3onedata

# IEM6300-20G
# Layer 2 Industrial Ethernet Switch Module
# CLI User Manual

Document Version 01
Issue Date: 6/14/2022

**Industrial Ethernet Communication Solution Expert** **3onedata Co., Ltd.**

## Trademark statement

3onedata , 3onedata and 3One data are the registered trademark owned by 3onedata Co., Ltd. And other trademarks mentioned in this manual belong to their corresponding companies.

## Note

Purchased product, service or features should be constrained by 3onedata commercial contracts and clauses. The whole or part product, service or features described in this document may beyond purchasing or using range. 3onedata won't make any statement or warranty for this document content unless any other appointment exists.

Due to product version upgrading or other reason, this document content will be upgraded periodically. Unless other appointment exists, this document only for usage guide, all statement, information and suggestion in this document won't constitute any warranty.


## 3onedata Co., Ltd.


| | |
|---|---|
| Headquarter address: | 3/B, Zone 1, Baiwangxin High Technology Industrial Park, Song Bai Road, Nanshan District, Shenzhen, 518108, China |
| Technology support: | tech-support@3onedata.com |
| Service hotline: | +86 -880-4496 |
| E-mail: | sales@3onedata.com |
| Fax: | +86-0755-26703485 |
| Website: | http://www.3onedata.com |

# Preface

Switch CLI user manual has introduced:

- CLI configuration interface login
- CLI configuration rule and method
- Network management functions related CLI introduction

## Audience

This manual applies to the following engineers:

- Network administrators
- Technical support engineers
- Network engineer

## Text Format Convention

| Format | Description |
|---|---|
| " " | Words with “” represent the interface words. Such as: “Port No.”. |
| > | Multi-level path is separated by ">". For example, open local connection path description: open "Control Panel > Network Connection > Local Connection". |
| Light Blue Font | It represents the words clicked to achieve hyperlink. Font color as: "Light blue". |
| About this chapter | The section ‘about this chapter’ provide links to various sections of this chapter, as well as links to the Principles Operations Section of this chapter. |

## Symbols

| Format | Description |
|---|---|
| Notes | Remind the announcements in the operation, improper operation may result in data loss or equipment damage. |
|  Warning | Pay attention to the notes on the mark, improper operation may cause personal injury. |
|  Notes | Make a necessary supplementary instruction for operation description. |
|  Key | Configuration, operation, or tips for device usage. |
|  Tips | Pay attention to the operation or information to ensure success device configuration or normal working. |

## Port Convention

The port number in this manual is only an example, and does not represent the actual port with this number on the device. In actual use, the port number existing on the device shall prevail.

## Revision Record

| Version No. | Date | Revision Description |
|---|---|---|
| 01 | 06/14/2022 | Product release |

# Contents

PREFACE ..... 1
CONTENTS ..... I
1 QUICK START ..... 1
1.1 LOGIN TO THE SWITCH VIA CONSOLE PORT ..... 1
1.2 LOG IN AND RESET CONFIGURATION TO FACTORY DEFAULT ..... 3
1.3 SSH ..... 4
1.4 SET DEVICE HOSTNAME AND ADMIN USER PASSWORD ..... 4
1.5 SET VLAN 1 IP ADDRESS ..... 5
1.6 SET STATIC ARP ..... 6
1.7 DISPLAY AND SAVE CONFIGURATION TO FLASH ..... 7
2 ICLI BASICS ..... 10
2.1 COMMAND STRUCTURE AND SYNTAX ..... 10
2.2 NAME ETHERNET PORT ..... 13
2.3 USING THE KEYBOARD ..... 14
2.4 FILTERING OUTPUT ..... 18
2.5 UNDERSTANDING MODES AND SUB-MODES ..... 20
2.6 UNDERSTAND PRIVILEGE LEVEL ..... 23
2.7 UNDERSTANDING TERMINAL PARAMETERS ..... 25
3 CONFIGURE SYSTEM ..... 30
3.1 CONFIGURATION INSTANCE ..... 30
3.2 RESETTING OR REMOVING CONFIGURATION WITH "NO" ..... 32
4 MANAGE USERS ..... 34
4.1 ADD, MODIFY AND DELETE USER ..... 34
4.2 CONFIGURING PRIVILEGE LEVEL ..... 35
4.3 VIEW USER ..... 36
5 USING SHOW COMMANDS ..... 37
5.1 LISTS ALL SHOW COMMANDS ..... 37
5.2 USE CONTEXT-SENSITIVE HELP TO SEARCH ..... 39
5.3 DISPLAY RUNNING-CONFIG ..... 40
6 WORKING WITH CONFIGURATION FILES ..... 45
6.1 REVERTING TO DEFAULT CONFIGURATION ..... 45
6.2 USE CONFIGURATION FILES ..... 46
6.3 USING RELOAD COMMANDS ..... 47
6.4 WORKING WITH SOFTWARE IMAGES ..... 48

**7 SYSTEM ..... 50**
7.1 SYSTEM INFORMATION ..... 50
7.2 IP ..... 51
7.2.1 IP Configuration ..... 51
7.2.2 IP Status Monitoring ..... 52
7.3 NTP ..... 53
7.4 TIME ZONE ..... 54
7.5 LOG ..... 54
7.5.1 Configure Log ..... 54
7.5.2 Check Alarm Log ..... 55
7.6 温度保护 ..... 错误!未定义书签。
**8 PORT ..... 57**
8.1 PORT CONFIGURATION ..... 57
8.2 DDMI ..... 60
8.3 RELAY ALARM ..... 61
8.3.1 View Relay Status ..... 61
8.3.2 Configure Relay ..... 61
**9 SNMP ..... 63**
9.1 NAVIGATING THE SNMP CONFIGURATION ..... 63
9.2 CONFIGURE SNMP ..... 64
**10 RMON ..... 68**
10.1 STATISTICS CONFIGURATION ..... 68
10.2 HISTORY CONFIGURATION ..... 68
10.3 ALARM CONFIGURATION ..... 68
10.4 LINK EVENT CONFIGURATION ..... 69
10.5 STATISTICS MONITORING ..... 69
10.6 HISTORY MONITORING ..... 69
10.7 ALARM MONITORING ..... 69
10.8 EVENT MONITORING ..... 70
**11 ETHERNET SERVICES ..... 71**
11.1 PORT CONFIGURATION ..... 71
11.2 L2CP CONFIGURATION ..... 71
11.3 BANDWIDTH LIMITATION SUBSET ..... 71
11.4 EVCS CONFIGURATION ..... 72
11.5 ECES CONFIGURATION ..... 72
11.6 EVC STATISTICS MONITORING ..... 73
**12 CONFIGURE STATIC ROUTING ..... 75**
**13 LAYER 2 PROTOCOL CONFIGURATION ..... 77**
13.1 LINK AGGREGATION ..... 77
13.2 LACP ..... 78
13.3 MAC ADDRESS TABLE ..... 80
13.4 VLAN ..... 81
13.4.1 Port Based Configuration ..... 83

13.4.2 Configure MAC-based /Protocol based /IP Subnet-based VLAN ..... 88
13.5 PORT MIRRORING ..... 90
13.6 MULTIPLE SPANNING TREE PROTOCOL ..... 90
13.7 LLDP CONFIGURATION ..... 98
13.7.1 LLDP, LLDP-MED, and CDP ..... 99
13.7.2 LLDP Operation and Configuration ..... 99
13.7.3 LLDP-MED Operation and Configuration ..... 103
13.7.4 CDP Operation and Configuration ..... 111
13.7.5 Topology Example ..... 114
13.8 RING ..... 115
13.9 LOOP PROTECTION ..... 116
13.10 DHCP SERVER ..... 118
13.11 DHCP SNOOPING ..... 119
13.12 DHCP RELAY ..... 120
**14 ETHERNET RING PROTECTION SWITCHING CONFIGURATION ..... 122**
14.1 INTRODUCTION ..... 122
14.2 CONFIGURING ERPS FROM THE ICLI ..... 122
**15 CONFIGURING THE NETWORK ACCESS SERVER AND ACCESS CONTROL LIST ..... 126**
15.1 ACCESS CONTROL LIST ..... 126
15.2 NETWORK ACCESS SERVER ..... 129
**16 QOS CONFIGURATION ..... 136**
16.1 UNDERSTANDING QOS ..... 136
16.2 QOS CONFIGURATION EXAMPLES ..... 138
**17 CONFIGURE THE DHCP CLIENT ..... 148**
17.1 DHCP CLIENT ..... 148
**18 IP MULTICAST CONFIGURATION ..... 153**
18.1 IGMP/MLD SNOOPING ..... 153
18.2 IGMP/MLD PROXY ..... 154
18.3 IPMC PROFILE ..... 154
18.4 IPMC TRAFFIC FORWARDING ..... 154
18.5 IGMP/MLD SNOOPING OPERATION AND CONFIGURATION ..... 155
18.6 IGMP/MLD PROXY OPERATION AND CONFIGURATION ..... 163
18.7 IPMC PROFILE OPERATION AND CONFIGURATION ..... 166
18.8 IGMP/MLD UTILITY OPERATION AND CONFIGURATION ..... 172
18.9 IPMC CONFIGURATION EXAMPLES ..... 174
**19 HTTPS SETTING ..... 184**
19.1 UNDERSTANDING HTTPS ..... 184
19.2 CONFIGURATION PREREQUISITES ..... 185
19.3 CONFIGURING HTTPS ..... 185
**20 APPENDIX ONE: SAFETY REINFORCEMENT CONFIGURATION ..... 188**
20.1 STORM SUPPRESSION ..... 188
20.2 RATE LIMIT OF REPORTED CPU MESSAGE ..... 189
20.3 ISOLATE THE MANAGEMENT PLANE FROM THE USER PLANE ..... 190

20.4 SNMP ..... 191
20.5 LOGIN TO SWITCH VIA WEB NETWORK MANAGEMENT ..... 192

# 1 Quick Start

This document describes basic usage and configuration of the Industrial Command Line Interface (ICLI). The ICLI is a comprehensive management interface to the device. It is the only management interface accessible on the serial console; even without network connectivity, the device can be managed using a serial connection.

This section describes how to perform the following:

- Log in and reset configuration to factory defaults
- Set device hostname and admin user password
- Set VLAN 1 IP Address
- Verify connectivity using 'ping'
- Display the current configuration and save it to flash storage

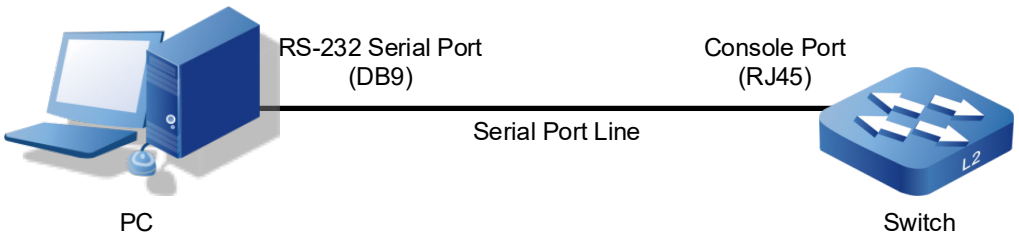
The following assumes the device is powered on and has a functional connection to a computer using the serial console port on the device (115200 baud, no parity, 8 data bits, 1 stop bit, no flow control).

The computer must run terminal emulator, such as TeraTerm or PuTTY on Windows, or Minicom on Linux.

## 1.1 Login to the Switch via Console Port

The PC can log in to the command line interface of the device by connecting to the Console port of the device.

Step 1 Connect the serial port of the computer to the Console port of the device through the serial port line to establish a local configuration environment, as shown in the topology diagram below.

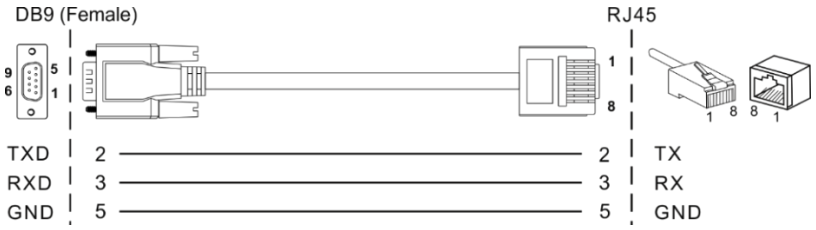



1. Connect DB9 at one end of serial port line to RS-232 serial port of PC.
2. Connect the RJ45 on the other end of the serial line to the Console port of the

device.

Note:

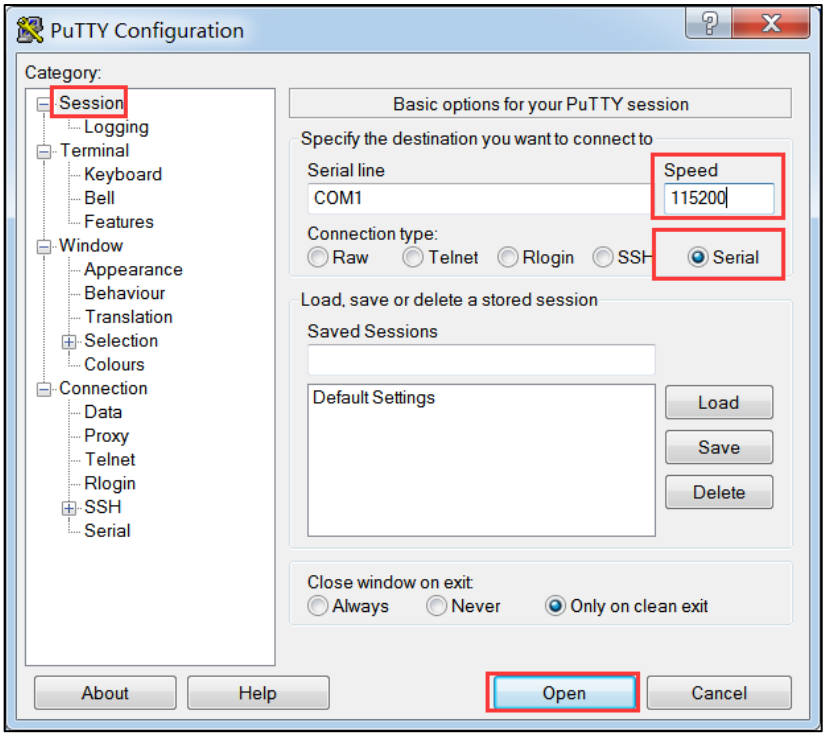
Diagram of internal connection line of serial port line/communication cable is shown below.




Step 2 Open the terminal simulation software on the PC, create a new connection, and set the interface and communication parameters of the connection. (Using PuTTY as an example here.)

1. Open PuTTY and click “Session” on the menu bar.
2. In the "Basic options for your PuTTY session" input box on the right, do the following:

- Select "Connection type" to "Serial".
- Enter "115200" in the "Speed" text box;
- Click “Open”.




Step 3 The "COM1-PuTTY" command line edit dialog box pops up. Press enter key to enter user name and password. The user name and password of the device are both admin by default, as shown below.

Step 4 End.

## 1.2 Log in and Reset Configuration to Factory Default

Notice

To ensure the safety of device and network, please keep the password properly and modify it regularly.

After using the device or system initialization for the first time, you need to use the default user name to log in to the CLI configuration interface through the CONSOLE port, and the WEB HTTP service will automatically start after logging in. The default user name and password are “admin”. Press Enter one or more times until the Username: prompt appears. Type admin and press Enter. At the Password: prompt type admin and press Enter.

After all users or new users successfully log in to the device for the first time, they need to modify the initial password. After the password is set successfully, you will be prompted to re-login, and the prompt' #' will be displayed after successful login. At last, enter "copy running-config startup-config" to save the password configuration.

Notes

The length of the password string must be greater than or equal to 8 and be composed of two or more of uppercase letters, lowercase letters, numbers and special characters.

```
Press ENTER to get started


Username: admin
Password:



First Login (please change the administrator account password)


Password:
Password (again):


Password changed successfully!
Press ENTER to get started
```

```
Username: admin
Password:
# copy running-config startup-config
Building configuration...
% Saving 4759 bytes to flash:startup-config
#
```

At this point, the admin user is operating at the highest privilege level, level 15. This means full control over the device and its configuration, and it is therefore possible to reset the configuration to factory defaults. Type reload defaults and press Enter. When the prompt

returns, the system has reverted to factory defaults as follows.

```
# reload defaults
% Reloading defaults. Please stand by.
#
```

## 1.3 SSH

SSH is enabled by default. You can use the following command to disable SSH.

```
# configure terminal
(config)# no ip ssh
```

After SSH is disabled, you will not be able to log in to the CLI configuration interface through the network port.

Use the following command to enable SSH.

```
# configure terminal
(config)#ip ssh
```

## 1.4 Set Device Hostname and Admin User Password

The ICLI has several different modes. The current mode is called exec mode; it allows the user to perform operations related to configuration files, reloading defaults, displaying system information, etc., but it does not allow the user to change detailed configuration items. Such operations are performed in the config mode.

To set the device hostname, first change to configuration mode by typing configuration terminal and pressing Enter, then type hostname mydevice and press

Enter, where mydevice is the appropriate name for the device. Finally, type exit and press Enter. Finally, type exit and press Enter.

```
# configure terminal
(config)# hostname mydevice
mydevice(config)# exit
mydevice#
```

The commands are executed immediately, so hostname changes the device hostname right

away.

The command for modifying the user password of current administrator is as follows.

```
mydevice# configure terminal
mydevice(config)# username admin privilege 15 password unencrypted very-secret
mydevice(config)# exit
mydevice#
```

The user, admin, now has the password “very-secret.” Other users can be added in similar fashion.

## 1.5 Set VLAN 1 IP Address

The objective is to assign an IP address to the device on VLAN 1. This is often sufficient for small local area networks that use Dynamic Host Configuration Protocol (DHCP) or static IP address allocation.

The system implements a DHCP client that, once enabled, will send out requests for IP address configuration. Those requests are received by a DHCP server on the network (if it exists and was appropriately configured). The server will then search through its pool of available IP addresses, allocate one, and return it to the DHCP client. The returned information typically includes IP address, netmask, and default gateway, but may also contain other information such as Domain Name Service (DNS) server addresses.

This configuration is similar to that of setting the host name: enter configuration mode, enter and execute configuration commands, and exit configuration mode. The following commands instruct the device to use DHCP to obtain an IP address, or, if DHCP fails, to use a static fallback address. Inclusion of a fallback IP is optional and may be omitted.

```
mydevice# configure terminal
mydevice(config)# interface vlan 1
mydevice(config-if-vlan)# ip address dhcp fallback 172.16.1.2 255.255.0.0
mydevice(config-if-vlan)# exit
```

```
mydevice(config)#
```

Notice how the prompt changes; the interface vlan 1 command enters a configuration sub-mode that allows, among other things, configuration of IP address.

Also note that IP addresses can only be assigned to VLAN interfaces.

After configuration is complete, the resulting IP address can be inspected. As seen below, the DHCP negotiation succeeded and the device obtained an address:

```
mydevice# show ip interface brief
Vlan        Address           Method           Status
-------     ---------         ------------     ----------
1           172.16.1.17/16    DHCP             UP
mydevice#
```

**`show ip interface brief`** displays all configured and active IP interfaces. The status should be UP. If it isn't, then the reason could be that there is no link on any port.

If DHCP negotiation fails, allocate the backup IP 172.16.1.2/255.255.0.0.

Now the most basic system configuration is complete. Management connectivity can be verified by issuing a **`ping`** command to a well-known external IP address:

```
mydevice# ping ip 172.16.1.1
PING server 172.16.1.1, 56 bytes of data.
64 bytes from 172.16.1.1: icmp_seq=0, time=0ms
64 bytes from 172.16.1.1: icmp_seq=1, time=0ms
64 bytes from 172.16.1.1: icmp_seq=2, time=0ms
64 bytes from 172.16.1.1: icmp_seq=3, time=0ms
64 bytes from 172.16.1.1: icmp_seq=4, time=0ms
Sent 5 packets, received 5 OK, 0 bad
mydevice#
```

If the Ping is successful, now you can login to the address 172.16.1.17 (or 172.16.1.2) on the VLAN1 interface via telnet or ssh.

## 1.6 Set Static ARP

The command to set static ARP is:

**`ip arp`** `<v_ipv4_abc> <v_mac_addr>`

CLI example: set the static ARP to 192.168.1.253 and the MAC address to 00:10:00:00:01:01.

```
# configure terminal
(config)# ip arp 192.168.1.253 00:10:00:00:01:01
```

CLI example: delete static ARP.

```
(config)# no ip arp 192.168.1.253
```

## 1.7 Display and Save Configuration to Flash

The current configuration of the device can be displayed in the form of a virtual file containing the full set of commands necessary to create an identical configuration. A few exceptions exist because certain items are not displayed, such as private SSH keys. This file is called running-config and is volatile by nature; it does not survive across reboots. It is therefore necessary to save the file to flash storage under the name startup-config, as this file is read and executed upon every boot and is therefore responsible for restoring the running configuration of the system to the state it had when the save took place.

The command show running-config will display the configuration settings as seen below. For brevity, some details were edited out. In addition, the set of interfaces is dependent on hardware capabilities.

```
# show running-config

Building configuration...

RSA                privatekey                set                27
wd3gqeUx5cBnT6kGOshVOFTk23h45O87N71tJKpYLw==

[...]RSA              privatekey              set              26
S8Rm+cLPYn+oHqkY6mR5Z6HU6Q9yqduOPv4+1w0=

username     admin     privilege     15     password     encrypted
k56kc1Il+61jrPPS3NOjdACwJkB6X6bo5mrb+xIRLQlR5vvqOLdmz8PaFDMHOP
av5uNBAShOE4Jz73Tg3JY00pny9kENLOALhLHbYcFfCPx+fFrOG8tNkNFpxcCH
kYmvR2oL0bwcy/7e+/6fxkUUi51L04T8Np4NDQXKeRrI1d7knx228nWhVrBhz8
79xeOU4tzpq1a0
8Unb7r12id/QIAlBspGpR/DNcYYvWnaFsUieO2yjRXnAntfpXbEy5jvKUybzuG
OxucBLLG1lZ338tkKlRXgpMuFZ6xRCAY02hGOT/HTR1XhgLGMnnXJCj8ywrAkl
3wEinksYLucft0mSew==

!

vlan 1

!

spanning-tree mst name Default revision 0

!

poe management mode class-reserved-power

poe supply 360

!

interface GigabitEthernet 1/1

 poe power limit 30.0

 no spanning-tree

! [...]
```

```
interface 2.5GigabitEthernet 1/10
 poe power limit 30.0
 no spanning-tree
!
interface vlan 1
 ip address 192.168.1.254 255.255.255.0
!
mep os-tlv oui 0xC sub-type 0x1 value 0x2
!
spanning-tree aggregation
 no spanning-tree
 spanning-tree link-type point-to-point
!
!
line console 0
!
line vty 0
! [...]
line vty 15
!
!
end
#
```

Lines that begin with ‘ ’ are comments. The file begins with the **hostname** command and the password for the admin user, followed by VLAN 1 and other items, such as Spanning Tree Protocol (STP). A list of all port interfaces on the device, ordered by switch ID, type, and port number comes next.

All port interfaces are at default settings, so nothing is displayed for them. As a general rule, only non-default configuration is displayed, otherwise the output would be huge and readability would suffer. There are a few exceptions that will be discussed later.

Following the physical interfaces are VLAN interface1. Only the former has an IP address assigned. Finally, the line section is shown. It specifies characteristics for the serial console (line console 0) or network ICLI management connections (line vty x).

The configuration shown above is also saved in startup-config.

```
mydevice# copy running-config startup-config
Building configuration...
% Saving 4759 bytes to flash:startup-config
```

```
mydevice # dir
Directory of flash:
   r- 1970-01-01 00:00:00     292 default-config
   rw 1970-01-01 00:01:53    4759 startup-config
2 files, 5051 bytes total.
mydevice# more flash:startup-config
RSA                privatekey                set                27
wd3gqeUx5cBnT6kGOshVOFTk23h45O87N71tJKpYLw==
[...]
```

The dir command lists the files in the flash file system while more outputs the contents of the designated file.

The skills exercised in this section form the basis for all day-to-day work with the ICLI on the device: logging in, displaying information with the show command, working with configuration files (**`show running-config`**, **`copy`**, **`dir`**, **`more`**), working with the actual configuration (**`configure terminal`**, **`exit`**), and sub-modes (**`interface ...`**).

