number of uni-cast packets that request to transmit

ifOutNUcastPkts The number of broad-cast and multi-cast packets that request to transmit

ifOutDiscards The number of outbound packets that are discarded event the packets is normal

ifOutErrors The The number of outbound packets that could not be transmitted because of errors

<uint> ifIndex

<1-2147483647> Sample interval

absolute Test each sample directly

delta Test delta between samples

rising-threshold Configure the rising threshold

SFlow Commands

SFlow

The sFlow Collector configuration for the switch can be monitored and modified here. Up to 1 Collector is supported. This page allows for configuring sFlow collector IP type, sFlow collector IP Address and Port Number for each sFlow Collector

collector:

Set sFlow Collector Configuration

Mode: **Global config**

Syntax: **sflow agent-ip** {ipv4 <ipv4_addr> | ipv6 <ipv6_addr>}

no sflow agent-ip

sflow timeout [receiver <range_list>] <0-2147483647>

no sflow timeout [receiver <range_list>]

sflow collector-address [receiver <range_list>] [<word>]

no sflow collector-address [receiver <range_list>]

sflow collector-port [receiver <range_list>] <1-65535>

no sflow collector-port [receiver <range_list>]

sflow max-datagram-size [receiver <range_list>] <200-1468>

no sflow max-datagram-size [receiver <range_list>]

sflow sampling-rate [sampler <range_list>] [<1-4294967295>]

sflow max-sampling-size [sampler <range_list>] [<14-200>]

no sflow max-sampling-size [sampler <range_list>]

sflow counter-poll-interval [sampler <range_list>] [<1-3600>]

no sflow counter-poll-interval [<range_list>]

sflow [<range_list>]

Parameter: **IPv4:** IP type

IPv6: IP type

<ip-address>: IP address

<1-65535>: TCP/UDP port number. By default, the port number is 6343

<0-2147483647>: Set the receiver timeout for list of receiver ID (RID). Collector cannot collect samples unless receivertimeout

<200-1500>: Set the reciever datagram length for list of receiver ID (RID)

<port-list>: available value is from switch physic port density, format: 1,3-5

ALL: Sample on both RX and TX

RX: Sample on RX

TX: Sample on TX

none: Sampling is disabled

<0-4095>: If parameter sample_rate is 'N' then 1/N of packets is sampled

<14-200>: Configures the size of the header of the sampled frame to be copied to the Queue for further processing. The Max header size ranges from 14 to 200 bytes

<0-3600>: Configures the polling interval for the counter sampling. The accepted value for Counter Polling Interval ranges from 0 to 3600 seconds. Default value is 0 seconds which means polling is disabled.

SMTP Commands

smtp:

Configure SMTP

Syntax: **smtp delete mailaddress** <1-6>

smtp delete { server | username | sender | returnpath | mailaddress <1-6> } smtp mailaddress <1-6> <word47>

smtp (returnpath | sender | server) <word47>

smtp username <word31> <word31>

smtp level <0-7>

Parameter:

delete	Delete command
mailaddress	Configure email address
returnpath	Configure email returnpath
sender	Configure email sender
server	Configure email server
username	Configure email user name
mailaddress	Delete email address
returnpath	Delete returnpath
sender	Delete sender
server	Delete email server
username	Delete username and password
<1-6>	Email address index
<word47>	Up to 47 characters describing mail address
<word47>	Up to 47 characters describing returnpath
<word47>	Up to 47 characters describing sender
<word47>	Up to 47 characters describing email server
<word31>	Up to 47 characters describing user name
<word31>	Configure email password

SNMP Commands

snmp-server:

Configure SNMP

Mode: **Global config**

Syntax:

snmp-server access <GroupName : word32> model { v1 | v2c | v3 | any } level { auth | noauth | priv } [read <ViewName : word255>] [write <WriteName : word255>]

snmp-server community v2c <Community : word127> [ro | rw]

snmp-server community v3 <word127> [<ipv4_addr> <ipv4_netmask>]

snmp-server contact <line255>

snmp-server engine-id local <Engineid : word10-32>

snmp-server host <word32> [Use this command to enter **config-snmps-host** mode]

snmp-server location <line255>

snmp-server security-to-group model { v1 | v2c | v3 } name <SecurityName : word32> group <GroupName : word32>

snmp-server trap

snmp-server user <Username : word32> engine-id <Engineid : word10-32> [{ md5 <Md5Passwd : word8-32> | sha <ShaPasswd : word8-40> } [priv { des | aes } <word8-32>]]

snmp-server version { v1 | v2c | v3 }

snmp-server view <ViewName : word32> <OidSubtree : word255> { include | exclude }