The configuration proceeds in the same manner as setting the hostname: Enter configuration mode, enter and execute configuration commands, and exit configuration mode. The following commands instruct the device to use DHCP to obtain an IP address, or, if DHCP fails, to use a static fallback address. Inclusion of a fallback IP is optional and may be omitted.

# 2 ICLI Basics

The following list shows the key ICLI characteristics:

- It is modal (certain operations are possible or impossible in specific modes)
- It is line-based (there are no screen editing features)
- It executes commands instantly upon end-of-line
- It is privilege-based (certain operations require the user to have a certain privilege level to succeed)
- It implements industrial de-facto behavior for network equipment CLIs (structurally and behaviorally, it resembles CLIs found on other equipment while still possessing unique characteristics in some areas)

The ICLI can be accessed directly using the console port, or over the network through telnet or ssh. In each case, the user has to log in before ICLI commands can be executed. This begins a session that lasts until logout.

Multiple sessions can co-exist at the same time, each providing separate environments: logged-in user ID, privilege level, command history, mode, and session settings. It is therefore perfectly possible for the same user to control several concurrent sessions, such as one serial console session and one ssh session.

The user database is either local or provided by a RADIUS or TACACS+ server. If it is a local user database, password and privilege level will be maintained on the device.

## 2.1 Command Structure and Syntax

A command is a single line of text consisting of keywords and parameters, for example:

```
mydevice# show vlan id 10
...
mydevice# show vlan id 20
...
```

The keywords are show, vlan, and id; whereas 10 and 20 are parameters, something that could contain another value in another command invocation.

Keywords are not case sensitive, thus show, SHOW, and Show are identical. Conversely, parameters may either be case-sensitive or not, depending on the command and parameter in question.

Keywords and certain parameters can be abbreviated as long as they are unambiguous. For example, these commands are identical:

```
mydevice# show interface GigabitEthernet 1/5 capabilities
...
mydevice# sh in g 1/5 c
...
```

This works because:

- There are many keywords that begin with ‘s’ but only one that begins with ‘sh’
- There are several commands that begin with ‘show i’ but only one that begins with ‘show in’
- The **`show interface`** command takes a port type as parameter. According to the hardware function, the options are: FastEthernet, GigabitEthernet, 2.5GigabitEthernet, 5GigabitEthernet and 10GigabitEthernet. Thus, ‘g’ is a unique abbreviation for GigabitEthernet
- 1/5 identifies the interface as belonging to switch 1, port 5. This parameter cannot be abbreviated and has to be written out in full.
- The show interface GigabitEthernet 1/5 command can output different kinds of information: function, statistics, status and other information. In this case, ‘c’ is a unique abbreviation for capabilities

With a bit of practice, this allows for highly efficient keyboard entry, in particular when coupled with the context-sensitive help features of the ICLI (see Context-Sensitive Help).

## Syntax

A command is described by its syntax, for example:

```
show interface list { status | statistics | capabilities |
switchport | veriphy }
```

and

```
show erps [ detail | statistics ]
```

The semantics are:

- keywords are written in bold.
- parameters are written in italics.
- [ ... ] indicates an optional construct: It may or may not be present.
- { ... } indicates a grouping; the constructs within belong together
- ‘|’ indicates a choice between two or more alternatives, (example, a | b | c which reads as “a or b or c”).

Thus, the first command syntax is simple: First `show`, then `interface`, then a list of interfaces, then exactly one of `status`, `statistics`, `capabilities`, `switchport`, and veriphy.

The second command is a bit more complex: `show` and `erps` are mandatory, but the remaining parameters and keywords are optional: The user may enter group IDs; the user may enter either ‘statistics’ or ‘detail’. For example:

- Show short-form ERPS (Ethernet Ring Protection Switching) information for all instances:

```
mydevice# show erps
...
```

- Show statistics for all instances:

```
mydevice# show erps statistics
...
```

- Show details for all instances:

```
mydevice# show erps detail
...
```

- But it is not allowed to show details and statistics at the same time:

```
mydevice# show erps detail statistics
^
% Invalid word detected at '^' marker.
```

- Show details for specific set of instances:

```
mydevice# show erps 1-6 detail
...
```

There are some slightly more complex features of the syntax that center around sequences of optional items such as [a] [b] [c].

- Each of a, b, c may or may not be present (“a c” is valid, as is no input)
- Order is not important (“a c” and “c a” are equivalent)
- Each optional item can be present exactly no times or one time (not repeated)

There are variations:

- Group of options, of which at least one must be present: { [a] [b] [c] }*1
- Group of options, where one or more has fixed position: [a] {[b]} [c]
- This says that ‘b’ is optional, but if it is present then it must follow after ‘a’ (if ‘a’ is present) and it must come before ‘c’ (if ‘c’ is present)

For example, assuming a command with this syntax:

```
a [b] [c] { d | e } {[f] [g]}*1
```

then valid input examples are:

- ‘a d f’, because ‘b’ and ‘c’ are optional, ‘d’ is picked instead of ‘e’, and ‘f’ is chosen as the mandatory optional
- ‘a d f g’, because ‘b’ and ‘c’ are optional, ‘d’ is picked instead of ‘e’, and both ‘f’ and ‘g’ are chosen in the final group of optional
- ‘a c b e g’, because the ‘b’ optional is omitted, ‘e’ is picked instead of ‘d’, and ‘g’ is chosen for the mandatory optional

## 2.2 Name Ethernet Port

An Ethernet interface, or port, is identified by three pieces of information:

- The type (FastEthernet, GigabitEthernet, 2.5GigabitEthernet, 5GigabitEthernet, 10GigabitEthernet)
- The switch it belongs to (for non-stacking systems, this value is always 1)
- The port number within the type and switch (numbering starts with 1 for each type, so a switch may have both GigabitEthernet 1/1 and 2.5GigabitEthernet 1/1)

Many ICLI commands accept a list of interfaces. In its simplest form, such a list is a sequence of (type, switch ID, port) information separated by whitespace. For example: GigabitEthernet 1/3 10GigabitEthernet 1/2. This allows a single list to mix different types.

The switch ID and the port numbers can be listed either as single numbers, as lists, or as sequences. A list is a comma-separated set of single port numbers or sequences, whereas a sequence is of the form: from—to.

Some examples:

- GigabitEthernet 1/5 for the single gigabit port number 5 on switch 1
- GigabitEthernet 1/2,4,10-12 for gigabit ports 2, 4, 10, 11, 12 on switch 1
- GigabitEthernet 1-3/2 for gigabit port 2 on switches 1, 2 and 3

It is possible to wildcard the type and/or switch ID and/or ports to mean “all types,” “all switch IDs,” and “all ports,” respectively. A wildcard is written with an asterisk instead of type, switch ID, or port, and some further abbreviations are possible:

- “*” means “ports of all types of all switches”
- Type “*” means “all ports of specified types of all switches”

For clarity, here are some examples. Assume a stack with two switches, switch ID 1 and 3. Each switch has 9 gigabit ports and two 2.5 gigabit ports. Then:

- interface * (or: interface * * *)
  All ports of all types on all switches: GigabitEthernet 1,3/1-9 2.5GigabitEthernet 1,3/1-2
- interface * 1/2
  Switch 1, port number 2 of all types: GigabitEthernet 1/2 2.5GigabitEthernet 1/2
- interface * */2
  All switches, all types, port number 2: GigabitEthernet 1,3/2 2.5GigabitEthernet 1,3/2
- interface * */4
  All switches, all types, port number 4: GigabitEthernet 1,3/4

There are no 2.5 gigabit ports in the result.

- interface GigabitEthernet 3/*
  Switch 3, all gigabit ports: GigabitEthernet 3/1-9
- interface 2.5GigabitEthernet * (or: interface 2.5GigabitEthernet */*)
  All 2.5 gigabit ports on all switches: 2.5GigabitEthernet 1,3/1-2

Wildcards will include the largest possible set of ports, but may output an error message if a specific switch ID or port number doesn’t exist.

For example, these sets are invalid:

- interface * 2/*
  All ports of all types on switch 2 – which isn't a member of the stack
- interface * */100
  There is no port 100 of any type on any switch
- interface GigabitEthernet */* 2.5GigabitEthernet 2/*
  Again, switch 2 doesn't exist so the entire set is considered invalid

Validity is determined per set of (type, switch ID, port) containing wildcards: the result for that set is valid if there is at least one port that matches the set. A list of sets is valid if all sets match at least one port each.

## 2.3 Using the Keyboard

The ICLI provides a rich set of keys to assist the user while working with the command line. The functionality is divided into:

- Basic line editing
- Command history
- Context-sensitive help
- Long lines and pagination

### Basic Line Editing

Basic line editing allows the input of characters to form a command line, while also allowing cursor movement and insertion/deletion of characters and words. The following table shows the available editing functions and keys.

Table1 • key of basic line editing

| Key | Operation |
|---|---|
| Left/Right | Move one character left/right |
| Home/Ctrl-A | Move to start of line |
| End/Ctrl-E | Move to end of line |
| Del/Ctrl-D | Delete character at cursor |
| Backspace/Ctrl-H | Delete character to the left of cursor |
| Ctrl-N | Delete the entire current line |
| Ctrl-U/Ctrl-X | Delete all characters to the left of the cursor |
| Ctrl-K | Delete all characters under the cursor and right |
| Ctrl-W | Delete from cursor to start of word on the left |
| TAB | Complete word at end-of-line |

## Command History

A session maintains a non-persistent command history of previously entered command lines. The history can be up to 32 lines long. Once full, a new line will push the oldest entry out.

Table 2 • Command History

| Key | Operation |
|---|---|
| Up/Ctrl-P | Previous line in command history |
| Down | Next line in command history |

The number of lines to keep in the history for the current session is configurable between 0 and 32, where 0 disables the history altogether.

```
mydevice# terminal history size 32
```

The current value is displayed as part of the output from `show terminal`:

```
mydevice# show terminal
Line is con 0.
* You are at this line now.
Alive from Console.
Default privileged level is 2.
Command line editing is enabled
Display EXEC banner is enabled.
Display Day banner is enabled.
Terminal width is 80.
length is 24.
history size is 32.
exec-timeout is 10 min 0 second.
Current session privilege is 15.
Elapsed time is 0 day 0 hour 6 min 20 sec.
Idle time is 0 day 0 hour 0 min 0 sec.
```

It is possible to list the history:

```
mydevice# show history
show running-config
copy running-config startup-config
dir
show history
mydevice#
```

The list begins with the oldest entry at top.

## Context-Sensitive Help

The ICLI implements several hundred commands ranging from the very simple to the very complex. It is therefore imperative that the user can be assisted in entering syntactically correct commands as well as discovering relevant commands. These objectives are supported by the context sensitive help features.

Table 3 • Context-Sensitive Help Key

| Key | Operation |
|---|---|
| ? | Show next possible input and description |
| ??/Ctrl-Q | Show syntax of possible command(s) |
| TAB | Show next possible input without description or expand current word if it is unambiguous |

The context-sensitive help only displays commands that are accessible at the current session privilege level (see Understanding Privilege Levels).

## Use Context-Sensitive Help

```
! Show possible next input for a command that begins with 'show
a':
 mydevice# show a?
     aaa           Authentication, Authorization and Accounting
methods
     access        Access management
     access-list    Access list
     aggregation    Aggregation port configuration
    alarmlog      System logging message
! The same, but without descriptions:
mydevice# show a<TAB>
aaa         access      access-list  aggregation  alarmlog
! If the user enters another 'g' the word 'aggregation' is the only
possibility:
mydevice# show ag?
aggregation    Aggregation port configuration
<cr>
! Pressing <TAB> now expands the word fully:
mydevice# show aggregation
```

```
! Possible next input is displayed with a press of '?': mydevice#
show aggregation ?

|    Output modifiers

mode Traffic distribution mode

<cr>

! The syntax is displayed with another press of '?': mydevice# show
aggregation ?

show aggregation [ mode ]

! This shows that there is an optional 'mode' word (square brackets
indicate an option).

! Repeated presses of '?' toggles display between next possible
input and syntax:

mydevice# show aggregation ?

|    Output modifiers

mode Traffic distribution mode

<cr>

mydevice# show aggregation ?

show aggregation [ mode ]

! Finally, the syntax display is also directly available with Ctrl-Q:
mydevice# show aggregation ^Q

show aggregation [ mode ]
```

## Long Lines and Pagination

A session has a configuration that indicates the width of the terminal in characters and the length in lines. It uses these parameters to control handling of long input lines and to control pagination of multi-line output. For details about changing these parameters, see UnderstandingTerminal Parameters.

Long lines come into play when a line is longer than the terminal width minus the prompt. In that case, part of the line will be hidden from display as indicated by '$' at the beginning and/or end of the visible part of the line.

For example:

```
mydevice# $there is text to the left of what is visible here
mydevice# there is text to the right of what is visible here$

mydevice# $there is text at both ends of what is visible here$
```

The first line has scrolled left; the second line has scrolled right; the third line has been scrolled to the middle of a quite long line.

Pagination appears each time execution of a command causes output of more lines than what has been configured as the terminal length. A typical example is the output from show running-config. After the first several lines have been output, the pagination prompt is presented:

```
! [lines of text]

-- more --, next page: Space, continue:  g, quit: ^C
```

The following keys control pagination:

Table 4 • Pagination Keys

| Key | Operation |
|---|---|
| Enter | Display next line of output |
| Space | Display next page of output |
| G | Display remainder of output without more pagination |
| Q/Ctrl-C | Display remainder of output |
| Any other key | Display next page of output. Certain terminal keys (arrows, Home, End, etc.) may appear as multiple characters to the ICLI, leading to multiple pages being output in quick succession. |

The terminal length (also sometimes called height) can be configured for the current session using the terminal length lines command. If lines = 0 is input, pagination is disabled.

```
mydevice# terminal length 0

mydevice# terminal length 25
```

The same is true for setting the terminal width in characters.

### Other Special Keys

One additional key is defined as a convenience. It allows the immediate return from any sub-mode to Exec mode.

Table 5 • Special Keys

| Key | Operation |
|---|---|
| Ctrl-Z | Return directly to Exec mode |

## 2.4 Filtering Output

The output from commands can be filtered in most cases. It is possible to limit the output to only those lines that match/trigger a specific substring. The available filtering is:

- Begin – display the first line that matches and all subsequent lines
- Include – display exactly those lines that match
- Exclude – display exactly those lines that do not match. The string is case-sensitive.

The syntax is:

```
command '|' { begin | include | exclude } string
! Execute a command that generates some output; no filtering initially:
mydevice# show users
Line is con 0.
* You are at this line now.
Connection is from Console. User name is admin.
Privilege is 15.
Elapsed time is 0 day 21 hour 52 min 50 sec.
Idle time is 0 day 0 hour 0 min 0 sec.
! Filter to include specific word:
mydevice# show users | include User name is admin.
! Exclude all lines that contain '0' (zero)
mydevice# show users | exclude 0
* You are at this line now.
Connection is from Console. User name is admin.
Privilege is 15.
! Begin output when specific word is matched:
mydevice# show users | begin Elapsed
Elapsed time is 0 day 21 hour 53 min 29 sec.
Idle time is 0 day 0 hour 0 min 0 sec.
```

## 2.5 Understanding Modes and Sub-Modes

The ICLI implements a number of modes that control the available command set. The modes are further influenced by the privilege level of the user; some modes or commands are only accessible to administrators while others require no privileges beyond login.

There are three major modes: Exec, Privileged Exec and Config. Under Config, there exist a number of sub-modes. The sub-modes allow configuration of specific VLANs, Ethernet interfaces, etc.

Table 6 • Modes

| Mode | Parent Mode | Note |
|---|---|---|
| Exec | | Lowest-privileged mode; used for basic system monitoring. Generally does not allow modifications to the system<br>Command: **disable**<br>Prompt: **hostname>** |
| Privileged Exec | Exec | Privileged mode; allows configuration and other modifications to the system<br>Command: **enable**<br>Prompt: **hostname#** |
| Config | Priv.Exec | Global configuration mode<br>Command: **configure terminal**<br>Prompt: **hostname(config)#** |
| VLAN Config | Config | Sub-mode for configuring active VLANs<br>Command: **vlan vlan_id_list**<br>Prompt: **hostname(config-vlan)#** |
| VLAN Interface Config | Config | Configure submode of VLAN interface<br>Command: **interface vlan vlan_id_list**<br>Prompt: **hostname(config-if-vlan)#** |
| Interface Config | Config | Sub-mode for configuring Ethernet interfaces<br>Command:**interface type switch_num/port_num**<br>Prompt: **hostname(config-if)#** |
| Line | Config | Sub-mode for configuring terminal lines<br>Command:**line { con \| vty } line_num**<br>Prompt: **hostname(config-line)#** |
| IPMC Profile Config | Config | Sub-mode for configuring IP Multicast profiles<br>Command: **ipmc profile profile_name**<br>Prompt:<br>**hostname(config-ipmc-profile)#** |

| Mode | Parent Mode | Note |
|---|---|---|
| SNMP Server Host Config | Config | Sub-mode for configuring SNMP server host entries<br>Command: **snmp-server host host_name**<br>Prompt: **hostname(config-snmps-host)#** |
| DHCP Pool Config | Config | Sub-mode for configuring DHCP client pools<br>Command:**ip dhcp pool pool_name**<br>Prompt: **hostname(config-dhcp-pool)#** |
| STP Aggregation Config | Config | Sub-mode for configuring Spanning Tree Protocol aggregation<br>Command: **spanning-tree aggregation**<br>Prompt: **hostname(config-stp-aggr)#** |
| JSON Notification Host Config | Config | Sub-mode for configuring JSON notification hosts<br>Command: **json notification host host_name**<br>Prompt:<br>**hostname(config-json-notif-host)#** |

It is possible for a user to transition between these modes using certain commands, subject to the user's privilege level and the current session privilege level (see Understanding Privilege Levels.).

The initial mode is determined by the privilege level of the logged-in user. If the privilege level is 0 or 1, the user is unprivileged and begins in the (Unprivileged) Exec mode. If the privilege level is higher, the session begins in Privileged Exec mode.

A user can raise the Exec mode privilege level to a higher value if an enable password has been configured for that level. This elevation is done with the enable level command, where level is a value between 1 and 15. The reverse operation (lowering the privilege level) is achieved with the disable command.

Once in Privileged Exec mode, it is possible to enter into the global configuration mode by entering the command configure terminal. Exit from global configuration is achieved by typing end or exit and then pressing Enter or pressing Ctrl-Z.

Access to a configuration sub-mode (for example, Ethernet interfaces) goes through global configuration or another sub-mode. Thus, it is possible to change directly from VLAN sub-mode to Ethernet interface sub-mode, for instance.

Thus, each mode and sub-mode implements a scope for commands. Inside each mode, a particular subset of commands is available. To get to other commands, one must generally change mode/sub-mode. This is necessary because there are commands with identical prefixes in different modes. For example, there are commands that begin with 'ip' in Privileged Exec, global configuration, and VLAN Interface Configuration modes.

There are two exceptions to this:

While in a configuration sub-mode, access to global configuration mode commands is possible as long as there is no ambiguity. Execution of a global configuration command exits the sub-mode.

Exec mode commands (whether privileged or unprivileged) are accessible from within global configuration or one of the sub-modes by using the do command.

The do command takes an arbitrary command line from Exec and executes it. In the following example, the user wants to change the IP address on the VLAN 1 interface and uses do to verify the current address while in the sub-mode.

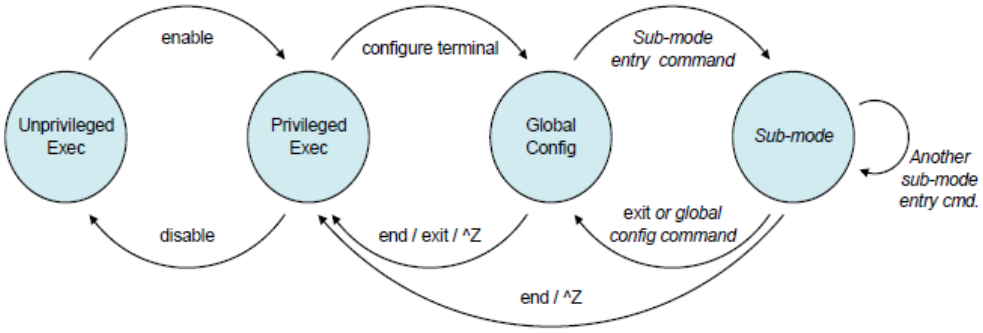
## Using ‘do’ While in a Sub-Mode

```
mydevice# configure terminal
mydevice(config)# interface vlan 1
mydevice(config-if-vlan)# do show ip interface brief
Interface       Address            Method   Status
--------------- ------------------- -------- ------
VLAN 1          192.168.1.254/24    Manual   UP mydevice
(config-if-vlan)# end
! When in Exec, no ‘do’ prefix is needed:
mydevice# show ip interface brief
Vlan Address          Method   Status
1 172.16.1.15/24        DHCP    UP
```

## ICLI Mode Transitions

The following illustration shows the possible transitions between major modes and sub-modes, and some of the relevant commands.

Figure • ICLI Mode Transitions




## Changing Between ICLI Modes

```
! Initial mode for this example is Unprivileged Exec. Raise level
! (and change mode):
mydevice> enable
Password: *********
mydevice#
```

```
! Note how the prompt changed from '>' to '#' to indicate the
privileged exec mode


! Enter global configuration mode:
mydevice# configure terminal


! Now create VLAN 100 and give it a name. This enters the VLAN sub-mode,
as
! indicated by a new prompt:
mydevice(config)# vlan 100
mydevice(config-vlan)# name MyVlan


! Change directly from VLAN sub-mode into Ethernet interface
sub-mode for
! interface instance 4 on switch 1, and set link speed to 'auto'
mydevice(config-vlan)# interface GigabitEthernet 1/4
mydevice(config-if)# speed auto


! Then enter a command from the global configuration mode; this
leaves Ethernet interface sub-mode
mydevice(config-if)# hostname mydevice


! Exit global configuration mode and go back to Privileged Exec
mydevice(config)# end
! And use 'disable' to go back to Unprivileged Exec:
mydevice# disable
mydevice>
```

## 2.6 Understand Privilege Level

A privilege level is a number in the range of 0 to 15, inclusive, with 0 being the lowest. It is assigned to a user session and used to determine access to ICLI commands. Only commands at the same or lower privilege level can be accessed.

Each user on the device has a default privilege level that is copied to the session's privilege level at login. It is, however, possible for the user to change the session privilege level by executing the *enable* or *disable* commands. This can be used, for example, as follows:

- The user account is configured with privilege level 0

- Whenever the user needs to perform higher-privileged commands, the user changes session priority level, executes the necessary commands, and then reverts back to the default priority level

Access to higher priority levels must be password protected by using the *enable password* or *enable secret* global configuration commands. The main difference between the two is whether passwords are displayed in clear text or encrypted form in *running-config*, and consequently, *startup-config*.

Password input can also be in encrypted or clear text form. The latter is used when an operator inputs a new password, as the operator will usually not know the encrypted form of the password.

Input password is displayed in ciphertext. The admin user is at level 15 by default, the highest possible privilege level.

## Configure Privilege Level keyword

The following example configures a level 15 password using enable secret, inspects the resulting configuration, then removes it again.

```
mydevice# configure terminal

! A secret can either be input in clear text or encrypted form;
! a digit indicates which kind follows on the command line:
mydevice(config)# enable secret ?
0    Specifies an UNENCRYPTED password will follow
5    Specifies an ENCRYPTED secret will follow

! In this case: Unencrypted. Then follows either the level for
! which a password is being configured, or, if no level is given,
! the password for level 15:
mydevice(config)# enable secret 0 ?
<word32>    Password
level       Set exec level password

! Thus, the following two commands are semantically identical:
mydevice(config)# enable secret 0 my-secret
mydevice(config)# enable secret 0 level 15 my-secret

! The running configuration can be inspected to see the encrypted
form:
mydevice(config)# do show running-config | include enable
enable secret 5 level 15 D29441BF847EA2DD5442EA9B1E40D4ED
```

```
! To remove the password use the 'no' form (the two are semantically
equivalent for level 15):
mydevice(config)# no enable secret
mydevice(config)# no enable secret level 15
mydevice(config)# do show running-config | include enable
mydevice(config)#
```

## 2.7 Understanding Terminal Parameters

Each system login creates a session, whether through the serial console, telnet or ssh. The session is initialized with settings that are configurable from the line configuration sub-mode, but most of them can also be changed from Exec mode while the session is active. Such changes are not persistent, however, and are lost when the session is terminated.

The following table lists available settings and modes where each can be configured.

Table 7 • Setting and Modes

| Set | Mode | Description |
|---|---|---|
| editing | Exec, Line | Enable/disable command line scrolling |
| exec-banner | Line | Enable/disable display of the Exec banner (configured with 'banner exec ...') |
| exec-timeout | Exec, Line | Inactivity timer; automatically log out after a period of inactivity. A value of zero disables automatic logout |
| history | Exec, Line | Length of command history buffer |
| length | Exec, Line | Terminal length in lines, used for pagination. Zero disables pagination |
| location | Line | A line of text that describes the terminal location (such as "Server room") |
| motd-banner | Line | Enable/disable display of Message-Of-The-Day banner (configured with 'banner motd ...') |
| privilege | Line | Distribute default priority |
| width | Exec, Line | Terminal width in characters, used for pagination |

The following table lists available settings and modes where each can be configured.

The system allows one serial console session and up to 16 network sessions. The console session is called "console 0" whereas each network session is called "vty X" where vty is an abbreviation for Virtual TTY and X is a value between 0 and 15.

The configuration appears near the bottom of running-config and looks like this:

```
line console 0
exec-timeout 0
!
line vty 0
!
line vty 1
!
line vty 2
! [...]
```

It is possible to specify different settings for each vty, but this is generally not recommended since there is no way to associate an incoming ssh or telnet connection with a specific vty.

## Changing Terminal Parameters

```
This example shows how to change some values for the current session,
and for all future console sessions.
! First inspect current settings for this session:
mydevice# show terminal
Line is con 0.
* You are at this line now. Alive from Console.
Default privileged level is 2.
 Command line editing is enabled
Display EXEC banner is enabled.
Display Day banner is enabled.
Terminal width is 80.
length is 24.
history size is 32.
exec-timeout is 10 min 0 second.

Current session privilege is 15.
Elapsed time is 0 day 0 hour 15 min 42 sec.
Idle time is 0 day 0 hour 0 min 0 sec.

! Then set terminal length to zero to disable pagination, and
exec-timeout to zero to disable automatic logout:
mydevice# terminal length 0
mydevice# terminal exec-timeout 0
```

```
mydevice# show terminal
Line is con 0.
* You are at this line now.
Alive from Console.
Default privileged level is 2.
Command line editing is enabled
Display EXEC banner is enabled.
Display Day banner is enabled.
Terminal width is 80.
length is 0.
history size is 32.
exec-timeout is 0 min 0 second.

Current session privilege is 15.
Elapsed time is 0 day 0 hour 16 min 31 sec.
Idle time is 0 day 0 hour 0 min 0 sec.

! Then we do the same, but for all future console sessions.
! Note how the commands have no 'terminal' prefix ('terminal length'
vs. 'length'):
mydevice# configure terminal
mydevice(config)# line console 0
mydevice(config-line)# exec-timeout 0
mydevice(config-line)# length 0
mydevice(config-line)# end
! Finally save the configuration to startup-config to make it
persistent:
mydevice# copy running-config startup-config
Building configuration...
% Saving 1287 bytes to flash:startup-config
mydevice#
```

## Using Banners

The system provides three different banners (text that is output as messages to the user):

- The Message Of The Day banner (MOTD), displayed upon connection to the system or when a console login attempt has timed out

- The Login banner, displayed before the first “Username:” login prompt
- The Exec banner, displayed upon successful login

All of these banners are configured in a similar manner, using the `banner` command:

```
banner [ motd | login | exec ] <banner>
```

The banner text can be either a single line or multiple lines. The first character of the text defines a delimiter character; the actual text of the banner then follows and ends at the first appearance of the delimiter character. The delimiters are not included in the actual text.

## Configuring Banners

```
! First configure the MOTD banner, which in this case is multi-line. '*' is used as delimiter character, but any printable character that isn't used in the message is usable:

mydevice# configure terminal

mydevice(config)# banner motd * This is the Message Of The Day Banner.

It spans multiple lines.

And one more. But now it ends. *

! Enter TEXT message.   End with the character '*'.

! Then the Login and Exec banners. Both are single-line. Note how different delimiters are used in each banner:

mydevice(config)# banner login XThis is mydevice.X

mydevice(config)# banner exec "WARNING: Production system. Be careful."

mydevice(config)# end


! Inspect configuration:

mydevice# show running-config

Building configuration...

banner motd "This is the Message Of The Day Banner.

It spans multiple lines.

And one more. But now it ends."

banner exec "WARNING: Production system. Be careful."

banner login "This is mydevice."

hostname mydevice

! [...]

end


! Test it: Log out, then log in again:
```

```
mydevice# exit


This is the Message Of The Day Banner.
It spans multiple lines.
And one more. But now it ends.
Press ENTER to get started<ENTER>
This is mydevice.
Username: admin
Password:


WARNING: Production system. Be careful.
mydevice#


! Finally save the configuration to startup-config to make it
persistent:
mydevice# copy running-config startup-config
Building configuration...
% Saving 1461 bytes to flash:startup-config
mydevice#
```

# 3 Configure System

Changes to system configuration can only be made from the global configuration mode and its sub-modes, except when working with configuration files or reloading defaults. This is done in Privileged Exec mode. The following steps outline the sequence.

- Raise privilege level to 15.
- Enter global configure mode.
- Input appropriate configuration commands. Optionally, enter sub-modes and input appropriate commands there.
- Exit global configuration mode.
- Verify configuration.
- Save configuration to Flash.

## 3.1 Configuration Instance

In this example, the hostname and VLAN 1 IP address is configured, verified, and saved. This example assumes the session is initially unprivileged.

- Raise privilege level:

```
> enable
Password: ***
```

- Enter global configure mode:

```
# configure terminal
```

- Enter configuration command. The IP address is set from within the

```
! VLAN interface submode:
(config)# hostname mydevice
mydevice(config)# interface vlan 1
mydevice(config-if-vlan)# ip address dhcp fallback 172.16.1.2
255.255.0.0
mydevice(config-if-vlan)# exit
```

- Leave global configuration mode and go back to Privileged Exec:

```
mydevice(config)# end
```

- Inspect and verify the configuration (some output omitted for brevity):

```
mydevice# show running-config
Building configuration...
[...]
!
vlan 1
!
[...]
!
interface GigabitEthernet 1/1
poe power limit 30.0
 no spanning-tree
[...]
!
interface vlan 1
ip address dhcp fallback 172.16.1.2 255.255.0.0
!
[...]
end
! More verification: Display IP interfaces and assigned IP address
and status:
mydevice# show ip interface brief
Vlan Address      Method   Status
-----------------------------------
1 172.16.1.15/24   DHCP     UP
! An address was obtained from DHCP, so the fallback wasn't used
! Try to inspect hostname:
mydevice# show hostname
^
% Invalid word detected at '^' marker.
! No such command exists, but it is possible to extract a single
line from running-config by using a filter:
mydevice# show running-config | include hostname
hostname mydevice
#
```

- Save configuration to Flash:

```
mydevice# copy running-config startup-config
Building configuration...
% Saving 1272 bytes to flash:startup-config
```

# 3.2 Resetting or Removing Configuration with "no”

It is possible to remove specific configuration items or reset them to their default values. In general, almost each configuration command has a corresponding no form. The ‘no’ form is syntactically similar (but not necessarily identical) to the configuration command, but either resets the parameters to defaults for the configurable item being addressed or removes the item altogether.

In many cases, ‘’no’’ can be read as no(t) different from default settings.

## Using "no" Forms

The following list shows the tasks accomplished:

- Configure the VLAN 1 interface IP address to use DHCP
- Inspect the configuration
- Delete IP address of VLAN 1

‘’no’’ operations can be viewed as reset-to-default, with the defaults being no IP address.

```
mydevice# configure terminal
mydevice(config)# interface vlan 1
mydevice(config-if-vlan)# ip address dhcp
mydevice(config-if-vlan)# exit
(config)# end

mydevice# show ip interface brief
Interface       Address            Method   Status
--------------- ------------------- -------- ------
VLAN 1          192.168.1.254/24    DHCP     UP
mydevice# configure terminal
mydevice(config)# interface vlan 1
mydevice(config-if-vlan)# no ip address
mydevice(config-if-vlan)# end
mydevice# show ip interface brief
Interface       Address            Method   Status
--------------- ------------------- -------- ------
```

```
mydevice#
```

Note:
The syntax of the configuration commands and their ‘no’ forms are different; the ‘no’ forms usually do not take as many parameters.

This is usually convenient but may give surprising results in certain cases. For example, an OAM MEP instance can configure Continuity Check using ‘mep <num> cc <priority> ...’ and reset it with ‘no mep <num> cc’. However, because MEPs are removed using the command ‘no mep <num>’, it is possible to unintentionally remove an existing MEP by entering ‘no mep 10 ccc’ – the extra ‘c’ means that the last word isn’t recognized as ‘cc’, leading to a match of the MEP removal command instead of the desired reset-CC command.

# 4 Manage Users

The following describes local user management on the device. RADIUS and TACACS+ users management is beyond the scope of this document. It is possible to create several user accounts on a system. Each user account has a set of configurable attributes:

- User name
- Password
- Privilege Level

All attributes are configured with the same command, `username`.

```
username <username> privilege <priv> password encrypted <encry_password_1> [ <encry_password_2> ]

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

no username <username>
```

`No username` would delete the given user account.

## 4.1 Add, Modify and Delete User

The following example adds two user accounts at different privilege levels, inspects configuration, and deletes one account again using 'no username'.

```
! Display current set of local user accounts:

mydevice# show running-config | include username

username admin privilege 15 password encrypted [...]


! Add two accounts, 'operator' and 'monitor'. The passwords are supplied in unencrypted form:

mydevice# configure terminal

mydevice(config)# username operator privilege 10 password unencrypted a-secret
```

```
mydevice(config)# username monitor privilege 1 password
unencrypted new-secret


! Verify that the configuration is correct. Note that passwords
are displayed in encrypted form:
mydevice(config)# do show running-config | include username
username admin privilege 15 password encrypted [...]
username operator privilege 10 password encrypted [...]
username monitor privilege 1 password encrypted [...]


! Delete the 'operator' user and verify it is removed from the
configuration:
mydevice(config)# no username operator
mydevice(config)# do show running-config | include username
username admin privilege 15 password encrypted [...]
username monitor privilege 1 password encrypted [...]
```

## 4.2 Configuring Privilege Level

The privilege level of the user. The allowed range is 0 to 15. If the privilege level value is 15, it can access all groups, that is, that is granted the fully control of the device. But others value need to refer to each group privilege level. User's privilege should be same or greater than the group privilege level to have the access of that group. By default setting, most groups privilege level 5 has the read-only access and privilege level 10 has the read-write access. And the system maintenance (software upload, factory defaults, and so on) need user privilege level 15. Generally, the privilege level 15 can be used for an administrator account, privilege level 10 for a standard user account and privilege level 5 for a guest account.

```
web privilege group <group_name> level { [ configRoPriv
<configRoPriv> ] [ configRwPriv <configRwPriv> ] [ statusRoPriv
<statusRoPriv> ] [ statusRwPriv <statusRwPriv> ] }*1
```

CLI example: view the privilege level of Aggregation.

```
# show web privilege group Aggregation level
Group Name                    Privilege Level
                             CRO CRW SRO SRW
------------------------------ --- --- --- ---
Aggregation                     5  10   5  10
```

CLI example: set the read-only privilege of Aggregation configuration to 3 and the write privilege to 5; Set the read-only privilege of Aggregation status to 3 and the write privilege to 5.

```
# configure terminal
(config)# web privilege group Aggregation level configRoPriv 3
(config)# web privilege group Aggregation level configRwPriv 5
(config)# web privilege group Aggregation level statusRoPriv 3
(config)# web privilege group Aggregation level statusRwPriv 5
```

## 4.3 View User

```
show users [ myself ]
```

Commands for viewing all CLI online user information.

```
# show users
Line is con 0.
   * You are at this line now.
   Connection is from Console.
   User name is admin.
   Privilege is 15.
   Elapsed time is 0 day 0 hour 38 min 17 sec.
   Idle time is 0 day 0 hour 0 min 0 sec.

Line is vty 0.
   Connection is from 192.168.1.161:22462 by Telnet.
   User name is admin001.
   Privilege is 5.
   Elapsed time is 0 day 0 hour 0 min 3 sec.
   Idle time is 0 day 0 hour 0 min 3 sec.
```

Commands for viewing users' own information.

```
# show users myself
Line is con 0.
   * You are at this line now.
   Connection is from Console.
   User name is admin.
   Privilege is 15.
   Elapsed time is 0 day 0 hour 41 min 51 sec.
   Idle time is 0 day 0 hour 0 min 0 sec.
```

# 5 Using show Commands

The family of show commands is the cornerstone of ICLI-based system monitoring. Most features implement one or more show commands that will display a relevant mix of status and configuration.

Notes:
The exact set of available commands, parameters, and output format depends on the system configuration and software version, so some of the following commands and examples may not be applicable to all systems.

The show commands exist only in the two Exec modes and are subject to session privilege level enforcement. Therefore, listing the largest possible set of show commands requires the session to be at level 15.

## 5.1 Lists All show Commands

The following example raises the session privilege level to 15. In this example, an enable secret has been specified, so password entry is required to proceed. Then the user inputs show and uses the context-sensitive help feature to list the possible show commands, in this case for a Carrier Ethernet system.

```
Username: admin
Password:
# show ?
   aaa              Authentication, Authorization and Accounting
methods
   access           Access management
   access-list       Access list
   aggregation       Aggregation port configuration
```

```
    alarmlog          System logging message
    clock             Configure time-of-day clock
    dot1x             IEEE Standard for port-based Network Access
Control
    erps              Ethernet Ring Protection Switching
    evc               Ethernet Virtual Connections
    history           Display the session command history
    interface         Interface status and configuration
    io                Configure IO
    ip                  Interface Internet Protocol configuration
commands
    ipmc              IPv4/IPv6 multicast configuration
    ipv6              IPv6 configuration commands
    lacp              LACP configuration/status
    line              TTY line information
    lldp              Display LLDP neighbors information.
    loop-protect       Loop protection configuration
    mac               Mac Address Table information
    mep               Maintenance Entity Point
    ntp               Configure NTP
    platform          Platform configuration
    poe               Power Over Ethernet.
    port-security      Port Security status - Port Security is a
module with no
                     direct configuration.
    privilege         Display command privilege
    process           process
    qos               Quality of Service
    radius-server      RADIUS configuration
    relay             Configure relay alarm
    ring              Configure ring
    rmon              RMON statistics
    running-config     Show running system information
    scheduling        Scheduling infomation
    snmp              Display SNMP configurations
    sntp              Configure SNTP
```

```
  spanning-tree     STP Bridge
  stpstate          stp state
  switchport        Display switching mode characteristics
  system            system
  systemlog         System logging message
  tacacs-server     TACACS+ configuration
  terminal          Display terminal configuration parameters
  time              Display current system time
  users             Display information about terminal lines
  version           System hardware and software status
  vlan              VLAN status
  web               Web
  xsq               Configure XSQ
```

## 5.2 Use Context-Sensitive Help to Search

The context-sensitive help feature for syntax display is also useful for determining the exact command to execute. In the following example, the user discovers the proper command **show ip statistics system** through exploration:

```
# show ip ?
  arp
  dhcp          Dynamic Host Configuration Protocol
  domain        Default domain name
  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
  ssh           Secure Shell
  statistics    Traffic statistics
# show ip statistics ?
  |           Output modifiers
  icmp        IPv4 ICMP traffic
  icmp-msg    IPv4 ICMP traffic for designated message type
  interface   Select an interface to configure
```

```
system      IPv4 system traffic
<cr>


! A repeated press of '?' displays the syntax:
mydevice# show ip statistics ?
show ip statistics [ system ] [ interface vlan <v_vlan_list> ] [ icmp ]
[ icmp-msg <type> ]


mydevice# show ip statistics system
IPv4 statistics:


  Rcvd:  48 total in 27096 bytes
         24 local destination, 0 forwarding
         0 header error, 0 address error, 0 unknown protocol
         0 no route, 0 truncated, 0 discarded
  Sent:  48 total in 27096 bytes
         24 generated, 0 forwarded
         0 no route, 0 discarded
  Frags: 0 reassemble (0 reassembled, 0 couldn't reassemble)
         0 fragment (0 fragmented, 0 couldn't fragment)
         0 fragment created
  Mcast: 0 received in 0 byte
         0 sent in 0 byte
  Bcast: 0 received, 0 sent
```

## 5.3 Display running-config

The virtual file running-config consists of a list of commands that, taken together, result in the currently running system configuration.

This list of commands is usually not 100% identical to the list of commands a user has input to configure the device. That is because running-config is a textual representation of the system configuration that is stored in binary form in the RAM memory of the device.

Because the effective device configuration is huge, running-config in the majority of cases only lists the delta between default settings and current settings. This significantly reduces the amount of output and greatly improves readability of the configuration, but it does require the reader to know what the default settings are.

With **show running-config all-defaults**, it is possible to include values that are at default.

## Default vs. Non-default vs. All Defaults

In this example, if the speed and duplex settings of an Ethernet interface are at default values (auto-negotiation), then nothing will be output. If the user then changes the speed to be fixed at 1 Gbps, then that value is now non-default and will be output. Duplex is also output because it is forced to 'full' when the speed is fixed at 1 Gbps.

```
! Display current configuration for an interface. All settings are
at default:
mydevice# show running-config interface GigabitEthernet 1/4
Building configuration...
interface GigabitEthernet 1/4
poe power limit 30.0
no spanning-tree
!
end

! Now set the speed to 1Gbps and display the configuration again:
mydevice# configure terminal
mydevice(config)# interface GigabitEthernet 1/4
mydevice(config-if)# speed 1000
mydevice(config-if)# end

mydevice# show running-config interface GigabitEthernet 1/4
Building configuration...
interface GigabitEthernet 1/4
poe power limit 30.0
no spanning-tree
speed 1000
duplex full
!
end

! Include all default settings for that interface:
mydevice# show running-config interface GigabitEthernet 1/4
all-defaults
Building configuration...
```

```
interface GigabitEthernet 1/4
 loop-protect
 no loop-protect action
 loop-protect tx-mode
 switchport mode access
 switchport access vlan 1
 switchport forbidden vlan remove 1-4095
 no ip igmp snooping filter
 no ip igmp snooping max-groups
 no ip igmp snooping mrouter
 no ip igmp snooping immediate-leave
-- more --, next page: Space, continue: g, quit: ^C
```

The output of **`show running-config`** can be restricted to a specific interface. There are several such filters, described below.

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

This displays the entire currently-running system configuration.

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

Only output the commands relevant to a particular feature. The feature list depends on system configuration and software version. For example:

```
# show running-config feature ?
  <cword>    Valid words are 'access' 'access-list' 'aggregation'
'auth'
             'clock' 'dhcp' 'dhcp-snooping' 'dhcp_server' 'dns'
'dot1x'
             'erps'    'evc'    'http'    'icli'    'io_alarm'
'ip-igmp-snooping'
             'ip-igmp-snooping-port'    'ip-igmp-snooping-vlan'
'ipmc-profile'
             'ipmc-profile-range' 'ipv4' 'ipv6-mld-snooping'
             'ipv6-mld-snooping-port' 'ipv6-mld-snooping-vlan'
             'json_rpc_notification'  'lacp'  'lldp'  'logging'
'loop-protect'
             'mac' 'mep' 'monitor' 'mstp' 'netmanager' 'ntp' 'poe'
'port'
             'port-security' 'qos' 'relay' 'rmon' 'snmp' 'sntp'
'ssh'
             'swring'      'time_range'      'user'      'vlan'
'web-privilege-group-level'
```

```
mydevice# show running-config feature vlan
Building configuration...
!
vlan 1
!
!
!
!
interface GigabitEthernet 1/1
!
interface GigabitEthernet 1/2
!
interface GigabitEthernet 1/3
!
... much output omitted for brevity ...
```

The structure of running-config is maintained in the output. Sub-modes such as VLANs and Ethernet interfaces are listed, but may be empty if the requested feature is irrelevant for the particular sub-mode.

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

By using this filter, the user can review a specific list of Ethernet interfaces. This may contain wildcards, for example:

```
mydevice# show running-config interface 2.5GigabitEthernet *
Building configuration...
interface 2.5GigabitEthernet 1/9
 no spanning-tree
!
interface 2.5GigabitEthernet 1/10
 no spanning-tree
!
end
```

In this example, there is only one VLAN on the system.

```
show running-config interface vlan <list> [ all-defaults ]
```

It is also possible to filter the list of VLAN interface, for example:

```
mydevice# show running-config interface vlan 1-10
Building configuration...
interface vlan 1
```

```
ip address 192.168.1.254 255.255.255.0!
end
```

In this example, there is only one VLAN interface on the system.

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

This command can be used for the console or list of virtual terminal devices (vty). On current designs, there is a single console device, 0. For example:

```
mydevice# show running-config line console 0
Building configuration...
line console 0
!
End
```

# 6 Working with Configuration Files

There are four configuration files:

- running-config – a virtual file containing the currently running system configuration.
- startup-config – contains the boot-time configuration. When configuration is changed, it must be copied to startup-config in order to be applied at the next boot.
- default-config – a read-only file used when configuration is restored to defaults. This file is also used if startup-config is missing. It contains product-specific customizations to the default settings of the device.
- User-defined – configuration files created by the user (up to 31). These are typically used for backups or variants of startup-config.

All of these except running-config are stored in the flash file system. The available operations are:

**copy** source destination

where source and destination can be one of:

```
running-config
startup-config (or flash:startup-config)
flash:filename
dir
```

List the contents of the flash file system.

```
#more flash: filename
```

Outputs the contents of the file to the terminal.

```
#delete flash: filename
```

Erases the specific file.

## 6.1 Reverting to Default Configuration

It is possible to reset the system to a default configuration in two ways:

- Deleting startup-config and rebooting
- Instructing the software to discard the current configuration and reset to defaults without rebooting

Deleting startup-config doesn't change running-config until the system is rebooted, at which time the defaults are loaded.

Conversely, discarding the current configuration does indeed affect running-config but does not touch startup-config. If you want to save the configuration, you should save startup-config to running-config.

Rebooting and resetting the default configuration is accomplished with the reload command:

```
#reload cold

#reload defaults [ keep-ip ]
```

The reload cold version reboots the system. If the system is stacking, a specific switch can be rebooted as well by supplying its switch ID.

The second method loads configuration defaults. If the `keep-ip` keyword is given, then the system attempts to keep the most relevant parts of the VLAN 1 IP setup in order to maintain management connectivity (the IP address setup and the active default route).

There is no guarantee, however, that the above is sufficient for reverting to default configuration: it depends on the actual network properties and the system's total IP configuration. In some cases, it may be preferable to explicitly un-configure the system using 'no' commands, or prepare a suitable configuration and download it to the system's `startup-config` and reboot.

## 6.2 Use Configuration Files

The following example assumes a file system that contains an additional file called backup, previously created with a `copy` command.

```
! List files in flash:

mydevice# dir

Directory of flash:

r- 1970-01-01 00:00:00   648 default-config

rw 1970-01-06 03:57:33   1313 startup-config

rw 1970-01-01 19:54:01   1237 backup

3 files, 3198 bytes total.


! Display the contents of the file 'backup' (output is abbreviated):
mydevice# more flash:backup

hostname mydevice

...
```

```
end
! Use file 'backup' for the next boot by overwriting startup-config:
mydevice# copy flash:backup startup-config
% Saving 1237 bytes to flash:startup-config

! Verify that the sizes are identical:
mydevice# dir
Directory of flash:
r- 1970-01-01 00:00:00   648 default-config
rw 1970-01-06 05:30:41   1237 startup-config
rw 1970-01-01 19:54:01   1237 backup
3 files, 3122 bytes total.

! Regret and delete startup-config. Note how 'flash:' is required:
mydevice# delete flash:startup-config
mydevice# dir
Directory of flash:
r- 1970-01-01 00:00:00   648 default-config
rw 1970-01-01 19:54:01   1237 backup
2 files, 1885 bytes total.

! Use the currently running config for next boot:
mydevice# copy running-config startup-config
Building configuration...
% Saving 1271 bytes to flash:startup-config
```

## 6.3 Using Reload Commands

```
! Reload defaults, but try to keep VLAN 1 configuration. First list
current IP
! settings:

# show ip interface brief
Interface       Address            Method   Status
--------------- ------------------- -------- ------
VLAN 1          192.168.1.254/24    Manual   UP
mydevice# reload defaults keep-ip
```

```
% Reloading defaults, attempting to keep VLAN 1 IP address. Please
stand by.
# show ip interface brief
Interface       Address            Method   Status
--------------- ------------------- -------- ------
VLAN 1          192.168.1.254/24    Manual   UP
! Contents of flash: are unchanged:
mydevice# dir
Directory of flash:
r- 1970-01-01 00:00:00   648 default-config
rw 1970-01-06 05:33:18   1237 startup-config
rw 1970-01-01 19:54:01   1237 backup
3 files, 3122 bytes total.

! Reload again, but don't try to keep VLAN 1 settings:
# reload defaults
% Reloading defaults. Please stand by.
! Verify that the default IP settings have been restored:
 # show ip interface brief
lan Address       Method     Status
--------------- ------------------- -------- ------
1 192.0.2.1/24    Manual       UP

! Reboot the system
# reload cold
% Cold reload in progress, please stand by.
! ... bootup output omitted ...
```

## 6.4 Working with Software Images

The system can store up to two software images in flash. The image selected for bootup is termed the Active image, while the other is termed the Alternate image.