Parameter:

<GroupName : word32>	group name
model	security model
any	any security model
v1	v1 security model
v2c	v2c security model
v3	v3 security model
level	security level
auth	authNoPriv Security Level
noauth	noAuthNoPriv Security Level
priv	authPriv Security Level
read	specify a read view for the group
write	specify a write view for the group
<ViewName : word255>	read view name
<WriteName : word255>	write view name
<line255>	contact string
local	Set SNMP local engine ID
<Engineid : word10-32>	local engine ID
name	security user
<SecurityName : word32>	security user name
group	security group
<GroupName : word32>	security group name
md5	Set MD5 protocol
<Md5Passwd : word8-32>	MD5 password
sha	Set SHA protocol

<ShaPasswd word8-40>	SHA password
priv	Set Privacy
des	Set DES protocol
aes	Set AES protocol
<word8-32>	Set privacy password

system:

Configure SNMP server

Mode: **Global config**

Syntax: **system** contact <v_line255>
system location <v_line255>
system name <v_line255>
system descriptuon <v_line255>
system reboot <Fri, Mon, Sat, Sun, Thr, Tue, Wed> {mode <enable/disable}

Parameter: **system** contact <v_line255>
system location <v_line255>
system name <v_line255>

shutdown:

Disable trap configuration

Mode: **Config-snmps-host**

Syntax: **shutdown**

Parameter: **none**

host:

SNMP host configuration

Mode: **Config-snmps-host**

Syntax: **host** { <ipv4_ucast> | <hostname> } [<1-65535>] [traps | informs]
host <ipv6_ucast> [<1-65535>] [traps | informs]
no host

Parameter: **none**

version:

Set SNMP trap version.

Mode: **Config-snmps-host**

Syntax: **version** { v1 [<word127>] | v2 [<word127>] | v3 [probe | engineID <word10-32>] [<word32>] }
no version

Parameter: **none**

informs:

Set SNMP trap version.

Mode: **Config-snmps-host**

Syntax: **informs retries** <0-255> timeout <0-2147>
no informs

Parameter: **none**

SSH Commands

ip ssh:

Enable SSH

Mode: **Global config**

Syntax: **ip ssh**

Parameter: **none**

show ip ssh:

Show SSH configuration

Mode: **Privileged exec**

Syntax: **show ip ssh**

Parameter: **none**

STP Commands

STP

The Spanning Tree Protocol (STP) can be used to detect and disable network loops, and to provide backup links between switches, bridges or routers. This allows the switch to interact with other bridging devices (that is, an STP-compliant switch, bridge or router) in your network to ensure that only one route exists between any two stations on the network, and provide backup links which automatically take over when a primary link goes down.

STP - STP uses a distributed algorithm to select a bridging device (STP- compliant switch, bridge or router) that serves as the root of the spanning tree network. It selects a root port on each bridging device (except for the root device) which incurs the lowest path cost when forwarding a packet from that device to the root device. Then it selects a designated bridging device from each LAN which incurs the lowest path cost when forwarding a packet from that LAN to the root device. All ports connected to designated bridging devices are assigned as designated ports. After determining the lowest cost spanning tree, it enables all root ports and designated ports, and disables all other ports. Network packets are therefore only forwarded between root ports and designated ports, eliminating any possible network loops.

Once a stable network topology has been established, all bridges listen for Hello BPDUs (Bridge Protocol Data Units) transmitted from the Root Bridge. If a bridge does not get a Hello BPDU after a predefined interval (Maximum Age), the bridge assumes that the link to the Root Bridge is down. This bridge will then initiate negotiations with other bridges to reconfigure the network to reestablish a valid network topology.

spanning-tree aggregation:

Aggregation mode.

Mode: **Global config**

Syntax: **spanning-tree aggregation**

Parameter: **none**

EXAMPLE:

```
EX26262F(config)# spanning-tree  aggregation
EX26262F(config-stp-aggr)#
```

spanning-tree edge:

Configure edge ports

Mode: **Global config**

Syntax: **spanning-tree** edge bpdu-filter

spanning-tree edge bpdu-guard

Parameter:

bpdu-filter	Enable BPDU filter (stop BPDU tx/rx)
bpdu-guard	Enable BPDU guard

EXAMPLE:

```
EX26262F(config)# spanning-tree edge bpdu-filter
EX26262F(config)#
```

spanning-tree mode:

Set stp protocol mode

Mode: **Global config**

Syntax: **spanning-tree** mode { stp | rstp | mstp }

Parameter:

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

EXAMPLE:

```
EX26262F(config)# spanning-tree mode mstp
EX26262F(config)#
```

spanning-tree mst:

STP bridge instance

Mode: **Global config**

Syntax: **spanning-tree** mst <Instance : 0-7> priority <Prio : 0-61440>

spanning-tree mst < Instance : 0-7> vlan <vlan_list>

spanning-tree mst forward-time <Fwdtime : 4-30>

spanning-tree mst max-age <Maxage : 6-40> [forward-time <Fwdtime : 4-30>]

spanning-tree mst max-hops <Maxhops : 6-40>

spanning-tree mst name <Name : word32> revision <0-65535>

Parameter:

<Instance : 0-7>	instance 0-7 (CIST=0, MST2=1...)

forward-time	Delay between port states
max-age	Max bridge age before timeout
max-hops	MSTP bridge max hop count
name	Name keyword
priority	Priority of the instance
vlan	VLAN keyword
<Prio : 0-61440>	Range in seconds
<vlan_list>	Range of VLANs
<Fwdtime : 4-30>	Range in seconds
<Maxage : 6-40>	Range in seconds
<Maxhops : 6-40>	Hop count range
<Name : word32>	Name of the bridge
revision	Revision keyword
<0-65535>	Revision number

EXAMPLE:

```
EX26262F(config)# spanning-tree mst 7 vlan 10
```

spanning-tree recovery:

Set error recovery timeouts.

Mode: **Global config**

Syntax: **spanning-tree** recovery interval <Interval: 30 - 86400>

Parameter:

interval	The interval
<Interval : 30-86400>	Range in seconds

EXAMPLE:

```
EX26262F(config)# spanning-tree recovery interval 50
```

spanning-tree transmit:

BPDUs to transmit

Mode: **Global config**

Syntax: **spanning-tree** transmit hold-count <Holdcount: 1 - 10>

Parameter:

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

EXAMPLE:

```
EX26262F(config)# spanning-tree transmit hold-count 5
```

Terminal Commands

terminal:

Set terminal line parameters

Mode: **Privilegd exec**

Syntax:

terminal editing

terminal exec-timeout <0-1440> [<0-3600>]

terminal help

terminal history size <0-32>

terminal length <0 or 3-512>

terminal width <0 or 40-512>

Parameter:

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
<0-1440>	Timeout in minutes
<0-3600>	Timeout in seconds
size	Set history buffer size
<0-32>	Number of history commands, 0 means disable
<0 or 3-512>	Number of lines on screen (0 for no pausing)
<0 or 40-512>	Number of characters on a screen line (0 for unlimited width)

UPnP Commands

UPnP

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

upnp:

Configure UPnP settings

Mode: **Global config**

Syntax: **upnp**

upnp advertising-duration <100 - 86400>

upnp ttl <1-255>

Parameter:

advertising-duration	Set advertising duration
ttl	Set TTL value
<100-86400>	advertising duration
<1-255>	TTL value

Username Commands

username:

Establish User Name Authentication.

Syntax: **username** <username> privilege <priv> password encrypted <encry_password>

username <username> privilege <priv> password none

username <username> privilege <priv> password unencrypted <password>

Parameter:

<Username: word31>	User name allows letters, numbers and underscores
privilege	Set user privilege level
<privilegeLevel: 0-15>	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
<Password: line31>	The UNENCRYPTED (Plain Text) user password. Any character is accepted, including space. Note that there is no way to get the Plain Text password after this command. The system will always display the ENCRYPTED password.
<Password: word4-44>	The ENCRYPTED (hidden) user password. Note that the ENCRYPTED password will be decoded by the system internally. You cannot directly use it as same as the Plain Text and it is not human-readable text normally.

VLAN Commands

VLAN

To assign a specific VLAN for management purpose. The management VLAN is used to establish an IP connection to the switch from a workstation connected to a port in the VLAN. This connection supports a VSM, SNMP, and Telnet session. By default, the active management VLAN is VLAN 1. Only one management VLAN can be active at a time.

vlan:

VLAN commands

Mode: **Global config**

Syntax:

vlan <vlan_list>

vlan ethertype s-custom-port <0x0600-0xffff>

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>

Parameter:

<vlan_list>	ISL VLAN IDs 1-4095
ethertype	Ether type for Custom S-ports
protocol	Protocol-based VLAN commands
s-custom-port	Custom S-ports configuration
<0x0600-0xffff>	Ether type (Range: 0x0600-0xffff>
eth2	Ethernet-based VLAN commands
<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
snap	SNAP-based VLAN group
<0x0-0xffffff>	SNAP OUI (Range 0x000000 - 0XFFFFFF)
rfc_1042	SNAP OUI is rfc_1042
snap_8021h	SNAP OUI is 8021h
<0x0-0xffff>	PID (Range: 0x0 - 0xFFFF)
llc	LLC-based VLAN group
<0x0-0xff>	DSAP (Range: 0x00 - 0xFF)
<0x0-0xff>	SSAP (Range: 0x00 - 0xFF)
group	Protocol-based VLAN group commands

<word16> Group Name (Range: 1 - 16 characters)

EXAMPLE:

```
EX26262F(config)# vlan ethertype s-custom-port 0x1111
EX26262F(config)# vlan protocol eth2 arp group 123
EX26262F(config)#
```

switchport vlan:

Configure VLAN characteristics on an interface.

Mode: **Config-if**

Syntax:

switchport vlan mac <mac_ucast> vlan <vlan_id>

switchport vlan protocol group <word16> vlan <vlan_id>

switchport vlan ip-subnet id <1-128> <ipv4_subnet> vlan <vlan_id>

no switchport vlan ip-subnet id <1~128>

switchport access vlan <vlan_id>

no switchport access vlan

switchport trunk native vlan <vlan_id>

no switchport trunk native vlan

switchport hybrid native vlan <vlan_id>

no switchport hybrid native vlan

switchport trunk vlan tag native

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

no switchport trunk allowed vlan

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

no switchport hybrid allowed vlan

switchport forbidden vlan {add|remove} <vlan_list>

no switchport forbidden vlan

switchport voice vlan mode { auto | force | disable }

no switchport voice vlan mode

switchport voice vlan security

switchport voice vlan discovery-protocol {oui | lldp | both}

no switchport voice vlan discovery-protocol

Parameter: **none**

Voice VLAN Commands

Voice VLAN

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

The Voice VLAN feature enables voice traffic forwarding on the Voice VLAN, then the switch can classify and schedule network traffic. It is recommended that there be two VLANs on a port - one for voice, one for data. Before connecting the IP device to the switch, the IP phone should configure the voice VLAN ID correctly.

voice:

Voice appliance attributes.

Mode **Global config**

Syntax:

voice vlan

voice vlan aging-time <aging_time>

voice vlan class { <traffic_class> | low | normal | medium | high }

voice vlan oui <oui> [description <description>]

voice vlan vid <vid>

Parameter:

advertising-duration	Set advertising duration
vlan	Vlan for voice traffic
aging-time	Set secure learning aging time
<10-10000000>	Aging time, 10-10000000 seconds
class	Set traffic class
<0-7>	Traffic class value
oui	OUI configuration
<oui>	OUI value
description	Set description for the OUI
<line32>	Description line
vid	Set VLAN ID
<vlan_id>	VLAN ID, 1-4095

EXAMPLE:

```
EX26262F(config)# voice vlan aging-time 3333
EX26262F(config)# voice vlan class 7
EX26262F(config)# voice vlan vid 3333
EX26262F(config)#
```

Web Commands

web:

Configure time of inactivity before automatic logout

Mode: **Global config**

Syntax: **web privilege group** <CWORD> level { [cro <0-15>] [crw <0-15>] [sro <0-15>] [srw <0-15>] }

no web privilege group [<cword>] level

Parameter:

privilege	Web privilege
group	Web privilege group
CWORD	Valid words are 'Aggregation' 'Debug' 'Dhcp_Client' 'Green_Ethernet' 'IP2' 'IPMC_Snooping' 'LACP' 'LLDP' 'Loop_Protect' 'MAC_Table' 'MEP' 'MVR' 'Maintenance' 'Mirroring' 'NTP' 'POE' 'Ports' 'Private_VLANs' 'QoS' 'RPC' 'Security' 'Spanning_Tree' 'System' 'Timer' 'UPnP' 'VCL' 'VLAN_Translation' 'VLANs' 'Voice_VLAN' 'sFlow'
level	Web privilege group level
cro	Configuration Read-only level
crw	Configuration Read-write level
sro	Status/Statistics Read-only level
srw	Status/Statistics Read-write level

EXAMPLE:

```
EX26262F(config)# web privilege group ptp level sro 10
```

EtherWAN has made a good faith effort to ensure the accuracy of the information in this document and disclaims the implied warranties of merchantability and fitness for a particular purpose, and makes no express warranties, except as may be stated in its written agreement with and for its customers.

EtherWAN shall not be held liable to anyone for any indirect, special or consequential damages due to omissions or errors. The information and specifications in this document are subject to change without notice.

June 8, 2017