It is possible to swap the Active and the Alternative image, and it is possible to upgrade to a new Active image. A swap simply switches the Active and Alternate designation on each image and reboots the system.

A firmware upgrade performs these steps:

- Download new firmware using HTTPS and verify suitability for the system

- Overwrite the current Alternate image with the newly downloaded image
- Swap Active and Alternate and reboot

The result is that the old Active build becomes the Alternate, and the newly downloaded image Active.

Related configuration commands:

```
show version

firmware swap

show version

!  lists various details about the system, including the images in
flash.
```

CLI example: use alternate firmware to replace active firmware.

```
# firmware swap

... Erase from 0x41fd0000-0x41fdffff: Low Library.

... Program from 0x87feeffc-0x87ffeffc to 0x41fd0000: Low Library.

... Program from 0x87fef006-0x87fef008 to 0x41fd000a: Low Library.

Alternate image activated, now rebooting.

! ... much output omitted for brevity
```

# 7 System

## 7.1 System Information

CLI example: display system information.

```
# show version
MEMORY          : Total=78804 KBytes, Free=62788 KBytes, Max=62771
KBytes
FLASH           : 0x40000000-0x41ffffff, 512 x 0x10000 blocks
MAC Address     : 00-02-6f-01-02-03
Device Number   : Need to fill in!
Previous Restart : Cold

System Contact   :
System Name      :
System Location  :
System Time      : 1970-01-01T01:19:17+00:00
System Uptime    : 01:19:17

Active Image
------------
Image           :  (primary)
Version         : 5.2.2.B2021070900R1224D20000
Date            : Jul  9 2021 10:24:54 by Jaguar

Alternate Image
---------------
Image           :  (backup)
```

```
Version         : 5.2.2.B2021070900R1224D20000
Date            : Jul  9 2021 10:24:54 by Jaguar

Bootloader
----------
Image           : RedBoot (bootloader)
Version         : version 1.1
Date            : 10:26:58, Jul  9 2021

------------------
SID : 1
------------------
Port Count      : 12
Product         : Managed Switch
Software Version : 5.2.2.B2021070900R1224D20000
Build Date      : Jul  9 2021 10:24:54 by Jaguar

SoftProductID:63
Port count:12
```

CLI example, set the system time to 16: 00 p.m, June 8th, 2021.

```
# configure terminal
(config)# time set 2021/06/08 16:00:00
```

# 7.2 IP

## 7.2.1 IP Configuration

Routing or host mode configuration.

Command:

```
ip routing
no ip routing
```

### IP Interface

Configure the IP address and DHCP service function of the VLAN interface.

Command:

```
interface vlan <vlist>
```

```
ip address { { <address> <netmask> } | { dhcp [ fallback
<fallback_address> <fallback_netmask> [ timeout
<fallback_timeout> ] ] } }
```

Parameters:

- < vlist >: VLAN entry.
- <address>: IPv4 address.
- <netmask>: subnet mask.
- <fallback_address>: fallback IP address
- < fallback_netmask >: fallback subnet mask.
- <fallback_timeout>: fallback timeout

### IP Routes

Add IP routes.

Command:

```
ip route <v_ipv4_addr> <v_ipv4_netmask> <v_ipv4_gw>
```

Parameters:

- <v_ipv4_addr>: IPv4 network address.
- <v_ipv4_netmask>: subnet mask.
- <v_ipv4_gw>: gateway.

### Static ARP

Static ARP binding.

Command:

```
ip arp <v_ipv4_abc> <v_mac_addr>
```

Parameters:

- <v_ipv4_abc>: IPv4 address.
- <v_mac_addr>: MAC address.

## 7.2.2 IP Status Monitoring

### IP Interface

Displays IP interface information.

Command:

```
show interface vlan [<vlan_list>]
```

### IP Routes

Display IP route information.

Command:

```
show ip route
```

### Neighbour cache

Display neighbor cache information.

Command:

```
show ip arp
```

## 7.3 NTP

The Network Time Protocol (NTP) synchronizes the time of day among a set of distributed time servers and clients. This helps a user correlate events from system logs and other time-specific events from multiple network devices. NTP uses the User Datagram Protocol (UDP) as its transport protocol. All NTP communications use Coordinated Universal Time (UTC).

NTP version 4 is implemented, although it is disabled by default. The NTP IPv4 or IPv6 address can be configured and a maximum of five servers is supported.

Enable/Disable NTP Client or Server.

Command:

```
ntp mode { client | server }

no ntp mode { client | server }
```

Configure NTP server IP address.

Command:

```
ntp server <index_var> ip-address <ipv4_var>
```

Parameters:

- <index_var>: the index value ranges from 1 to 5.
- <IPv4 _ var>: IPv4 address format is X.X.X.X.

Instance:

To configure the NTP and server address, execute the following CLI commands.

```
# configure terminal

! Enable NTP and set server address

(config)# ntp mode client

(config)# ntp server 1 ip-address 217.198.219.102
```

The software allows the user to configure the local time zone. The switch must be configured to acquire the time from an NTP server. The default time zone is configured as None. An acronym may optionally be assigned to a selected time zone.

Show NTP Status.

Command:

```
show ntp mode { client | server } status
```

```
show ntp status
```

## 7.4 Time Zone

Time Zone Configuration.

Command:

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

Parameters:

- <word_var>: The acronym can be up to 16 alpha-numeric characters in length, allowing special characters such as, '-' (hyphen), '.'(period) and '_'(underline). The acronym is case sensitive.
- <hour _ var>: UTC time zone-12 – 12.

Instance:

CLI example, set the system time zone to (GMT+08: 00) Beijing, Chongqing, Hong Kong, Urumqi, and set the acronym to BJ.

```
(config)# clock timezone BJ 8
```

Timezone.

Command:

```
show clock detail
```

## 7.5 Log

### 7.5.1 Configure Log

Log configuration, related commands are as follows:

```
(config)# logging ?
host    host
level   Severity level
on      Enable Switch logging host mode

(config)# logging level ?
   error          Severity 3: Error conditions
   informational   Severity 6: Informational messages
   notice         Severity 5: Normal but significant condition
   warning        Severity 4: Warning conditions
```

CLI example, enable server mode and set the server address to receive logs to 192.168.1.2.

```
# configure ter
(config)# logging  on
(config)# logging host 192.168.1.2
```

### 7.5.2 Check Alarm Log

The command to view the alarm log:

```
# show alarmlog ?
   |              Output modifiers
   error          Severity 3: Error conditions
   informational    Severity 6: Informational messages
   notice         Severity 5: Normal but significant condition
   warning        Severity 4: Warning conditions
<cr>
```

Example: View the alarm log with the level of "Error"

```
# show alarmlog error
```

## 7.6 Temperature Protection

Temperature settings of the group.

Command:

```
thermal-protect grp <0-3> temperature <0-255>
```

Parameter:

- <0-3>: group ID.
- <0-255>: Temperature, unit℃.

Example:

```
(config)# thermal-protect grp 1 temperature 85
```

Port group settings.

Command:

```
thermal-protect grp <0-3>
```

Parameter:

- <0-3>: group ID.

Example:

```
(config)# interface GigabitEthernet 1/1
(config-if)# thermal-protect grp 1
```

Display information.

Command:

```
show thermal-protect [interface NAME]
```

Example:

```
# show thermal-protect interface *
```

# 8 Port

## 8.1 Port Configuration

### View Port Configuration

You can view port configuration through **show interface ?**.

View port configuration, the following commands can be supported.

```
# show interface GigabitEthernet 1/1 ?
*                  All switches or All ports
GigabitEthernet      1 Gigabit Ethernet Port
2.5GigabitEthernet    2.5 Gigabit Ethernet Port
capabilities         Display capabilities.
description          Description of interface
statistics           Display statistics counters.
status               Display status.
switchport           Show interface switchport information
transceiver          Show interface transceiver
veriphy              Display the latest cable diagnostic results.
```

CLI example: view the Port 1's status.

```
# show interface GigabitEthernet 1/1 status
```

CLI example: view the Port 1's performance parameter.

```
# show interface GigabitEthernet 1/1 capabilities
GigabitEthernet 1/1 Capabilities:
  Model:               CEServices
  Type:                10/100/1000BaseT
  Speed:               10,100,1000,auto
  Duplex:              half,full,auto
```

```
 Trunk encap. type:     802.1Q
 Trunk mode:           access,hybrid,trunk
 Channel:             no
 Broadcast suppression: no
 Flowcontrol:          yes
 Fast Start:           no
 QoS scheduling:       tx-(8q)
 CoS rewrite:          yes
 ToS rewrite:          yes
 UDLD:                no
 Inline power:         yes
 RMirror:             no
 PortSecure:           yes
 Dot1x:               no
```

CLI example: view Port 1's statistical monitoring

```
show interface GigabitEthernet 1/1 statistics
```

## Modify Port Configuration

In the config view, ports can be configured, and the supported commands are as follows.

```
(config)# interface GigabitEthernet 1/1
(config-if)# ?
   access-list          Access list
   aggregation          Create an aggregation
   description          Description of the interface
   do                  To run exec commands in the configuration
mode
   duplex               Interface duplex
   end                 Go back to EXEC mode
   evc                 Ethernet Virtual Connections
   excessive-restart       Restart backoff algorithm after 16
collisions (No  excessive-restart means discard frame after 16
collisions)
   exit                Exit from current mode
   flowcontrol          Traffic flow control.
   frame-length-check      Drop frames with mismatch between
EtherType/Length  field and actually payload size.
```

```
   help                Description of the interactive help system
   ip                  Interface Internet Protocol configuration
commands
   lacp                Enable LACP on this interface
   mac                 MAC keyword
   media-type           Media type.
   mtu                 Maximum transmission unit
   no                  Negate a command or set its defaults
   poe                 Power Over Ethernet.
   qos                 Quality of Service
   relay               Port alarm
   shutdown            Shutdown of the interface.
   snmp-server          Set SNMP server's configurations
   spanning-tree        Spanning Tree protocol
  speed               Configures interface speed. If you use 10, 100,
or 1000 keywords with the auto keyword the port will
only advertise the specified speeds.
   switchport          Switching mode characteristics
```

CLI example: set the speed of Port1 to 1Gps.

```
(config-if)# interface GigabitEthernet 1/1
(config-if)# speed 1000
```

CLI example: set Port1 to full duplex mode, enable flow control.

```
(config-if)# interface GigabitEthernet 1/1
 (config-if)# speed 1000
(config-if)# duplex ?
   auto   Auto negotiation of duplex mode.
   full   Forced full duplex.
   half   Forced half duplex.
(config-if)# duplex full
(config-if)# flowcontrol on
```

CLI example: close Port 3 and the closed port will not be accessible.

```
# configure terminal
(config-if)#  interface GigabitEthernet 1/1 GigabitEthernet 1/3
(config-if)# shutdown
```

CLI example: open Port 1 and Port 3.

```
(config)# interface GigabitEthernet 1/1
```

```
(config-if)# no shutdown
(config)# interface GigabitEthernet 1/3
(config-if)# no shutdown
```

## 8.2 DDMI

DDMI can be enabled by the following command.

```
(config)# ddmi
```

CLI example: view DDMIs enabled status.

```
# show DDMI
Current mode: Enabled
```

View DDMI monitoring data

```
# show interface GigabitEthernet 1/11 transceiver


GigabitEthernet 1/11
------------------------------
Tranceiver Information
============================================================
============
Vendor           :
Part Number       :
Serial Number     :
Revision          :
Data Code         :
Transceiver       : NONE


DDMI Information
++ : high alarm, +  : high warning, -  : low warning, -- : low alarm.
Tx: transmit, Rx: receive, mA: milliamperes, mW: milliwatts.
============================================================
============
% SFP module doesn't support DDMI
```

# 8.3 Relay alarm

## 8.3.1 View Relay Status

The relay status of power supply and port could be viewed by the following commands.

```
# show relay
Switch relay alarm is disabled
Switch relay power1 alarm is disabled
Switch relay power2 alarm is disabled
relay is configured on following
GigabitEthernet 1/1 disable
GigabitEthernet 1/2 disable
GigabitEthernet 1/3 disable
GigabitEthernet 1/4 disable
GigabitEthernet 1/5 disable
GigabitEthernet 1/6 disable
GigabitEthernet 1/7 disable
GigabitEthernet 1/8 disable
GigabitEthernet 1/11 disable
GigabitEthernet 1/12 disable
2.5GigabitEthernet 1/9 disable
2.5GigabitEthernet 1/10 disable
```

CLI example, view Port 1's relay status.

```
# show relay interface GigabitEthernet 1/1
GigabitEthernet 1/1 disable
```

## 8.3.2 Configure Relay

### Enable Relay Alarm

CLI example: enable power supply 1’s relay alarm.

```
# configure terminal
(config)# relay power 1
```

CLI example: enable Port 1’s relay alarm.

```
# configure terminal
```

```
(config)# interface GigabitEthernet 1/1
(config-if)# relay
```

## Disable Relay Alarm

CLI example: disable power supply 1’s relay alarm.

```
# configure terminal
(config)# no relay power 1
```

CLI example: disable Port 1’s relay alarm.

```
(config-if)# no relay
```

# 9 SNMP

## 9.1 Navigating the SNMP Configuration

The command to view SNMP is as follows.

```
# show snmp ?
   |                 Output modifiers
   access             access configuration
   community           Community
   host               Set SNMP host's configurations
   mib                MIB (Management Information Base)
   security-to-group   security-to-group configuration
   user               User
   view               MIB view configuration
   <cr>
```

CLI example: view the community configuration of SNMP V3.

```
# show SNMP community V3
Community   : public
Source IP   : 0.0.0.0
Source Mask : 0.0.0.0

Community   : private
Source IP   : 0.0.0.0
Source Mask : 0.0.0.0
```

## 9.2 Configure SNMP

The related commands of SNMP configuration are as follows.

```
# configure terminal
(config)# snmp ?
   access              access configuration
   community           Set the SNMP community
   contact             Set the SNMP server's contact string
   engine-id           Set SNMP engine ID
   host                Set SNMP host's configurations
   location            Set the SNMP server's location string
   security-to-group    security-to-group configuration
   trap                Set trap's configurations
   user                Set the SNMPv3 user's configurations
   version             Set the SNMP server's version
   view                MIB view configuration
   <cr>
```

CLI example: enable and disable SNMP, and view the configuration results.

```
(config)# snmp
(config)# end
# show snmp

SNMP Configuration
SNMP Mode                   : enabled
SNMP Version                : 3
Read Community              : default
Write Community             : private
Trap Mode                   : disabled

SNMPv3 Communities Table:
Community   : public
Source IP   : 0.0.0.0
Source Mask : 0.0.0.0

Community   : private
```

```
Source IP   : 0.0.0.0
Source Mask : 0.0.0.0



SNMPv3 Users Table:
User Name             : default_user
Engine ID             : 800007e5017f000001
Security Level         : NoAuth, NoPriv
... much output omitted for brevity ...

# configure terminal
(config)# no snmp
(config)# end
# show snmp

SNMP Configuration
SNMP Mode                  : disabled
SNMP Version                : 3
Read Community              : default
Write Community             : private
Trap Mode                  : disabled

SNMPv3 Communities Table:
Community   : public
Source IP   : 0.0.0.0
Source Mask : 0.0.0.0

Community   : private
Source IP   : 0.0.0.0
Source Mask : 0.0.0.0



SNMPv3 Users Table:
User Name             : default_user
Engine ID             : 800007e5017f000001
```

```
Security Level          : NoAuth, NoPriv
... much output omitted for brevity ...
```

CLI example: enable and disable SNMP Trap.

```
(config)# snmp-server trap
(config)# no snmp-server trap
```

CLI example: create a new community pub1, and set the original address of SNMP access to 192.168.1.200 and the source mask to 255.255.255.0.

```
(config)# snmp community v3 pub1 192.168.1.200 255.255.255.0
```

CLI example: update the system engine ID of SNMP, note that updating the engine ID will clear all original local users.

```
(config)# snmp engine-id local 800007e5017f000002
```

CLI example: The commands of creating new Trap entries and disabling all Trap entries.

```
(config)# snmp-server host host1
(config-snmps-host)# shutdown
```

CLI example: add community name public3, source IP is 192.168.1.254, and destination address is 255.255.255.0.

```
(config)# snmp community V3 public3 192.168.1.100 255.255.255.0
```

CLI example: create a new user user1, set the user engine to 800007e5017f000001, the authentication mode to md5 and the encryption method to AES, and set authentication password and privacy password.

```
(config)# snmp user user1 engine-id 800007e5017f000001 md5 pri aes
Auth Password Set
   Please enter the new Password:
   Enter the Password again:

Private Password Set
   Please enter the new Password:
   Enter the Password again:
The MD5 and AES protocol has security risks. Please use it caution.
```

 Notice

The encryption algorithms adopted by the device include AES, DES, SHA1 and MD5, among which:

- AES and DES encryption algorithms are reversible, SHA1 and MD5 encryption algorithms are irreversible.
- DES / MD5 / SHA1 encryption algorithm has low security and exists security risks.

Therefore, within the range of encryption algorithms supported by the protocol, it is recommended

to use more secure encryption algorithms, such as AES.

CLI example: delete the user entry with user name user1 and user engine 800007e5017f000001.

```
(config)# no snmp user user1 engine-id  800007e5017f000001
```

CLI example: create a new View, set the view type to include and MIB word OID to .1.0.1.

```
(config)# snmp view view1 .1.0.1 include
```

CLI example: create a security group with the security name usm-user and the group name ro-group.

```
(config)# snmp security-to-group model v3 name usm-user group
ro-group
```

# 10 RMON

## 10.1 Statistics Configuration

Command:

```
rmon collection stats <id>
```

Parameters:

- <id>: statistics ID, 1-65535.

## 10.2 History Configuration

Command:

```
rmon collection history <id> [ buckets <buckets> ] [ interval
<interval> ]
```

Parameters:

- <id>: history ID, 1-65535.
- <buckets>: the maximum number of sampling entries, 1--65535.
- <interval>: the sampling interval is 1-3600s.

## 10.3 Alarm Configuration

Command:

```
rmon alarm <id> { ifInOctets | ifInUcastPkts | ifInNUcastPkts |
ifInDiscards | ifInErrors | ifInUnknownProtos | ifOutOctets |
ifOutUcastPkts | ifOutNUcastPkts | ifOutDiscards | ifOutErrors }
<ifIndex> <interval> { absolute | delta } rising-threshold
<rising_threshold> [ <rising_event_id> ] falling-threshold
<falling_threshold> [ <falling_event_id> ] { [ rising | falling
| both ] }
```

Parameters:

- <ID>: 1-65535, alarm entry id.
- <ifIndex>: interface index.
- <interval>: the sampling interval is 1-2147483647.
- <rising_threshold>: rising thresholds value, -2147483648-2147483647.
- <rising_event_id>: rising event ID.
- <Falling_threshold>: falling thresholds value, -2147483648-2147483647.
- <falling_event_id>: falling event ID.

## 10.4 Link Event Configuration

Command:

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

Parameters:

- <id>: event ID.
- <community>: Trap community.
- <description>: description.

## 10.5 Statistics Monitoring

Command:

```
show rmon statistics [ <id_list> ]
```

Parameters:

- <id_list>: ID entry 1-65535.

## 10.6 History Monitoring

Command:

```
show rmon history [ <id_list> ]
```

Parameters:

- <id_list>: ID entry 1-65535.

## 10.7 Alarm Monitoring

Command:

```
show rmon alarm [ <id_list> ]
```

Parameters:

- <id_list>: ID entry 1-65535.

## 10.8 Event Monitoring

Command:

```
show rmon event [ <id_list> ]
```

Parameters:

- <id_list>: ID entry 1--65535.

# 11 Ethernet Services

## 11.1 Port Configuration

Command:

```
interface GigabitEthernet <port_type_list>
evc [ dei { colored | fixed } ] [ tag { inner | outer } ] [ addr { source | destination } ]
```

Parameters:

- <port_type_ist>: port number.

## 11.2 L2CP Configuration

Command:

```
interface GigabitEthernet <port_type_list>
evc l2cp (peer | forward ) <l2cp _list>
```

Parameters:

- <port_type_ist>: port number.
- <l2cp _list>:The value range of L2CP list is from 0 to 31, where destination BPDU(01-80-C2-00-00-0X)MAC address is 0-15 and GARP(01-80-C2-00-00-2X)MAC address is 16-31; the value range of X is 0-F.

## 11.3 Bandwidth Limitation Subset

Command:

```
evc policer [ update ] <policer_id> [ { enable | disable } ] [ type { mef | single } ] [ mode { coupled | aware } ] [ rate-type { line | data } ] [ cir <cir> ] [ cbs <cbs> ] [ eir <eir> ] [ ebs <ebs> ]
```

Parameters:

- <policer_id>:policer ID, 1-256.
- <cir>: rate of message to be sent，0-10000000kbps.
- <cbs>:size of message to be sent，0-100000bytes.
- <eir>: rate of excess message, 0-10000000kbps.
- <cbs>:size of excess message，0-100000bytes.

## 11.4 EVCs Configuration

Command:

- NNI Ports.

```
evc <evc_id> interface ( <port_type> [ <port_list> ] )
```

- EVC Parameters.

```
evc <evc_id> [ name <evc_name> ] { [ vid <evc_vid> ] } [ ivid <ivid> ]
[ learning [ disable ] ]
```

- Inner Tag.

```
evc <evc_id> [ inner-tag add { [ type { none | c-tag | s-tag |
s-custom-tag } ] [ vid-mode { normal | tunnel } ] [ vid <it_add_vid> ]
[ preserve [ disable ] ] [ pcp <it_add_pcp> ] [ dei <it_add_dei> ]
```

- Outer Tag.

```
evc <evc_id> [ outer-tag add vid <ot_add_vid> ]
```

Parameters:

- <evc_id>:EVC ID，1-256.
- <Port_type>: port type.
- <port_list>: port number
- <evc_name>:EVC name，supports 1-256 characters(A-Z, a-z, 0-9).
- <evc_vid>:EVC VLAN ID，1-4095.
- <Ivid>: The Inner VLAN ID.
- <It_add_vid>: The Inner tag VID.
- <It_add_pcp>: The inner tag PCP，0-7.
- <it_add_dei>: The inner tag DEI，0-1.
- <ot_add_vid>: The external tag VID.

## 11.5 ECEs Configuration

Command:

- UNI Ports.

```
evc ece <ece_id> [ interface ( <port_type> [ <port_list> ] ) ]
```

- UNI matching - tag type.

```
evc ece <ece_id> [ outer-tag { [ match { [ type { untagged | tagged
| c-tagged | s-tagged | any } ] [ vid { <ot_match_vid> | any } ]
```

```
[ pcp { <ot_match_pcp> | any } ] [ dei { <ot_match_dei> | any } ] } ]
[ add { [ mode { enable | disable } ] [ preserve [ disable ] ] [ pcp
<ot_add_pcp> ] [ dei <ot_add_dei> ] } ] } ]
```

- UNI matching - frame type.

```
evc ece <ece_id> [ frame-type { any | { ipv4 [ proto { <pr4> | udp
| tcp | any } ] [ dscp { <dscp4> | any } ] [ sip { <sip4> | any } ]
[ dip { <dip4> | any } ] [ fragment { yes | no | any } ] [ sport
{ <sp4> | any } ] [ dport { <dp4> | any } ] } | { ipv6 [ proto { <pr6>
| udp | tcp | any } ] [ dscp { <dscp6> | any } ] [ sip { <sip6>
| any } ] [ dip { <dip6> | any } ] [ sport { <sp6> | any } ] [ dport
{ <dp6> | any } ] } } ]
```

- Action.

```
evc ece <ece_id> [ direction { both | uni-to-nni | nni-to-uni } ]
[ evc { <evc_id> | none } ] [ pop <pop> ] [ policy <policy_no> ]
[ cos { <cos> | disable } ]
```

- MAC Parameters.

```
evc ece <ece_id> [ smac { <smac> | any } ] [ dmac { <dmac> | unicast
| multicast | broadcast | any } ]
```

Parameters:

- <ece_id>:ECE ID，1-256.
- <Port_type>: port type.
- <port_list>: port number.
- <ot_match_vid>: The external match VID.
- <ot_match_pcp>: The external match PCP, 0-7.
- <ot_match_dei>: The external match DEI, 0-1.
- <It_add_pcp>: The egress tag PCP, 0-7.
- <it_add_dei>: The egress tag DEI，0-1.
- <Pr4>: IP protocol type, 0-255.
- <dscp4>:DSCP filter value or range.
- <sip4>:source IP address.
- <dip4>:destination IP addresses.
- <Sp4>:source port.
- <Dp4>:destination port.
- <Pop>: PoP tag statistics, 0-2.
- <policy_no>:ACL strategy, 0-255.
- <cos>:CoS service type, 0-7.
- <Smac>: Source MAC address.
- <Dmac>: Destination MAC address.

## 11.6 EVC Statistics Monitoring

Command:

```
show evc statistics [ interface ( <port_type> [ <port_list> ] ) ]
[ cos <cos> ] [ green | yellow | red | discard ]
```

```
show evc { [ <evc_id> | all ] } [ ece [ <ece_id> ] ]
```

Parameters:

- <Port_type>: port type.
- <port_list>: port number.
- <cos>:CoS service type, 0-7.
- <evc_id>:ECE ID，1-256.

# 12 Configure Static Routing

An IP address identifies a device on an IP network. The IP version 4 (IPv4) address is 32 bits long. An IPv4 address can only be assigned through a VLAN interface. The address can be set manually (called a static IP) or automatically by using the DHCP protocol. For more information, see Configuring DHCP Client Switch Application Software to Handle Software Static IPv4 Routes.

## Traditional Network

Routing involves both a TCP/IP host and an IP router. The following illustration shows the configuration for a traditional network with two IP networks and a router. Each IP network needs to have an IP address assigned and a gateway where packets can be forwarded to.

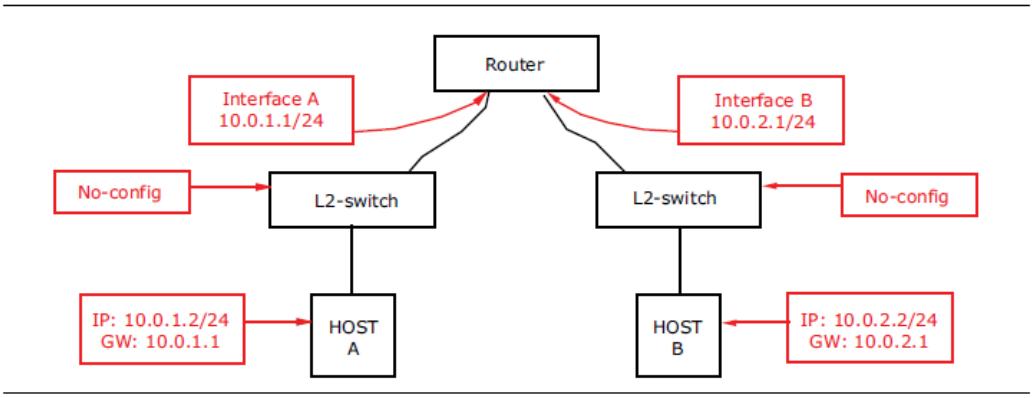



Figure • IP Routing of using Router and L3 Switch

## Using a VLAN-Aware Switch

The following illustration shows the same network configured to use a VLAN-aware switch. Using VLANs is a method of separating flows within the same switch.

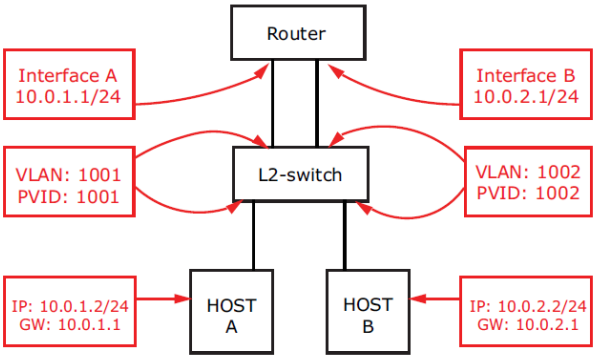



Figure • IP Routing using a Router and VLAN-Aware Switch

## Configuration using ICLI

The following steps implement the configurations using the command line interface.

**Step1.** Create VLAN 1001 and 1002 to separate the two IP networks

```
Switch# configure terminal
Switch(config)# vlan 1001
Switch(config-vlan)# vlan 1002
Switch(config-vlan)# exit
```

**Step2.** Define the port VLAN for each port by using the switchport access vlan command to specify the VLAN for each interface. Untagged frames are then classified to this VLAN.

```
Switch(config)# interface GigabitEthernet 1/1
Switch(config-if)# switchport access vlan 1001
Switch(config-if)# exit
Switch(config)# interface GigabitEthernet 1/2
Switch(config-if)# switchport access vlan 1002
Switch(config-if)# exit
```

**Step3.** Configure router leg A and B by using the ip address command to set primary IP address for the interfaces.

```
Switch(config)# interface vlan 1001
Switch(config-if-vlan)#  ip  address  10.0.1.1  255.255.255.0
Switch(config-if-vlan)# exit
Switch(config)# interface vlan 1002
Switch(config-if-vlan)#  ip  address  10.0.2.1  255.255.255.0
Switch(config-if-vlan)# end
```

# 13 Layer 2 Protocol Configuration

This document describes how to configure switch to perform Layer 2 functions such as Link Aggregation (LAG), Link Aggregation Control Protocol (LACP), Virtual LANs (VLANs), Mirroring and Multiple Spanning Tree Protocol (MSTP). Configuration examples are provided for the command line interface (CLI).

## 13.1 Link Aggregation

Aggregation enables the use of multiple ports in parallel to increase the link speed beyond the limits of a single port, and to increase the redundancy for higher availability. If the system has 6 ports, the maximum aggregation group is 3 (6 divided by 2).

### Adding a Port to an Aggregation Group

CLI example: Add the first Gigabit port into group 1

```
# configure terminal
(config)# interface GigabitEthernet 1/1
(config-if)# aggregation ?
group   Create an aggregation group
(config-if)# aggregation group ?
<uint> The aggregation group id
(config-if)# aggregation group 1
```

### Configuring the Aggregation Mode

The aggregation feature uses the following keys to calculate the destination port for the frame. The default method is the source MAC address, IP address, and TCP/UDP port number. By default, Destination MAC Address is not used.

CLI Example: Change aggregation mode to dmac, ip, port, and smac

```
# configure terminal
(config)# aggregation mode ?
```

```
Dmac    Destination MAC affects the distribution
ip      IP address affects the distribution
port IP port affects the distribution
smac Source MAC affects the distribution
<cr>
(config)# aggregation mode dmac ip port smac
(config)# do show aggregation mode
Aggregation Mode:

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

The current aggregation mode can be viewed using the **show aggregation mode** command.

```
# show aggregation mode
Aggregation Mode:

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

# 13.2 LACP

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

## Enable LACP

When LACP is enabled on a port, with the lacp command, it will form an aggregation when 2 or more ports are connected to the same partner. The default value is Disabled.

CLI Example: Enable LACP on the first Gigabit port

```
# configure terminal
(config)# interface GigabitEthernet 1/1
(config-if)# lacp
```

CLI Example: Disable LACP on the first Gigabit port

```
# configure terminal
```

```
(config)# interface GigabitEthernet 1/1
(config-if)# no lacp
```

## Configure Keyword

The port's LACP key ranges from 1 to65535. The Auto setting will set the key according physical link speed, 10Mb = 1, 100Mb = 2, 1Gb = 3. Using the Specific setting, a user-defined value can be entered. Ports with the same Key value can participate in the same aggregation group, while ports with different keys cannot. The default value is automatic.

CLI Example: Set LACP key to 3 on the first Gigabit port

```
# configure terminal
(config)# interface GigabitEthernet 1/1
(config-if)# lacp key ?
<1-65535>  Key value
auto Choose a key based on port speed
(config-if)# lacp key 3
```

## Configuring the Role

LACP role shows the activity status. An Active role transmits LACP packets each second, while Passive waits for an LACP packet from a partner, also known as the "speak if spoken to" role. The default value is active.

CLI Example: Set LACP Role to Passive on the first Gigabit port

```
# configure terminal
(config)# interface GigabitEthernet 1/1
(config-if)# lacp role ?
active  Transmit LACP BPDUs continously
passive Wait for neighbour LACP BPDUs before transmitting
(config-if)# lacp role passive
```

## Configuring the Timeout

The Timeout controls the period between BPDU transmissions. Fast transmits LACP packets each second while Slow waits for 30 seconds before sending a LACP packet. The default value is Fast.

CLI example: Set LACP Timeout to slow on the first Gigabit port

```
# configure terminal
(config)# interface GigabitEthernet 1/1
(config-if)# lacp timeout ?
Fast   Transmit BPDU each second (fast timeout)
slow   Transmit BPDU each 30th second (slow timeout)
```

```
(config-if)# lacp timeout slow
```

### Configure Priority

Priority controls the priority of the port. If the LACP partner wants to form a larger group than is supported by this device, then this parameter controls which ports will be active and which ports will be in a backup role. Lower number means greater priority. The default value is 32768.

CLI Example: Set LACP priority to 1000 on the first Gigabit port

```
# configure terminal
(config)# interface GigabitEthernet 1/1
(config-if)# lacp port-priority ?
<1-65535>  Priority value, lower means higher priority
(config-if)# lacp port-priority 1000
```

### Display State

The current LACP mode can be viewed with the show lacp command, as follows:

```
# show lacp ?
internal   Internal LACP configuration
neighbour  Neighbour LACP status
statistics Internal LACP statistics
system-id  LACP system id
```

## 13.3 MAC Address Table

Switching is based upon the DMAC address contained in the frame. The switch builds up a table that maps MAC addresses to switch ports for knowing which ports the frames should go to. This table contains both static and dynamic entries. The static entries are configured by the network administrator if the administrator wants to do a fixed mapping between the DMAC address and switch ports.

The frames also contain a source MAC address (SMAC address), which shows the MAC address of the equipment sending the frame. The SMAC address is used by the switch to automatically update the MAC table with these dynamic MAC addresses. Dynamic entries are removed from the MAC table if no frame with the corresponding SMAC address has been seen after a configurable age time.

The MAC address table related configuration commands are as follows:

- Set MAC aging time
- Set automatic MAC address learning:
  - Automatic MAC address learning of VLAN
  - Automatic MAC address learning of port
- Add static MAC address for VLAN

```
mydevice(config)# mac address-table?
```

```
   aging-time    Mac address aging time
   learning      Mac Learning
static       Static MAC address
mydevice(config)# mac address-table learning ?
vlan    VLAN
mydevice(config)#  interface GigabitEthernet 1/6
mydevice(config-if)# mac address-table learning
```

### Set the Aging Time

By default, dynamic entries are removed from the MAC table after 300 seconds. This removal is also called aging.

CLI Example: Change the aging time to 600 seconds

```
# configure terminal
(config)# mac address-table aging-time ?
<0,10-1000000>Aging time in seconds, 0 disables aging
(config)# mac address-table aging-time 600
```

### Adding a Static MAC Address Entry

CLI Example: Add static MAC address: 00:00:00:00:00:01 in VLAN 2 on the first Gigabit port

```
# configure terminal
(config)# mac address-table ?
   aging-time    Mac address aging time
   learning      Mac Learning
static       Static MAC address
(config)#  mac  address-table  static  00:00:00:00:00:01  vlan  2
interface GigabitEthernet 1/1
```

### Display MAC Address Table

The current MAC address table can be viewed with the show mac address-table command as follows:

```
# show mac address-table
```

## 13.4 VLAN

The following illustration shows an example VLAN configuration.

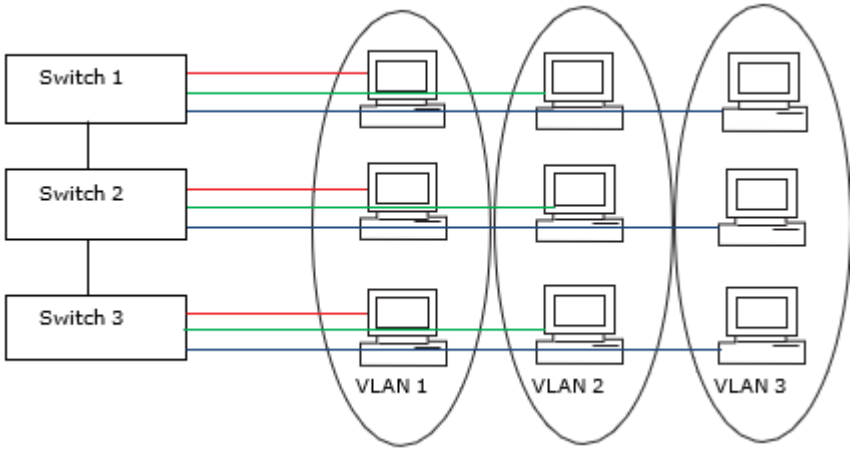



Figure • VLAN Quick Configuration Example

Because VLAN 1 is created by default, one need only add VLAN 2 and 3, as follows:

```
# configure terminal
(config)# vlan 2
(config)# vlan 3
```

Set the access port. Assume that port 1 through3 are connected to the PC. The PVID of each port is different.

```
# configure terminal
(config)# interface GigabitEthernet 1/1
(config-if)# switchport mode access
(config-if)# switchport access vlan 1
(config)# exit
(config)# interface GigabitEthernet 1/2
(config-if)# switchport mode access
(config-if)# switchport access vlan 2
(config)# exit
(config)# interface GigabitEthernet 1/3
(config-if)# switchport mode access
(config-if)# switchport access vlan 3
(config)# exit
```

Set the Trunk Port. Assume that port 4 is connected to the other switch. Set the received VLAN to 1-3.

```
# configure terminal
(config)# interface GigabitEthernet 1/4
(config-if)# switchport mode trunk
(config-if)# switchport trunk allowed vlan 1-3
```

```
Configure the port such that frames are always transmitted with
a tag on port 4.
(config-if)# switchport trunk vlan tag native
```

## Global Configuration

## Existing VLAN

CLI Example: Adding VLAN 2

```
# configure terminal
(config)# vlan 2
```

CLI Example: Removing VLAN 2

```
# configure terminal
(config)# no vlan 2
```

CLI Example: Show existing VLANs

```
# show vlan brief
VLAN    Name    Interfaces
1    default    Gi 1/1-6
2    VLAN0002
```

The Allowed Access VLAN field only affects ports configured as access ports. Ports in other modes are members of all VLANs specified in the allowed VLANs field . By default, only VLAN 1 is enabled. More VLANs may be created by using the following list syntax.

```
# configure terminal
(config)# vlan1,10-13,200,300
```

Individual elements are separated by commas and ranges are specified with a dash separating the lower and upper bound. Spaces are allowed in between the delimiters. The example creates VLANs 1, 10, 11, 12, 13, 200, and 300.

## VLAN Naming

CLI Example: Set VLAN2’s name to test

```
# configure terminal
(config)# vlan 2
(config-vlan)# name test
```

# 13.4.1 Port Based Configuration

## Port mode

Port mode determines the fundamental behavior of the port in question. A port can be in one of three modes, with Access being the default.

## Access

Access ports are normally used to connect to end stations. Access ports have the following characteristics:

- Member of exactly one VLAN, the Port LAN or Access VLAN, which by default is 1
- Accepts untagged frames and C-tagged frames
- Discards all frames that are not classified to the Access VLAN
- Upon egress all frames are transmitted untagged

## Trunk

Trunk ports can carry traffic on multiple VLANs simultaneously, and are normally used to connect to other switches. Trunk ports have the following characteristics.

- Member of all existing VLANs by default (limited by the use of allowed VLANs)
- All frames except those classified to the Port VLAN or Native VLAN get tagged on egress by default (frames classified to the Port VLAN do not get C-tagged on egress)
- Egress tagging can be changed to tag all frames, in which case only tagged frames are accepted on ingress

## Hybrid:

Hybrid ports resemble trunk ports in many ways while including additional port configuration features. In addition to the characteristics described for trunk ports, hybrid ports have the following abilities.

- Ingress filtering can be controlled
- Ingress acceptance of frames and configuration of egress tagging can be configured independently

CLI Example: Configure as Access port on the first Gigabit port

```
# configure terminal
(config)# interface GigabitEthernet 1/1
(config-if)# switchport mode access
```

CLI Example: Configure as Trunk port on the first Gigabit port

```
# configure terminal
(config)# interface GigabitEthernet 1/1
(config-if)# switchport mode trunk
```

CLI Example: Configure as Hybrid port on the first Gigabit port

```
# configure terminal
(config)# interface GigabitEthernet 1/1
(config-if)# switchport mode hybrid
```

## Port VLAN

Port VLAN determines the port's VLAN ID, or PVID. Allowed VLANs are in the range 1 through 4095, default being 1.

On ingress, frames get classified to the Port VLAN if the port is configured as VLAN unaware, the frame is untagged, or VLAN awareness is enabled on the port, but the frame is priority tagged (VLAN ID = 0).

On egress, frames classified to the Port VLAN do not get tagged if Egress Tagging is set to untag port VLAN.

The Port VLAN is called an "Access VLAN" for ports in Access mode and Native VLAN for ports in Trunk or Hybrid mode.

CLI Example: Set Port VLAN to 2 on the first Gigabit port (configured as access mode)

```
# configure terminal
(config)# interface GigabitEthernet 1/1
(config-if)# switchport access vlan ?
   <vlan_id>  VLAN ID of the native VLAN when this port is in trunk mode
(config-if)# switchport access vlan 2
```

CLI Example: Set port VLAN to 2 on the first Gigabit port (configured as trunk mode)

```
# configure terminal
(config)# interface GigabitEthernet 1/1
(config-if)# switchport trunk native vlan 2
```

CLI Example: Set port VLAN to 2 on the first Gigabit port (configured as hybrid mode)

```
# configure terminal
(config)# interface GigabitEthernet 1/1
(config-if)# switchport hybrid native vlan 2
```

## Ingress Filtering

Hybrid ports allow for changing ingress filtering. Access and Trunk ports always have ingress filtering enabled.

If ingress filtering is enabled, frames classified to a VLAN that the port is not a member of get discarded.

If ingress filtering is disabled, frames classified to a VLAN that the port is not a member of are accepted and forwarded to the switch engine. However, the port will never transmit frames classified to VLANs that it is not a member of.

CLI example: Set ingress filtering on the first Gigabit port

```
# configure terminal
(config)# interface GigabitEthernet 1/1
```

```
(config-if)# switchport hybrid ?
acceptable-frame-type    Set acceptable frame type on a port
allowed                  Set allowed VLAN characteristics when
interface is in hybrid mode
egress-tag               Egress VLAN tagging configuration
ingress-filtering        VLAN Ingress filter configuration
native                   Set native VLAN
```

## Ingress Acceptance

Hybrid ports allow for changing the type of frames that are accepted on ingress.

## Tagged or Untagged

Both tagged and untagged frames are accepted.

## Tagged Frame Only

Only tagged frames are accepted on ingress. Untagged frames are discarded.

## Untagged Frame Only

Only untagged frames are accepted on ingress. Tagged frames are discarded.

CLI example: Configure ingress filtering on the first Gigabit port

```
# configure terminal
(config)# interface GigabitEthernet 1/1
(config-if)# switchport hybrid acceptable-frame-type ?
all     Allow all frames
tagged  Allow only tagged frames
untagged   Allow only untagged frames
```

## Egress Tagging

Ports in Trunk and Hybrid mode may control the tagging of frames on egress.

## Untag Port VLAN

Frames classified to the Port VLAN are transmitted untagged. Other frames are transmitted with the relevant tag.

## Tag All

All frames, whether classified to the Port VLAN or not, are transmitted with a tag.

## Untag All

All frames, whether classified to the Port VLAN or not, are transmitted without a tag. This option is only available for ports in Hybrid mode.

CLI Example: Set egress tagging on the first Gigabit port

```
# configure terminal
(config)# interface GigabitEthernet 1/1
(config-if)# switchport hybrid egress-tag ?
all     Tag all frames
none    No egress tagging
```

## Allowed VLANs

Ports in Trunk and Hybrid mode may control which VLANs they are allowed to become members of. Access ports can only be members of the Access VLAN.

The field's syntax is identical to the syntax used in the Existing VLANs field. By default, a port may become a member of all possible VLANs, and therefore set it to 1-4095.

The field may be left empty, which means that the port will not be member of any of the existing VLANs.

CLI example: Set port VLAN to 2 on the first Gigabit port (configured as trunk mode)

```
# configure terminal
(config)# interface GigabitEthernet 1/1
(config-if)# switchport trunk allowed vlan ?
<vlan_list>   VLAN IDs of the allowed VLANs when this port is
in hybrid mode
add           Add VLANs to the current list
all           All VLANs
except        All VLANs except the following
none          No VLANs
remove        Remove VLANs from the current list
```

CLI example: Set port VLAN to 2 on the first Gigabit port (configured as hybrid mode)

```
# configure terminal
(config)# interface GigabitEthernet 1/1
(config-if)# switchport hybrid allowed vlan ?
<vlan_list>   VLAN IDs of the allowed VLANs when this port is in
hybrid mode
add           Add VLANs to the current list
all           All VLANs
except        All VLANs except the following
none          No VLANs
remove        Remove VLANs from the current list
```

## Forbidden VLANs

A port may be configured to never be a member of one or more VLANs. This is particularly useful when dynamic VLAN protocols such as MVRP and GVRP must be prevented from dynamically adding ports to VLANs.

The trick is to mark such VLANs as forbidden on the port in question. The syntax is identical to the syntax used in the Existing VLANs field.

By default, the field is left blank, which means that the port may become a member of all possible VLANs.

CLI example: Configure forbidden VLAN on the first Gigabit port.

```
# configure terminal
(config)# interface GigabitEthernet 1/1
(config-if)# switchport forbidden vlan ?
add         Add to existing list.
remove      Remove from existing list.
```

## Show VLAN Status

CLI Example

```
# show vlan ?
brief       VLAN summary information
id          VLAN status by VLAN id
ip-subnet   Show VLAN ip-subnet entries.
mac         Show VLAN MAC entries.
name        VLAN status by VLAN name
protocol    Protocol-based VLAN status
status      Show the VLANs configured for each interface.
<cr>
```

# 13.4.2 Configure MAC-based /Protocol based /IP Subnet-based VLAN

Supported commands for Configuring MAC-based /Protocol based /IP Subnet-based VLAN are as follows:

```
mydevice# configure ter
(config)# interface GigabitEthernet 1/1
mydevice(config-if)# switchport vlan ?
   ip-subnet    VCL IP Subnet-based VLAN configuration.
   mac         MAC-based VLAN commands
```

```
protocol    Protocol-based VLAN commands
(config-if)# exit

mydevice(config)# vlan protocol ?
   eth2    Ethernet-based VLAN commands
   llc     LLC based VLAN group
snap    SNAP-based VLAN group

mydevice(config-if)# switchport vlan ip-subnet ?
   <ipv4_subnet>    Source IP address and mask (Format:
                    xx.xx.xx.xx/mm.mm.mm.mm).
id              Specify an index for the IP subnet entry
 (deprecated).

mydevice(config-if)# switchport vlan mac ?
   <mac_ucast>    48 bit unicast MAC address: xx:xx:xx:xx:xx:xx
mydevice(config-if)# switchport vlan protocol?
   group    Protocol-based VLAN group commands
mydevice(config-if)# switchport vlan protocol group ?
   <word16>    Group Name (Range: 1 - 16 characters)
mydevice(config-if)# switchport vlan protocol group 1 ?
vlan    VLAN keyword
```

CLI example: configure the subnet 192.168.1.0/255.255.255.0 as VLAN1.

```
mydevice(config-if)#       switchport       vlan       ip-subnet
192.168.1.0/255.255.255.0 vlan 1
```

CLI example: configure the MAC address 00:00:00:00:00:01 as VLAN1.

```
mydevice(config-if)# switchport vlan mac 00:00:00:00:00:01 vlan
1
```

CLI example: divide the data flow of arp protocol of Port 1 into VLAN1

```
mydevice(config)# vlan protocol eth2 arp group 1
mydevice(config)# interface GigabitEthernet 1/1
mydevice(config-if)# switchport vlan protocol group 1 vlan 1
```

# 13.5 Port Mirroring

Note

This function is only used for network traffic monitoring and fault location, and does not involve any operations related to collecting user data.

## Local Mirroring

For debugging network problems or monitoring network traffic, the switch system can be configured to mirror frames from multiple ports to a mirror port.

## Mirror the Traffic of Port X to Port Y

1. Mirror the traffic (both rx and tx) of the first Gigabit port

```
(config)# monitor source interface GigabitEthernet 1/1 both
```

2. Configure the mirror destination port to Gigabit port 6.

```
(config)# monitor destination interface GigabitEthernet 1/6
```

# 13.6 Multiple Spanning Tree Protocol

## Bridge Settings

## ICLI Commands for Basic Settings

The following ICLI commands refer to the basic settings.

The protocol version is set by the ICLI command:

```
(config)# spanning-tree mode [mstp|rstp|stp]
```

The bridge priority is set by:

```
(config)# spanning-tree mst 0 priority ?
<0-61440>   bridge priority in increments 0f 4096 (Lower
Priority indicates greater likelihood of becoming
            root)
```

The bridge priority should be set to a multiple of 4096, that is, one of 4096*i, where i=0, …, 15.

The forward delay is set by:

```
(config)# spanning-tree mst forward-time <4-30>
```

<4-30> is one of the numbers of 4, 5,…,30.

The max age is set by:

```
(config)# spanning-tree mst max-age <6-40>
```

The max hop is set by:

```
(config)# spanning-tree mst max-hop <6-40>
```

The transmit hold count is set by:

```
(config)# spanning-tree transmit hold-count <1-10>
```

## ICLI Commands for Advanced Settings

The following ICLI commands refer to the advanced settings.

The edge port BPDU filtering is enabled with the ICLI command:

```
(config)# [no] spanning-tree edge bpdu-filter
```

The edge port BPDU guard is enabled with the ICLI command:

```
(config)# [no] spanning-tree edge bpdu-guard
```

The port error recovery and port error recovery timeout is set by one ICLI command:

```
(config)# [no] spanning-tree recovery interval <30-86400>
```

which both enables and sets the value. The no form disables it.

## MSTI Configuration

By default, all VLAN IDs are mapped to the Common and Internal Spanning Tree (CIST). If the protocol version is set to MSTP, then a VLAN ID can be mapped to one out of 8 spanning trees, where CIST is one. The 7 others are called MSTI1,…, MSTI7. A MSTI configuration also has a name and revision. All these values have to be identical on the switches in the network. Otherwise the configuration will not take effect.

The configuration identity is configured as follows.

```
(config)# spanning-tree mst name <ConfigurationName> revision
<RevisionNumber>
```

where <ConfigurationName> is a string of maximum length 32 characters, and <RevisionNumber> is an integer in the range of 0,…,65535.

The VLANs are added to MSTI1 and MIST2 with the following commands.

```
(config)# [no] spanning-tree mst 1 vlan 10-15

(config)# [no] spanning-tree mst 2 vlan 16,18
```

The no form deletes all VLANs in the MSTI in question.

## MSTI Priorities

Each MSTI and CIST can be given a priority. The lower the priority numeric values, the higher priority.

A Bridge Identifier is constructed per CIST, MSTI1,…,MSTI7, the bridge priority number. This is concatenated with the MAC address of the switch. In this way the bridge Identifier is unique.

A low bridge Identifier indicates a higher priority. A high priority means that the switch tends to be the root of the spanning tree. If two switches have the same bridge priority, then for example, setting MSTI1 priority higher, or setting MSTI2 lower, makes one switch tends the root.

## STP CIST Port Configuration

STP is configured on a port basis.

All parameters, except Path Cost and Priority, are specific for the port and not for CIST. These two parameters can be set for each MSTI, but the other parameters cannot because they apply to the port. If, for example, spanning tree is disabled (as it is for port 3), it applies to the CIST and all the MSTIs.

When using the ICLI, the CIST Aggregation Port Configuration commands are performed at the Config mode prompt as follows.

```
(config)#
```

The CIST Normal Port Configuration commands are performed in the Config Interface mode prompt as follows.

```
(config-if)#
```

The following commands below assume that the user is in the interface config mode.

## STP Enabled

A port can be individually enabled or disabled for taking part in the spanning tree protocol with the following command.

```
(config-if)# [no] spanning-tree
```

## Path Cost and Priority

The path cost and priority are set by the following commands:

```
(config-if)# spanning-tree mst 0 cost <Cost>
(config-if)# spanning-tree mst 0 port-priority <Priority>
```

<Cost> is a number in the range 1 to 200000000 or it may be auto. If set to auto, then the path cost will be set to some value appropriate for the physical link speed, using IEEE 802.1D recommended values.

<Priority> is a number in the range 0 to 240 and a multiple of 16. If it is not a multiple of 16 then it will be set to 0.

The path cost is used by STP when selecting ports. Low cost is chosen in favor of high cost. And if two ports have the same cost, then priority is used as a tie breaker.

## Admin Edge and Auto Edge

These two features are activated by the following ICLI commands.

```
(config-if)# [no] spanning-tree edge
(config-if)# [no] spanning-tree auto-edge
```

The first command changes the field Admin Edge, and the second changes Auto Edge. These two values control how a port is declared to be an edge port or not. An edge port is a port which is not connected to a bridge.

If auto edge is enabled, then the port determines whether it is an edge port by registering if BPDUs are received on that port. The admin edge determines what the port should start as, being edge or not, until auto edge if enabled, then change.

The decision can be seen by selecting Monitor > Spanning Tree > Bridge Status, then clicking on CIST. Then the Edge field shows the decision.

## Restricted Role and Restricted TCN

These two features are activated by the following ICLI commands.

```
(config-if)# [no] spanning-tree restricted-role
(config-if)# [no] spanning-tree restricted-tcn
```

If restricted role is enabled it causes the port not to be selected as root port for the CIST or any MSTI, even if it has the best spanning tree priority vector. Such a port will be selected as an alternate port after the root port has been selected. If set, it can cause lack of spanning tree connectivity. It can be set by a network administrator to prevent bridges external to a core region of the network influence the spanning tree active topology, possibly because those bridges are not under the full control of the administrator. This feature is also known as Root Guard.

If restricted TCN is enabled it causes the port not to propagate received topology change notifications and topology changes to other ports. If set it can cause temporary loss of connectivity after changes in a spanning tree's active topology as a result of persistently incorrect learned station location information. It is set by a network administrator to prevent bridges external to a core region of the network, causing address flushing in that region, possibly because those bridges are not under the full control of the administrator or the physical link state of the attached LANs transits frequently.

## BPDU Guard

This feature is activated by the following ICLI command.

```
(config-if)# [no] spanning-tree bpdu-guard
```

If enabled, causes the port to disable itself upon receiving valid BPDU's. Contrary to the similar bridge setting, the port Edge status does not effect this setting.

## Point-to-Point

This feature is activated by the following ICLI command.

```
(config-if)# [no] spanning-tree link-type
{auto|point-to-point|shared}
```

where the no form is equivalent to setting it to auto.

Setting the link to point-to-point, shows up as Forced True. Setting it to shared, is shown as Force False. Setting it to auto shows as Auto.

## MSTI Ports

The ICLI commands for setting the path cost and priority is the same as for CIST, but with the change that the MSTI is not 0 (MSTI0 is CIST), but a number from 1 to 7.

```
(config-if)# spanning-tree mst <MSTI> cost <Cost>
(config-if)# spanning-tree mst <MSTI> port-priority <Priority>
```

Here <MSTI> is the number of the MSTI, from 1 to 7. The other parameters are the same as in the CIST case.

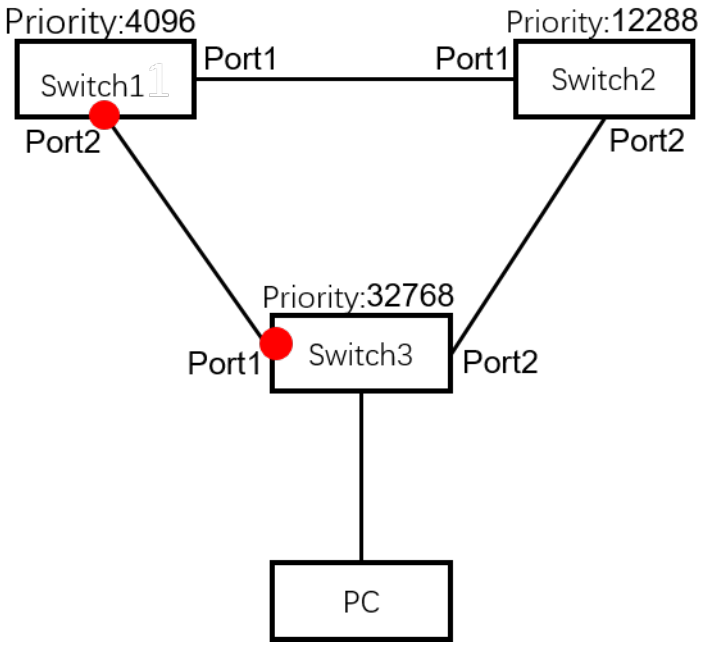
<Cost> is a number in the range 1 to 200000000 or it may be auto. If set to auto, then the path cost will be set to some value appropriate for the physical link speed, using IEEE 802.1D recommended values.

<Priority> is a number in the range 0 to 240 and a multiple of 16. Note that if it is not a multiple of 16 then it will be set to 0.

The path cost is used by STP when selecting ports. Low cost is chosen in favor of high cost. And if two ports have the same cost, then priority is used as a tie breaker.

## Single Ring Configuration Instance

Use three switches for single ring configuration experiment. Set the version of the spanning tree to STP, and configure the global priority of the spanning tree as shown in the following figure.




The port roles of each switch in the single ring are as follows:

- The highest priority of Switch 1 is the root bridge, Port 1 is the designated port, and Port 2 is the blocked port;
- Port 1 of Switch 2 is the root port and Port 2 is the designated port;
- Port 1 of Switch 3 is the root port and Port 2 is the blocked port.

Configuration Command of Switch 1 is as follows:

```
# configure terminal
```

```
(config)# interface GigabitEthernet 1/1
(config-if)# spanning-tree
(config-if)#exit
(config)# interface GigabitEthernet 1/2
(config-if)# spanning-tree
(config-if)#exit
(config)# spanning-tree mode stp
(config)# spanning-tree mst 0 priority 4096
```

Configuration Command of Switch 2 is as follows:

```
(config)# interface GigabitEthernet 1/1
(config-if)# spanning-tree
(config-if)#exit
(config)# interface GigabitEthernet 1/2
(config-if)# spanning-tree
(config-if)#exit
(config)#spanning-tree mode stp
(config)#spanning-tree mst 0 priority 12288
```

Configuration Command of Switch 3 is as follows:

```
(config)# interface GigabitEthernet 1/1
(config-if)# spanning-tree
(config-if)#exit
(config)# interface GigabitEthernet 1/2
(config-if)# spanning-tree
(config-if)#exit
(config)spanning-tree mode stp
(config)spanning-tree mst 0 priority 32768
```

View the spanning tree activity status of Switch 1, and you can see that Switch 1 is a root bridge. The MAC address of Switch 1 used in the example is 00-22-6F-01-B1-20.

```
# show spanning-tree active
CIST Bridge STP Status
Bridge ID    : 4096.00-22-6F-01-B1-20
Root ID      : 4096.00-22-6F-01-B1-20
Root Port    : -
Root PathCost: 0
Regional Root: 4096.00-22-6F-01-B1-20
Int. PathCost: 0
```

```
Max Hops     : 20
TC Flag      : Steady
TC Count     : 0
TC Last      : -
Port       Port Role       State       Pri   PathCost   Edge   P2P
Uptime
---------  --------------  ----------  ---   --------   ----   ---
-------------
Gi 1/1     DesignatedPort  Learning    128     20000  No     Yes  0d
00:00:32
Port       Port Role       State       Pri   PathCost   Edge   P2P
Uptime
```

View the port status of Switch 1: Port 1 is in forwarding status and Port 2 is in blocking status.

```
# show stpstate
Port  StpState      LinkState
1     Forwarding     Link
2     Blocking       Down
3     Blocking       Down
4     Blocking       Down
5     Blocking       Down
6     Blocking       Down
7     Blocking       Down
8     Forwarding     Link
9     Blocking       Down
10    Blocking       Down
11    Blocking       Down
12    Blocking       Down
```

View the spanning tree activity status of Switch 2.

```
#   show spanning-tree active
CIST Bridge STP Status
Bridge ID    : 12288.00-22-6F-00-00-66
Root ID      : 4096.00-22-6F-01-B1-20
Root Port    : 1
Root PathCost: 20000
Regional Root: 12288.00-22-6F-00-00-66
Int. PathCost: 0
```

```
Max Hops     : 20
TC Flag      : Steady
TC Count     : 129
TC Last      :   0d 00:03:50
Port       Port Role       State       Pri  PathCost  Edge  P2P
Uptime
---------  --------------  ----------  ---  --------  ----  ---
-------------
Gi 1/1     RootPort        Forwarding  128     20000  No    Yes  0d
00:41:04
Gi 1/2     DesignatedPort  Forwarding  128     20000  No    Yes  0d
00:33:53
```

View the port status of Switch 2: Ports 1 and 2 are in forwarding status.

```
# show stpstate
Port  StpState      LinkState
1     Forwarding     Link
2     Forwarding     Link
3     Blocking       Down
4     Blocking       Down
5     Blocking       Down
6     Blocking       Down
7     Blocking       Down
8     Forwarding     Down
9     Blocking       Down
10    Blocking       Down
11    Blocking       Down
12    Blocking       Down
```

View the spanning tree activity status of Switch 3.

```
#  show spanning-tree active
CIST Bridge STP Status
Bridge ID    : 32768.00-22-6F-00-00-0C
Root ID      : 4096.00-22-6F-01-B1-20
Root Port    : 2
Root PathCost: 40000
Regional Root: 32768.00-22-6F-00-00-0C
Int. PathCost: 0
Max Hops     : 20
```

```
TC Flag     : Steady

TC Count    : 0

TC Last     : -

Port       Port Role       State       Pri  PathCost  Edge  P2P
Uptime

---------  --------------  ----------  ---  --------  ----  ---
-------------

Gi 1/2     RootPort        Learning    128    20000  No    Yes  0d
00:00:20
```

View the port status of Switch 3: Port 1 is in blocking status and Port 2 is in forwarding status.

```
# show stpstate

Port  StpState      LinkState

1     Blocking      Down

2     Forwarding    Link

3     Blocking      Down

4     Blocking      Down

5     Blocking      Down

6     Blocking      Down

7     Forwarding    Down

8     Blocking      Down

9     Blocking      Down

10    Blocking      Down

11    Blocking      Down

12    Blocking      Down
```

## 13.7 LLDP Configuration

This document provides step-by-step guidance on how to use ICLI command to set up LLDP, LLDP-MED, and CDP for discovering connected network equipment managed by a management platform, which may be a computer running an IP-capable operating system such as FeeBSD, Linux, or Windows.

Using ICLI as the management interface requires a serial console connection between the device and management platform. No network connection is required to use ICLI, but the terminal emulator software needs to be installed.

It is also recommended that the intended audience of this document is familiar with IP / HTTP technology and has experience in setting up OS application service.

### 13.7.1 LLDP, LLDP-MED, and CDP

LLDP is used to exchange information between network equipment by advertising information about themselves to the link partners at each interface. The link partners are called neighbors or remote devices. LLDP is defined in IEEE 802.1AB.

LLDP-MED is an extension to the LLDP standard defined in TIA1057. An LLDP-MED enabled device is capable of conveying its capability and configuration to neighbors to guarantee the consistent attributes for the same media service or application across the network.

CDP is a proprietary protocol that runs over Layer 2 (the data link layer) to automatically discover and learn about other devices connected to the network. When CDP awareness is enabled, CDP frames are transformed into LLDP information and added to the neighbor entries table. LLDP will not actively transmit CDP PDUs.

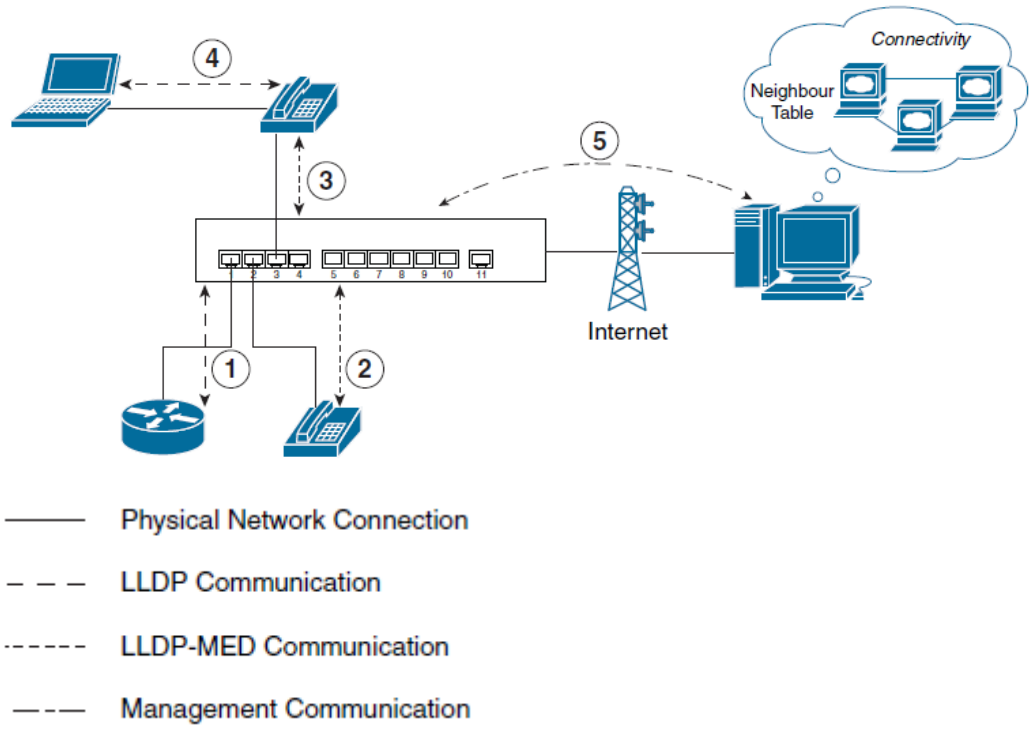
### 13.7.2 LLDP Operation and Configuration

LLDP enables directly connected devices to discover information about each other. It advertises information about the device itself at each interface, allowing other devices in the LAN to learn everything about their peers. Common deployed applications that use the information conveyed by LLDP include the following:

- Network topology - Network management system can accurately represent a map of the network topology.
- Emergency service - Not only to determine the device location, but also to setup ELIN used for emergency calling. According to the gathered information, public resource coordination for emergency service may also be done.
- VLAN configuration - The device can tell the peers which VLAN could be used for streaming services.
- Power negotiation - When the device also supports PoE, the connected equipment and the device can negotiate the expected power consumption.

With this capability in the network, automatic device discovery is very helpful for network administration and easy for streaming application deployment. The following figure illustrates the basic concept of an LLDP operation.

Figure LLDP Operations




Using LLDP reduces network administration effort by simply connecting the network equipment. In the preceding illustration, one VoIP phone and a laptop are connected in a chain to share the same port on a device that supports LLDP, while another VoIP phone and network equipment are connected to other ports on the same device.

1 When the network equipment is connected, LLDP communication starts and it is recognized as a neighbor that provides networking capability.
2 When the IP phone is connected, LLDP recognizes this neighbor is capable of running VoIP application by exchanging LLDP-MED information. Further, the switch might then be able to reserve power (PoE) if the corresponding setting is configured on both IP phone and switch.
3 LLDP recognizes another IP phone is connected and records its information in neighbor table.
4 When the laptop is connected to the phone, LLDP starts among laptop and phone and switch at the same time, even they may not be physically adjacent.
5 The management system, from either local or remote connection, can now query the device to explore the actual network topology.

LLDP also provides the configurable parameters used for transmitting LLDP PDU, which contains multiple TLVs. The following table shows the basic LLDP parameters and their corresponding descriptions.

Table 1 • LLDP parameters

| Parameters | Description |
|---|---|
| Tx Interval | The switch periodically transmits LLDP frames to its neighbors for having the network discovery information up-to-date. The interval between each LLDP frame is determined by this value, in seconds. |

| | |
|---|---|
| Tx Hold | Each LLDP frame contains information about how long time the information in the LLDP frame shall be considered valid. The LLDP information valid period is set to Tx Hold multiplied by Tx Interval seconds. |
| Tx Delay | If the system configuration is changed (e.g. the IP address) a new LLDP frame is transmitted, but the time between the LLDP frames will always be at least the value of Tx Delay seconds. Tx Delay cannot be larger than ¼ of the Tx Interval value. |
| Tx Re-Initialization | When a port is disabled, LLDP is disabled or the switch is rebooted, a LLDP shutdown frame is transmitted to the neighboring units, signaling that the LLDP information isn't valid anymore. Tx Re-Initialization controls the amount of seconds between the shutdown frame and a new LLDP initialization. |
| Port Description | Optional TLV: Port description will be included in LLDP information transmitted. |
| System Name | Optional TLV: System name will be included in LLDP information transmitted. |
| System Description | Optional TLV: System description will be included in LLDP information transmitted. |
| System Capability | Optional TLV: System capability will be included in LLDP information transmitted. |
| Management Address | Optional TLV: Management address will be included in LLDP information transmitted. |

In addition to the basic system information about the network equipment, the optional information regarding specific application can be distributed by LLDP devices that support "Configuring LLDP-MED".

## Configure LLDP

LLDP is enabled by default (doing both Tx and Rx for LLDPDU) on all the switch ports. The LLDP setup is thus limited to making sure that the LLDP parameter and system TLV are configured as expected. The following is a quick summary of the steps.

6 Enable LLDP on the specific port(s).
7 Set up per port LLDP system TLV to be advertised, if necessary.
8 Set up global LLDP Tx parameters, if necessary.
9 Save the configuration, if needed.

The following table shows the default LLDP settings and their configurable value range.

Table 2 • Default LLDP Settings and Configurable Value Range

| **Parameters** | **Default** | **Configurable Range** |
|---|---|---|
| Tx Interval | 30s | 5 - 32768 seconds |
| Tx Hold | 4 times | 2 -10 times |

| | | |
|---|---|---|
| Tx Delay | 2s | 1-8192s |
| Tx Re-Initialization | 2s | 1 - 10 seconds |
| Port LLDP Administration | Tx and RX | Send, receive, send and receive, neither receive nor send. |
| Port Tx Port Description | True | True or False |
| Port Tx System Name | True | True or False |
| Port Tx System Description | True | True or False |
| Port Tx System Capability | True | True or False |
| Port Tx Management Address | True | True or False |

## LLDP Setup using ICLI

The following table shows the steps used to set up LLDP using ICLI.

Table 3 • LLDP Setup Using ICLI

| Step | Action | Purpose |
|---|---|---|
| 1 | Configure terminal.<br>Example<br>**# configure terminal**<br>**(config)#** | Enter global configure mode. |
| 2 | **interface interface-id**<br>Example<br>**(config)# interface * (config-if)#** | Specifies the interface for configuring LLDP, and enters interface configuration mode. |
| 3 | **lldp transmit**<br>Example<br>**(config-if)# lldp transmit**<br>**(config-if)#** | Enable/Disable transmission of LLDP frames. |
| 4 | **lldp receive**<br>Example<br>**(config-if)# lldp receive**<br>**(config-if)#** | Enable/Disable decoding of received LLDP frames. |
| 5 | **lldp tlv-select {management-address \| port-description \| system-capabilities \| system-description \| system-name}**<br>Example<br>**(config-if)# lldp tlv-select system-name**<br>**(config-if)#** | Enable/Disable transmission of optional system TLV. |
| 6 | **exit**<br>Example<br>**(config-if)# exit**<br>**(config)#** | Exits from interface configuration mode and returns to global configuration mode. |
| 7 | **lldp timer seconds**<br>Example<br>**(config)# lldp timer 30** | Sets LLDP Tx interval (The time between each LLDP frame transmitted in seconds). |

| Step | Action | Purpose |
|---|---|---|
| | **(config)#** | |
| 8 | **lldp holdtime seconds**<br>Example<br>**(config)# lldp holdtime 4 (config)#** | Sets LLDP hold time (The neighbor switch will discard the LLDP information after hold time multiplied by timer seconds). |
| 9 | **lldp transmission-delay seconds**<br>Example<br>**(config)# lldp transmission-delay 2 (config)#** | LLDP transmission delay (the amount of time that the transmission of LLDP frames will delayed after LLDP configuration has changed) in seconds. |
| 10 | **lldp reinit seconds**<br>Example<br>**(config)# lldp reinit 2 (config)#** | LLDP Tx re-initialization delay in seconds. |
| 11 | **End time**<br>Example<br>**(config)# end**<br>**#** | Returns to privileged EXEC mode. |
| 12 | **copy running-config startup-config**<br>Example:<br>**# copy running-config startup-config**<br>**#** | (Optional)<br>Saves settings in the configuration file. |

## 13.7.3 LLDP-MED Operation and Configuration

LLDP-MED provides a device with an additional ability for serving a specific application. Depending on LLDP-MED operation mode per interface, a device acts either as a connectivity device or an endpoint device on the designated port. The difference between working as a network connectivity device or an endpoint device is a matter of initializing the LLDP-MED TLVs transmission. A network connectivity device does not start LLDP-MED TLVs transmission until it has detected an endpoint device as link partner. An endpoint device starts LLDP-MED TLVs transmission at once.

To achieve these related properties, LLDP-MED defines an LLDP-MED fast start interaction between the protocol and the application layers on top of the protocol. Initially, a network connectivity device will only transmit LLDP TLVs in an LLDPDU. Only after an LLDP-MED endpoint device is detected, will an LLDP-MED capable network connectivity device start to advertise LLDP-MED TLVs in outgoing LLDPDUs on the associated port. To share LLDP-MED information as quickly as possible, the LLDP-MED application will temporarily speed up the transmission of the LLDPDU to start within a second when a new LLDP-MED neighbor has been detected.

Because there is a risk of an LLDP frame being lost during transmission between neighbors, it is recommended to repeat the fast start transmission multiple times to increase the possibility of the neighbors receiving the LLDP frame. With fast start repeat count it is possible to specify the number of times the fast start transmission is repeated.

LLDP-MED and the LLDP-MED fast start are only intended to run on links between LLDP-MED network connectivity devices and endpoint devices, and as such does not apply to links between LAN infrastructure elements, including network connectivity devices, or other types of links.

The following four major additional abilities are supported by the LLDP-MED.

1 Capability discovery - Enables endpoints to determine the capabilities supported by the connected device. It can also be used to indicate type of the connected device (a phone, a switch, a wireless router, etc.).
2 Location identification discovery - Enables the network equipment (mainly IP phones) to be aware of its location information that can be used for location based applications, especially the emergency services.
3 Network policy discovery - Provides a mechanism for a switch to notify a connected equipment the VLAN ID that the equipment should use. The equipment can plug into any switch, obtain its VLAN ID, and then start communications.
4 Power discovery - Enables two direct connected devices to convey power information, when PoE is introduced, because the switch with PoE capability provides power to the connected equipment.

The following table shows the supported location identification optional TLVs for LLDP-MED.

Table 4 • Supported Location Identification Optional TLVs for LLDP-MED

| **Optional TLV** | **Description** |
|---|---|
| ELIN Address | Emergency call service ELIN identifier, which is used during emergency call setup to a traditional CAMA or ISDN trunk-based PSAP. |
| Country Code | The two-letter ISO 3166 country code in capital ASCII letters. |
| State | National subdivisions (state, canton, region, province, prefecture). |
| County | County, parish, gun (Japan), district. |
| City | City, township, shi (Japan). |
| City District | City division, borough, city district, ward, chou (Japan). |
| Block (Neighborhood) | Neighborhood, block. |
| Street | Street |
| Street Direction | Leading street direction |
| Trailing Street | Trailing street suffix. |
| Street Suffix | Street suffix |
| House No. | House number |
| House No. Suffix | House no. suffix. |

| Optional TLV | Description |
|---|---|
| Landmark | Landmark or vanity address. |
| Additional | Location Info. Additional Location Info. |
| Name | Name (residence and office occupant). |
| Zip Code | Zip code. |
| Building | Building (structure). |
| Apartment | Unit (Apartment, suite). |
| Floor | Floor. |
| Room No. | Room number. |
| Place Type | Place type. |
| Postal Community Name | Postal community name. |
| P.O. Box | P.O. Box |
| Additional | CodeAdditional code. |

The following table shows the supported network policy optional TLVs for LLDP-MED.

Table 5 • Supported Network Policy Optional TLVs for LLDP-MED

| Optional TLV | Description |
|---|---|
| Datum | Specify the geodetic system to be used: WGS84, NAD83/NAVD88 and NAD83/MLLW. |
| Latitude | Latitude degrees (within 0-90 degrees) in either north of the equator or south of the equator. |
| Longitude | Longitude degrees (within 0-180 degrees) in either east of the primmeridian or west of the prime meridian. |
| Altitude | Altitude value based on the altitude type (meter or floor). |
| ELIN Address | Emergency call service ELIN identifier, which is used during emergency call setup to a traditional CAMA or ISDN trunk-based PSAP. |
| Country Code | The two-letter ISO 3166 country code in capital ASCII letters. |
| State | National subdivisions (state, canton, region, province, prefecture). |
| County | County, parish, gun (Japan), district. |
| City | City, township, shi (Japan). |
| City District | City division, borough, city district, ward, chou (Japan). |
| Block (Neighborhood) | Neighborhood, block. |
| Street | Street |
| Street Direction | Leading street direction |
| Trailing Street | Trailing street suffix. |
| Street Suffix | Street suffix |
| House No. | House number |
| House No. Suffix | House no. suffix. |

| Optional TLV | Description |
|---|---|
| Landmark | Landmark or vanity address. |
| Additional Location Info. | Additional Location Info. |
| Name | Name (residence and office occupant). |
| Zip Code | Zip code. |
| Building | Building (structure). |
| Apartment | Unit (Apartment, suite). |
| Floor | Floor. |
| Room No. | Room number. |
| Place Type | Place type. |
| Postal Community Name | Postal Community Name |
| P.O. Box | P.O. Box |
| Additional | CodeAdditional code. |

The following table shows the supported network policy optional TLVs for LLDP-MED.

Table 6 • Supported Network Policy Optional TLVs for LLDP-MED

| Optional TLV | Description |
|---|---|
| Media Application Type | The specific application types handled are as follows: Voice, Guest Voice, Softphone Voice, Video Conferencing, Streaming Video and Control / Signaling (conditionally support a separate network policy for the media types above). |
| VLAN ID | VLAN identifier (VID) for the port as defined in IEEE 802.1Q. It is valid only when policy is using a ‘tagged’ VLAN. |
| Tag | Tag indicating whether the specified application type is using a 'tagged' or an 'untagged' VLAN. |
| L2 Priority | 802.1p CoS value used to prioritize the specified application. |
| DCP | DSCP value to be used to provide Diffserv node behavior for the specific application. |

A network policy is intended for use with applications that have specific, real-time network policy requirements such as interactive voice and/or video services. It is potentially advertised and associated with multiple sets of application types supported on a given port.

## Configuring LLDP-MED

The LLDP-MED defaults support four kinds of discovery options: Capability, Location Identification, Network Policy, and Power. They also default to transmit capabilities, network policy, and location TLVs in LLDP-MED message exchanges. LLDP needs to be enabled to handle protocol messages before setting LLDP-MED. The following is a

quick summary of the steps, and it is assumed LLDP is enabled and functional. For information about LLDP configuration, see LLDP-MED Operation and Configuration.

## Capability Discovery

1 Enable capability discovery on specific interface(s).
2 Configure per interface LLDP-MED device type, if necessary.
3 Save the configuration, if needed.

## Location Identification Discovery

1 Configure fast start repeat count for LLDP-MED.
2 Configure geodetic system settings.
3 Configure ELIN address for emergency service, if necessary.
4 Configure location information settings.
5 Enable location identification discovery on specific interface(s).
6 Setup per interface LLDP-MED device type, if necessary.
7 Save the configuration, if needed.

## Network Policy Discovery

1 Create network policy for the expected application type.
2 Associate the created network policy with selected interface(s).
3 Enable network policy discovery on specific interface(s).
4 Configure per interface LLDP-MED device type, if necessary.
5 Save the configuration, if needed.

## Power Discovery

PoE has to be enabled to cooperate with LLDP-MED.

1 Enable power discovery on specific interface(s).
2 Save the configuration, if needed.

## Default Setting and Configurable Value Range

The following table shows the default LLDP-MED settings and their configurable value range.

Table 7 • Default LLDP-MED Settings and Configurable Value Range

| Parameters | Default | Configurable Range |
|---|---|---|
| Fast Start Repeat Count | 4 | 1 – 10 |
| Transmit TLVs | Feature network-policy & location | capabilities, network-policy and location |
| Map Datum Type | WGS84 | WGS84,NAD83/NAVD88 and NAD83/MLLW |
| Latitude Type | North | North or South |
| Latitude | 0 | 0.0000 – 90.0000 |
| Longitude Type | East | East or West |
| Longitude | 0 | 0.0000 – 180.0000 |
| Altitude Type | Meters | Meters or Floors |

| Parameters | Default | Configurable Range |
|---|---|---|
| Altitude | 0 | -2097151.9到2097151.9 |
| ELIN Address | Null string | String in 0 – 25 characters |
| Country Code | Null string | String in 0 – 2 characters |
| State | Null string | String in 0 – 250 characters |
| County | Null string | String in 0 – 250 characters |
| City | Null string | String in 0 – 250 characters |
| City District | Null string | String in 0 – 250 characters |
| Block (Neighborhood) | Null string | String in 0 – 250 characters |
| Street | Null string | String in 0 – 250 characters |
| Street Direction | Null string | String in 0 – 250 characters |
| Trailing Street | Null string | String in 0 – 250 characters |
| Street Suffix | Null string | String in 0 – 250 characters |
| House No. | Null string | String in 0 – 250 characters |
| House No. Suffix | Null string | String in 0 – 250 characters |
| Landmark | Null string | String in 0 – 250 characters |
| Additional Location Info. | Null string | String in 0 – 250 characters |
| Name | Null string | String in 0 – 250 characters |
| Zip Code | Null string | String in 0 – 250 characters |
| Building | Null string | String in 0 – 250 characters |
| Apartment | Null string | String in 0 – 250 characters |
| Floor | Null string | String in 0 – 250 characters |
| Room No. | Null string | String in 0 – 250 characters |
| Place Type | Null string | String in 0 – 250 characters |
| Postal Community | Null string | String in 0 – 250 characters |
| P.O. Box | Null string | String in 0 – 250 characters |
| Additional Code | Null string | String in 0 – 250 characters |
| Network Policy ID | N/A | 0 – 31 |
| Media Application Type | voice | voice<br>voice-signaling<br>guest-voice<br>guest-voice<br>signaling soft<br>phone-voice<br>video-conferencing<br>streaming-video<br>video-signaling |
| VLAN ID | 1 | 1 – 4095 |
| Tag | Tagged | Tagged or Untagged. |
| L2 Priority | 0 | 0 – 7 |
| DSCP | 0 | 0 – 63 |
| Port MED Device Type | Connectivity | Connectivity or endpoint |

| Parameters | Default | Configurable Range |
|---|---|---|
| Port MED Optional TLV | Capabilities & location & network-policy & poe | Capabilities location network-policy poe |
| Port Policy List | N/A | Created network policy ID |

## LLDP-MED Setup using ICLI

The following table shows the steps used to set up LLDP-MED using ICLI.

Table 8 • Setting up LLDP-MED Using ICLI

| Step | Action | Purpose |
|---|---|---|
| 1 | **configure terminal**<br>Example<br>**# configure terminal (config)#** | Enter global configure mode. |
| 2 | **lldp med fast counts**<br>Example<br>**(config)# lldp med fast 4 (config)#** | Specifies the fast start repeat count for LLDP-MED. |
| 3 | **lldp med datum {nad83-mllw \| nad83-navd88 \| wgs84}**<br>Example<br>**(config)# lldp med datum wgs84 (config)#** | Specifies the geodetic system type. |
| 4 | **lldp med location-tlv**<br>**{**<br>**elin-addr string \|**<br>**latitude {north \| south} degrees \|**<br>**longitude {east \| west} degrees \|**<br>**altitude {meters \| floors} values**<br>**}**<br>Example<br>**(config)# lldp med location-tlv altitude meters 0 (config)#** | Assign the geographic coordinate value for the device. Also, the ELIN identification could be specified. |
| 5 | **lldp med location-tlv civic-addr**<br>**{**<br>**additional-code string \|**<br>**additional-info string \| apartment string \|**<br>**block string \| building string \| city string**<br>**\| country string \| county string \|**<br>**district string \| floor string \|**<br>**house-no string \| house-no-suffix string \|**<br>**landmark string \|** | Specifies civic location information. |

| Step | Action | Purpose |
|---|---|---|
| | **leading-street-direction string \| name string \| p-o-box string \| place-type string \| postal-community-name string \| room-number string \| state string \| street string \| street-suffix string \| trailing-street-suffix string \| zip-code string }**<br>Example<br>**(config)# lldp med location-tlv civic-addr country TW (config)# lldp med location-tlv civic-addr zip-code 30055 (config)# lldp med location-tlv civic-addr house-no-suffix 23F, 2B (config)#** | |
| 6 | **lldp med media-vlan-policy policy-id { guest-voice \| guest-voice-signaling \| softphone-voice \| streaming-video \| video-conferencing \| video-signaling \| voice \| voice-signaling }**<br><br>**{ tagged vlan-id [l2-priority cos] \| untagged }**<br>**[dscp dscp]**<br>Example<br>**(config)# lldp med media-vlan-policy 0 streaming-video untagged (config)# lldp med media-vlan-policy 1 voice tag 1 23 l2-priority 3 dscp 21 (config)#** | Creates a network policy that can be assigned to an interface for a specific kind of application. |
| 7 | **interface interface-id**<br>Example<br>**(config)# interface 10GigabitEthernet 1/2 (config-if)#** | Specifies the interface for setting LLDP-MED, and enters interface configuration mode. |
| 8 | **lldp med type {connectivity \| end-point}**<br>Example<br>**(config-if)# lldp med type connectivity (config-if)#** | Selects either Network Connectivity Device or an Endpoint Device as the interface role. |

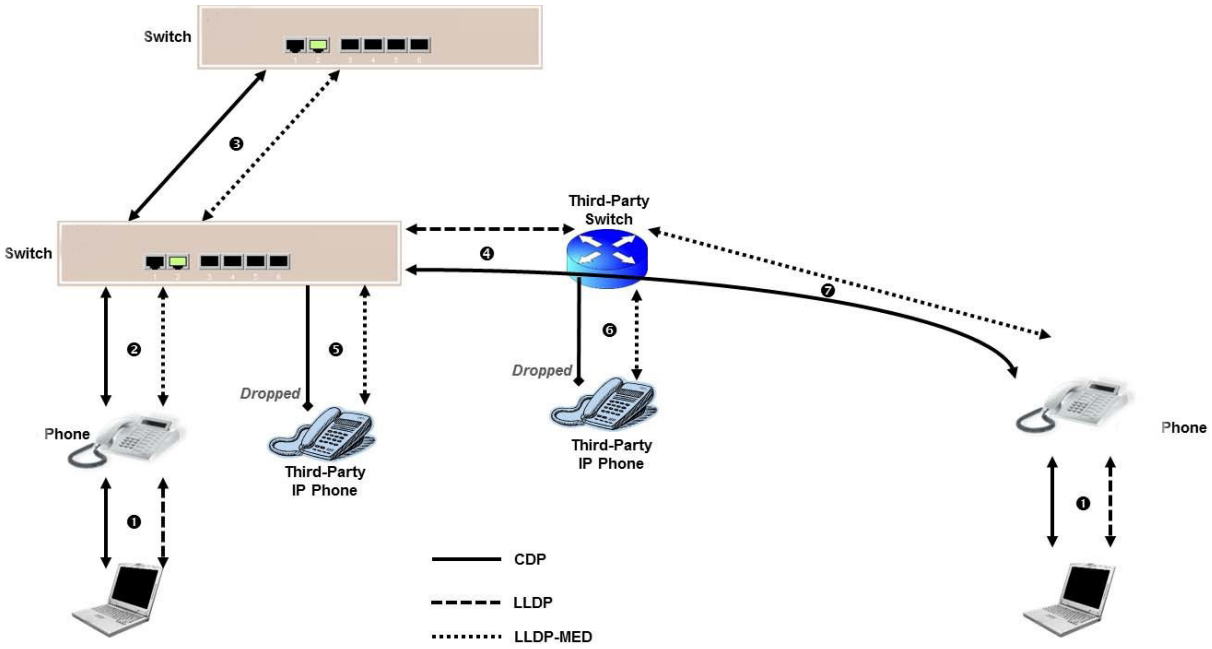
| Step | Action | Purpose |
|---|---|---|
| 9 | **lldp med transmit-tlv {capabilities \| location \| network-policy \| poe}**<br>Example<br>**(config-if)# lldp med transmit-tlv capabilities location network-policy poe (config-if)#** | Specifies the optional TLVs to be transmitted. |
| 10 | **lldp med media-vlan policy-list policy-range**<br>Example<br>**(config-if)# lldp med media-vlan policy-list 0-1 (config-if)#** | Specifies the media policy that an interface will apply. |
| 11 | **End time**<br>Example<br>**(config-if)# end**<br>**#** | Returns to privileged EXEC mode. |
| 12 | **copy running-config startup-config**<br>Example<br>**# copy running-config startup-config**<br>**#** | (Optional)<br>Saves settings in the configuration file. |

## 13.7.4 CDP Operation and Configuration

CDP is an L2 proprietary discovery protocol for all CDP devices (routers, bridges, access servers, and switches). It provides the similar concept in using LLDP for network management applications to discover devices that are neighbors of already known devices. For more information, see documents for the current CDP capabilities.

LLDP is CDP-aware. It only identifies a device connected to a device and makes it a neighbor. The following figure from a technical white paper illustrates how CDP works.

Figure CDP Operations




The following steps describe how CDP works.

1 A laptop connected to a phone can support CDP. Some applications running on that PC (example VT Advantage) also support CDP. The phone therefore uses CDP to support these applications.
2 Both the switch and the phone exchange CDP messages.
3 Both switches exchange CDP and LLDP messages.
4 The switch exchanges LLDP messages with the third-party switch but still advertises CDP messages. In this case, the third-party switch usually ignores CDP messages and floods the CDP messages to other interfaces, meaning devices connected to the third-party switch receive CDP messages from the switch as if they are directly connected to the switch. Recommends turning off CDP on the port connected to the third-party switch that guarantees application's functionality to a certain extent.
5 A third-party phone drops CDP messages from the switch but exchanges the LLDP-MED messages with the switch.
6 A third-party phone drops CDP messages flooded by the third-party switch and only exchanges the LLDP-MED messages with the third-party switch.
7 A phone generates both CDP and LLDP-MED messages. The third-party switch again ignores CDP messages and floods them out to other interfaces. However, the third-party switch still exchanges LLDP-MED messages with the connected phone. Again, recommends turning off CDP on the switch's port connected to the third-party switch.

## Configuring CDP

LLDP is only aware of the existence of devices upon receiving CDP messages. The CDP operation is restricted to decoding incoming CDP frames, and CDP frames are only decoded if LLDP on the port is enabled.

If all ports have CDP awareness disabled, the device forwards CDP frames received from neighbor devices. If at least one port has CDP awareness enabled, all CDP frames are terminated by the device.

Only CDP TLVs that can be mapped to a corresponding field in the LLDP neighbors' table are decoded. All other TLVs are discarded (Unrecognized CDP TLVs and discarded CDP frames are not shown in the LLDP statistics.). CDP TLVs are mapped into LLDP neighbors table, as follows:

- CDP TLV “Device ID” is mapped to the LLDP “Chassis ID” field.
- CDP TLV "Address" is mapped to the LLDP "Management Address" field. The CDP address TLV can contain multiple addresses, but only the first address is shown in the LLDP neighbors table.
- CDP TLV "Port ID" is mapped to the LLDP "Port ID" field.
- CDP TLV "Version and Platform" is mapped to the LLDP "System Description" field.
- Both the CDP and LLDP support "system capabilities", but the CDP capabilities cover capabilities that are not part of the LLDP. These capabilities are shown as "others" in the LLDP neighbors' table.

  Note:
  When CDP awareness on an interface is disabled, the CDP information is not removed immediately, but gets removed when the hold time is exceeded.

The following steps summarize the process of configuring CDP.

1 Enable LLDP on the specific interface(s).
2 Enable CDP awareness for the specific interface(s).
3 Save the configuration, if needed.

## Default Setting and Configurable Value Range

The following table shows the default CDP settings and their configurable value range.

Table 9 • Default CDP Settings and Configurable Value Range

| Parameters | Default | Configurable Range |
|---|---|---|
| Per Port LLDP Administration | Tx and RX | Tx, Rx, Tx and Rx, Disabled |
| CDP Awareness | Error | True or False |

## CDP Setup using ICLI

The following table shows the steps used to set up CDP using ICLI.

Table 10 • Setting up CDP using ICLI

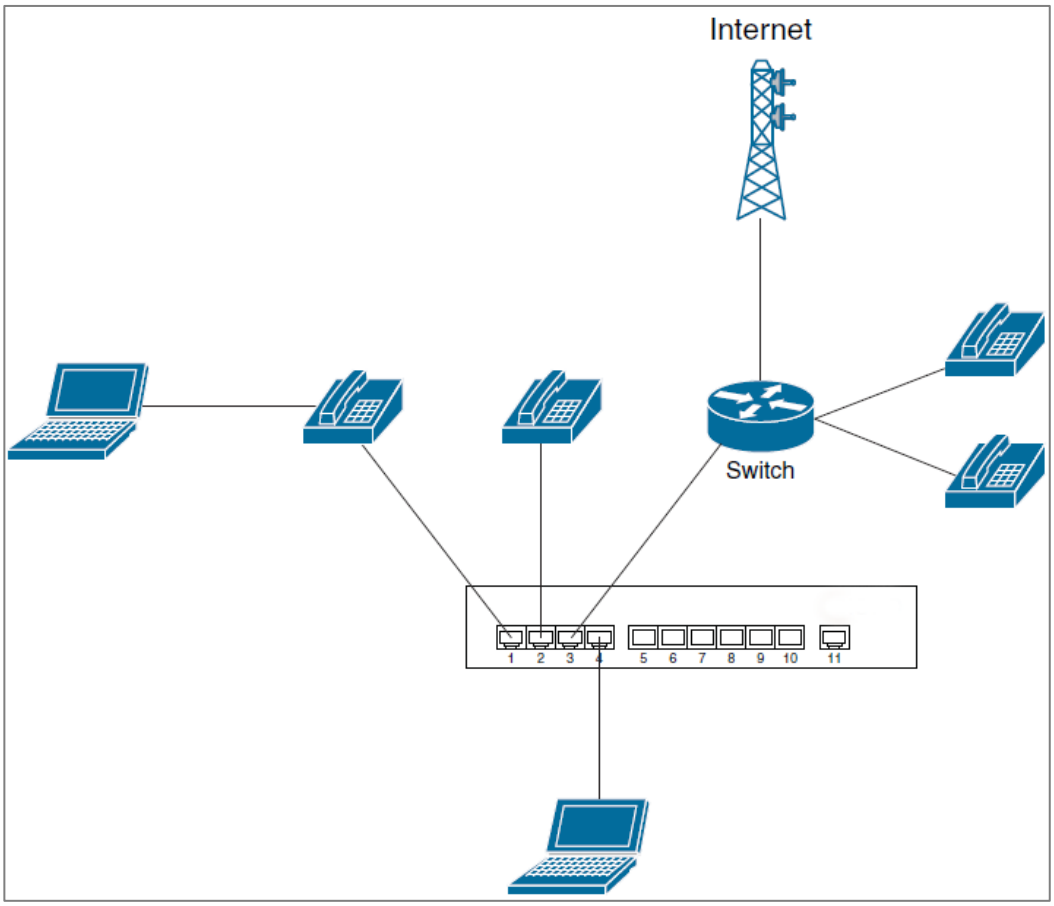
| Step | Action | Purpose |
|---|---|---|
| 1 | **configure terminal**<br>Example<br>**# configure terminal**<br>**(config)#** | Enter global configure mode. |
| 2 | **interface interface-id**<br>Example<br>**(config)# interface * (config-if)#** | Specifies the interface for enabling LLDP, and enters interface configuration mode. |

| | | |
|---|---|---|
| 3 | **lldp cdp-aware**<br>Example<br>**(config-if)# lldp cdp-aware**<br>**(config-if)#** | Specifies if the interface is CDP aware. |
| 4 | <br>Example<br>**(config-if)# end** | Returns to privileged EXEC mode. |
| 5 | **copy running-config startup-config**<br>Example<br>**# copy running-config startup-config #** | (Optional)<br>Saves settings in the configuration file. |

## 13.7.5 Topology Example

The following topology illustration is used to demonstrate the examples, which assume the device boots up with default configurations.

Figure Topology Example



## Deploy IP Telephony Network using ICLI

The major goal in setting up the IP telephony network is to prioritize the voice data among phones, software, or hardware.

```
# configure terminal
(config)# lldp med media-vlan-policy 0 voice tagged 111 l2-priority 7 dscp 5
(config)# lldp med media-vlan-policy 1 softphone-voice untagged dscp 5
(config)# interface GigabitEthernet 1/1-4
(config-if)# lldp med type connectivity
(config-if)# lldp med transmit-tlv capabilities network-policy
(config-if)# interface GigabitEthernet 1/1-3
(config-if)# lldp med media-vlan policy-list 0
(config-if)# interface GigabitEthernet 1/4
(config-if)# lldp med media-vlan policy-list 1
(config-if)# end
#
```

# 13.8 Ring

Ring is a private protocol that can't realize communication with other manufacturers' devices. Ring is an Ethernet Ring network algorithm developed and designed for highly reliable industrial control network applications that require link redundancy backup. its design concept is completely in accordance with international standards (RSTP and RSTP) implementation, and do the necessary for industrial control application optimization, with Ethernet link redundancy, fault fast automatic recovery ability.

Ring adopts the design of no master station. The devices running the Ring protocol discover the loop in the network by exchanging information with each other, and block a certain port. Finally, the ring network structure is trimmed into a tree network structure without loop, thus preventing messages from circulating continuously in the ring network, and avoiding the reduction of processing capacity caused by repeated reception of the same message. In a multi-Ring network composed of 250 switches, when the network is interrupted or fails, the ring can ensure that the user network automatically resumes link communication within 20 ms.

## Global Configuration

Enable the Ring network.

```
# configure terminal
(config)# ring
```

Disable the Ring network.

```
# configure terminal
(config)# no ring
```

### Ring Configuration

Single ring Configuration

```
# configure terminal
(config)# ring group <group-id> <ring-id> single <port1> <port2>
<hello-time> (master | slave)
```

In a single Ring, Ring supports master/slave and no master configuration to meet various network environment requirements. When all devices are configured in Slave mode, the single ring has no master station structure, that is, there is no designated backup link. When a device is designated to be configured in master mode, the device serves as the master device, and the single-ring network in which it is located has a master station structure; Other single-ring devices need to be configured in Slave mode and serves as the slave device

Link / coupling ring / dual homing network configuration.

```
# configure terminal
(config)# ring group <group-id> <ring-id> (chain | couple |
dualhoming) <port1> <port2> <hello-time>
```

### Network ID

When multiple switches form a ring, the current ring ID would be network ID. Different ring network has different ID. The ring network identification must remain the same in one ring network.

### Ring Port

Port that can be used for the formation of ring network in switch. In a coupling ring, the coupling port is the port connected to the different network identifiers, and the control port is the port in the link where the two rings meet.

### Hello-time

The sending cycle of hello-time packet, ranging from 0-300(*100ms), and 0 means not to send.

## 13.9 Loop Protection

Loop protection periodically sends a detection message from the interface to check whether the message is returned to the device, and then determines whether there are loops between the interface, the device's underlying network or the device, or between the two interfaces of the device. After a loop is detected, the device sends a trap to the NMS and records a log, and takes a preconfigured action on the looped

interface (the interface is shut down by default) to minimize impact of the loop on the device and entire network.

## Global Configuration

Enable loop protection.

```
# configure terminal
(config)# loop-protect
```

Disable loop protection.

```
# configure terminal
(config)# no loop-protect
```

## Transmission Time

The time interval of transmitting loop detection packet, unit: second.

```
# configure terminal
(config)# loop-protect transmit-time <1-10>
```

## Shutdown Time

After detecting the loop, enable the loop protection and disable the port time, unit: second. 0 means disabling the port.

```
# configure terminal
(config)# loop-protect shutdown-time  <0-604800>
```

## Port Configuration

Enable port loop protection.

```
# configure terminal
(config)# interface GigabitEthernet 1/1
(config-if)# loop-protect
```

Disable port loop protection.

```
# configure terminal
(config)# interface GigabitEthernet 1/1
(config-if)# no loop-protect
```

## Action

The processing methods of the interface after the loop is detected, such as log alarm and close the port.

```
# configure terminal
(config)# interface GigabitEthernet 1/1
(config-if)# loop-protect action ?
   log        Generate log
```

```
   shutdown    Shutdown port
```

### Tx Mode

Controls whether the port is actively generating loop protection PDU's, or whether it is just passively looking for looped PDU's.

```
# configure terminal
(config)# interface GigabitEthernet 1/1
(config-if)# loop-protect tx-mode
```

## 13.10DHCP Server

A DHCP server assigns IP addresses from specified address pools to DHCP clients. It can also manage these clients and provide network parameters such as the default gateway address, Domain Name System (DNS) server address, and Windows Internet Name Service (WINS) server address. A DHCP server can accept broadcasts from locally attached LAN segments or DHCP requests forwarded by DHCP relay agents within the network.

### Global Configuration

Enable DHCP Server.

```
# configure terminal
(config)# ip dhcp server
```

Enable DHCP server on VLAN interface.

```
# configure terminal
(config)# interface vlan 1
(config-if-vlan)# ip dhcp server
```

### Reserve IP Address Configuration

DHCP server will not allocate these excluded IP addresses to DHCP client.

```
# configure terminal
(config)# ip dhcp excluded-address <ipv4_addr>
```

### Address Pool

According to the DHCP pool, DHCP server will allocate IP address and deliver configuration parameters to DHCP client.

```
# configure terminal
(config)# ip dhcp pool 1
(config-dhcp-pool)# ?
   broadcast            Broadcast address in use on the client's
subnet
```

```
   client-identifier     Client identifier
   client-name           Client host name
   default-router        Default routers
   dns-server            DNS servers
   do                   To run exec commands in the configuration
mode
   domain-name           Domain name
   end                  Go back to EXEC mode
   exit                 Exit from current mode
   file                 Boot file name (option 67)
   hardware-address      Client hardware address
   help                 Description of the interactive help system
   host                 Client IP address and mask
   lease                Address lease time
   netbios-name-server   NetBIOS (WINS) name servers
   netbios-node-type     NetBIOS node type
   netbios-scope         NetBIOS scope
   network              Network number and mask
   nis-domain-name       NIS domain name
   nis-server           Network information servers
   no                   Negate a command or set its defaults
   ntp-server            NTP servers
   option               DHCP option parameters field.
   sname                Optional server host name (option 66)
   vendor               Vendor configuration
```

# 13.11DHCP Snooping

DHCP Snooping is a security feature of DHCP (Dynamic Host Configuration Protocol) that ensures that DHCP clients receive IP addresses from valid DHCP servers and records the corresponding relationship between IP address of DHCP client and MAC address to prevent DHCP attack on network.

## Snooping Mode

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

```
# configure terminal
```

```
(config)# ip dhcp snooping
```

### Port Mode Configuration

Trusted: Configures the port as trusted source of the DHCP messages.

```
# configure terminal
(config)# interface GigabitEthernet 1/1
(config-if)# ip dhcp snooping trust
```

## 13.12DHCP Relay

DHCP relay agent forwards DHCP messages between a DHCP server and DHCP clients, and helps the DHCP server to dynamically allocate network parameters to the DHCP clients.

When a DHCP client broadcasts request messages with the destination IP address 255.255.255.255, only the DHCP server on the same network segment as the DHCP server can receive the request messages. If a DHCP server is on a different network segment from the DHCP client, the DHCP server can not receive request messages from the DHCP client, a DHCP relay agent must be deployed to forward DHCP messages to the DHCP server. Different from traditional IP message forwarding, the DHCP relay agent modifies the format of a message to generate a new DHCP message and then forwards it after receiving DHCP request or respond message.

### Relay Mode

When DHCP relay mode operation is enabled, the agent forwards and transfers DHCP messages between the clients and the server when they are not in the same subnet domain. And the DHCP broadcast message won't be flooded for security considerations.

```
# configure terminal
(config)# ip dhcp relay
```

### Relay Information Mode

When DHCP relay information mode operation is enabled, the agent inserts specific information (option 82) into a DHCP message when forwarding to DHCP server and removes it from a DHCP message when transferring to DHCP client.

```
# configure terminal
(config)# ip dhcp relay information option
```

### Relay Information Policy

When DHCP relay information mode operation is enabled, if the agent receives a DHCP message that already contains relay agent information it will enforce the policy.

- Replace: Replace the original relay information when a DHCP message that already contains it is received.

- Keep: Keep the original relay information when a DHCP message that already contains it is received.
- Drop: Drop the package when a DHCP message that already contains relay information is received.

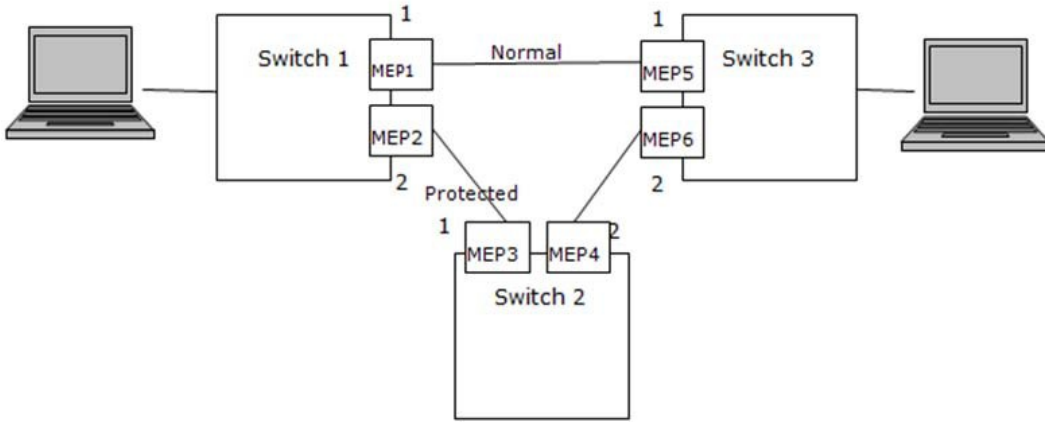
```
# configure terminal

(config)# ip dhcp relay information policy ?

   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
```

# 14 Ethernet Ring Protection Switching Configuration

## 14.1 Introduction

This document shows how to configure the Ethernet Ring Protection Switching (ERPS) for switches using the ICLI commands. The following figure builds a simple network of 3 switches to demonstrate these functions.

Figure Ethernet Ring Protection Switching (ERPS) Model




## 14.2 Configuring ERPS from the ICLI

### Initial Switch Configuration

The following command disables STP.

```
#Configure port 1-2
(config)# interface GigabitEthernet 1/1-2
(config-if)#switchport mode hybrid
#disable Spanning Tree Protocol
(config-if)#no spanning-tree
```

## Configuring MEP and ERPS on Switch 1 (RPL Owner)

```
#create mep 1 on port 1
(config)# mep 1 down domain port flow 1 level 0 interface GigabitEthernet 1/1
#set vlan for MEP traffic
(config)# mep 1 vid 3001
#set id of peer mep mep 1 peer-mep-id 5
#enable ccm, default is 1FPS mep 1 cc 0
#enable RAPS
(config)# mep 1 aps 0 raps
(config)# mep 2 down domain port flow 2 level 0 interface GigabitEthernet 1/2
(config)# mep 2 mep-id 2
(config)# mep 2 vid 3001
(config)# mep 2 peer-mep-id 3
(config)# mep 2 cc 0
(config)# mep 2 aps 0 raps
#create erps on port 1 and port 2
(config)# erps 1 major port0 interface GigabitEthernet 1/1 port1 interface GigabitEthernet 1/2
#set MEP ID for the corresponding port
(config)# erps 1 mep port0 sf 1 aps 1 port1 sf 2 aps 2
#set to RPL owner
(config)# erps 1 rpl owner port1
#set protected VLAN
(config)# erps 1 vlan 1
```

## Configuring MEP and ERPS on Switch 2 (RPL Neighbor)

```
(config)# mep 1 down domain port flow 1 level 0 interface GigabitEthernet 1/1
(config)# mep 1 mep-id 3
(config)# mep 1 vid 3001
(config)# mep 1 peer-mep-id 2
(config)# mep 1 cc 0
(config)# mep 1 aps 0 raps
```

```
(config)# mep 2 down domain port flow 2 level 0 interface
GigabitEthernet 1/2
(config)# mep 2 mep-id 4
(config)# mep 2 vid 3001
(config)# mep 2 peer-mep-id 6
(config)# mep 2 cc 0
(config)# mep 2 aps 0 raps
(config)# erps 1 major port0 interface GigabitEthernet 1/1 port1
interface GigabitEthernet 1/2
(config)# erps 1 mep port0 sf 1 aps 1 port1 sf 2 aps 2
#set to RPL neighbour
(config)# erps 1 rpl neighbor port0
(config)# erps 1 vlan 1
```

## Configuring MEP and ERPS on Switch 3

```
(config)# mep 1 down domain port flow 1 level 0 interface
GigabitEthernet 1/1
(config)# mep 1 mep-id 5
(config)# mep 1 vid 3001
(config)# mep 1 peer-mep-id 1
(config)# mep 1 cc 0
(config)# mep 1 aps 0 raps
(config)# mep 2 down domain port flow 2 level 0 interface
GigabitEthernet 1/2
(config)# mep 2 mep-id 6
(config)# mep 2 vid 3001
(config)# mep 2 peer-mep-id 4
(config)# mep 2 cc 0
(config)# mep 2 aps 0 raps
(config)# erps 1 major port0 interface GigabitEthernet 1/1 port1
interface GigabitEthernet 1/2
(config)# erps 1 mep port0 sf 1 aps 1 port1 sf 2 aps 2
(config)# erps 1 vlan 1
```

Note:

On SWITCH. To set the CCM rate to 100FPS or 300FPS, the peer MAC address must be known as shown here as shown below: Or set it to lower rate first, until the peer

MAC address is learned, and then change it to a higher rate.

```
(config)# mep 1 peer-mep-id <peer mep id> mac <peer mac address>
mep 1 cc 0 fr300s
```

Finally, the ERPS status can be checked with the show erps command.

# 15 Configuring the Network Access Server and Access Control List

This document describes how to configure Network Access Server (NAS) and Access Control List (ACL) functionality within the Switch Application Software. Configuration can be performed by means of the Industrial Command Line Interface (ICLI).

## 15.1 Access Control List

The access control list (ACL) is controlled with the ICLI command access-list in the config- and interface config mode. For more information about config and interface config modes, see Understanding Modes and Sub-Modes. The basic configuration commands are as follows:

```
(config)# access-list …
```

and

```
(config-if)# access-list …
```

The following sections describe the three ACL configuration categories: port, rate limiter and access control list.

### Port

For each port, a rule can be configured for what should happen with an ingress packet. For the rule on a port to take effect, the packet in question must be associated with a policy ID. For now, we will assume that the policy ID is 0. This is the value a packet is associated with if no effort has been made to change that. For information about the policy ID, see "ECE Configuration Policy ID".

**Action** can be Permit or Deny. Permit means that packets received on that port are forwarded the normal way, whereas Deny means that packets are ejected. So if we set Action to Deny for port 1 with PolicyID=0, then no packets are switched through the system.

**Rate Limiter ID** can be Disabled or a number in the range of 1-16, which points to one of the 16 rate limiters instances. The rate limiter ID maps to a packets per second number, which defines the rate. For more information see "Rate Limiters".

**Port Redirect** specifies that packets matching the rule in question are redirected to a given port, or if Disabled should be forwarded the normal way, in which case the port redirect is disabled.

**Logging** specifies that packets matching the rule are logged. The packets can be displayed by the following ICLI command

```
# show logging
```

This shows a log with one item per incident. Use the following command to display the full information for incident 46.

```
# show logging 46
```

**Shutdown** specifies that when the rule is hit, then the port shall be shutdown.

**State** specifies whether the port is enabled or disabled. Changing it to Disable, turns the port off. If Shutdown is enabled and the rule is hit, then the system will change the value to Disable. Re-enable the port by changing it to Enable. It will stay enabled until the next time the rule is hit.

Counter tells how many times this rule has been hit.

Use the following ICLI commands to set up these rules from the interface-config mode.

```
(config-if)# access-list policy <PolicyID>
(config-if)# access-list action <deny | permit>
(config-if)# access-list rate-limit <1-16>
(config-if)# access-list redirect interface gi 1/2
(config-if)# [no] access-list logging
(config-if)# [no] access-list shutdown
(config-if)# access-list port-state
```

This command cannot be used to give several parameters in one line. Logging and shutdown is disabled with the **no** command.

The last of the commands are not in the web GUI. They are used to enable a port that has been shut down from when shutdown was enabled.

## Rate Limiters

Rate limiters map rate limiter IDs to a rate. The rate can be given in any of the following formats.

- Packets per second
- 100 pps (100 packets per second)
- 100 kbps (100 kilobits per second)

The rate limit ID is a number between 1 and 16.

The ICLI command for setting the rate limit can be one of the following:

```
(config)# access-list rate-limiter <1-16> pps <0-3276700>
(config)# access-list rate-limiter <1-16> 100kbps <0-10000>
```

where <1-16> represents the number 1 to 16. The rate is the last number times the unit.

## Access Control List

In the Ports section above, a list of rules, one per port, along with associated actions were defined. In this section more complicated rules will be described.

In this example the selected source MAC address shall be 00-00-00-00-00-12 and the destination MAC shall be broadcast. Also the EtherType shall be 0x9876. The VLAN ID shall be 2 and priority 2 or 3. So if an ingress packet on any port (since the Ingress Port is set to All) has these attributes, then it will match this rule. Upon a match the actions mentioned will be performed.

The ICLI command for building this rule is as follows. For clarity each element is placed one a separate line, but can be written on a single line.

```
(config)# access-list ace 1
vid 2
tag-priority 2-3
dmac-type broadcast
frame etype
etype-value 0x9876
smac 00-00-00-00-00-12
logging
```

This ACE entity has the number 1. This number is called the AceId, which can be in the range of 1-256.

```
(config)# access-list ace <AceId> …
```

The elements in the command can be in any order, except that ace <AceId> must come first.

When adding more than one rule, which likely will be the case, then the rules are parsed in some order. When a rule is added similar to the one above, it is put in the end of the list. So it will be the last rule to be checked, until another rule is added.

It is possible to specify where a rule shall be inserted in the hierarchy. This is done by specifying which rule shall come next. This is demonstrated as follows, assuming an empty ACL list.

```
(config)# access-list ace 20 vid 100
(config)# access-list ace 15 vid 101
(config)# access-list ace 25 vid 102 next 15
```

The first command will insert the aceID 20 into an empty list. It is the first and only element. The aceID 15 is then inserted at the end of the list to lead to the order 20, 15. The next 15 field in the third aceID inserts it before rule 15. The final rule ordering is 20, 25 and 15.

### ECE Configuration Policy ID

Policy ID was set to 0 in Ports (ignore), and any in Access Control List.

An ECE rule goes into the IS1, before the IS2 where the ACL rule resides. Therefore when the Policy ID in the Actions table is given some value for an ECE, that value can be used in ACLs.

The ICLI command is:

```
(config)# evc ece <EceId> policy <Policy ID> …
```

## 15.2 Network Access Server

### Types of NAS

This feature provides access control on a port basis. There are two types of authentication, namely IEEE 802.1X and MAC based. The 802.1X provide the following three kinds:

- Port based 802.1X
- Single 802.1X
- Multi 802.1X

The following three terms are used in the 802.1X context:

- Supplicant, client (PC) with some 801.1X software
- Authenticator, the switch
- Authentication server, e.g. a RADIUS server

So the supplicant/client is connected to the authenticator/switch on some port, and the authenticator can reach an authentication server.

The idea is that the supplicant wants access to the port, so it sends an Extensible Authentication Protocol over LAN (EAPoL) message to the authenticator, which in turn asks the authenticator server, if this supplicant can be accepted. If so, then the authenticator opens the port for the supplicant, and communication can begin. Depending on how the authenticator is configured, this process behaves in different ways.

### Port Based 802.1X

In this method if the supplicant, S, is on a network, N, which is connected to the authenticator on some port, A, then if S opens port A, then everyone on network N has access.

### Single 802.1X

This mode is similar to port based 802.1X, however in this case only the supplicant that did open the port on the authenticator is allowed to transmit and receive packets. This is done by means of the supplicant MAC address.

## Multi 802.1X

This mode is similar to single 802.1X, except here more than one supplicant can register on the port. One fine point here is that multicast packets are not sent to the supplicants from the switch.

## MAC Based Authentication

If one thinks of a supplicant as consisting of a client and of a supplicant component that takes care of negotiating the port opening when the client transmits the first packet, then MAC based authentication can be understood as multi 802.1X where the supplicant component is moved into the authenticator/switch. This embedded supplicant component then uses the MAC address of the client as the user name and password in the form aa-bb-cc-dd-ee-ff. This has the advantage that the client does not have to have supplicant software.

## Port Configuration

The four of them are described above. The remaining two are Force Authorized and Force Unauthorized. The first is the default, which means the port is open. The second means that there is no access.

The ICLI commands for changing admin state options are as follows:

```
(config-if)# dot1x port-control auto |
force-authorized |
force-unauthorized |
mac-based |
multi |
single
```

Note:

Auto means port based 802.1X as described in the following section.

## System Configuration

After the admin state has been set for the ports, the NAS feature has to be enabled on the switch or authenticator.

## Mode

Mode enables the NAS functionality globally. The corresponding ICLI command is as follows.

```
(config)# [no] dot1x system-auth-control
```

## Re-authentication Enabled

Re-authentication is enabled by the following ICLI command:

```
(config)# [no] dot1 re-authentication
```

The no variant disables it. This means that the supplicant is re-authenticated on a periodic basis. The period is the re-authentication period.

This parameter affects ports with port based 801.1X, single 802.1X, or multi 802.1X admin states.

If a supplicant does not re-authenticate, the authenticator releases the resources that were associated with it.

Note:

For MAC based authentication, similar functionality is provided by the aging period.

## Re-authentication Period

The re-authentication period is set by the following ICLI command:

```
(config)# [no] dot1x authentication timer re-authenticate <1-3600>
```

where <1-3600> is the time in seconds. The no variant sets it to the default, which is 3600 seconds. This attribute is associated with re-authentication enabled attribute.

## EAPOL Timeout

The EAPOL timeout is set by the following ICLI command:

```
(config)# [no] dot1x timeout tx-period <1-65535>
```

The no variant sets it to the default, which is 30 seconds.

This parameter affects ports with port based 801.1X, single 802.1X, or multi 802.1X admin states.

The EAPOL timeout is the re-transmission time for request identity EAPoL frames from the authenticator towards the supplicant.

## Aging Time

The aging period is set by the following ICLI command:

```
(config)# [no] dot1x authentication timer inactivity <10-1000000>
```

Default value is 300 seconds.

This parameter affects ports with single 801.1X, multi 802.1X, or MAC based authentication. In these cases, together with port based 802.1X, re-authentication handles the timeout, if enabled.

Aging is a kind of timeout for MAC based authentication. If a client has been registered by this method, and has not been heard from for greater than the aging period, then the authenticator releases the resources that were associated with it.

## Hold Time

The hold time is set by the following ICLI command:

```
(config)# [no] dot1x timeout quite-period <10-1000000>
```

Where the no variant sets the hold time to the default, which is 10 seconds.

This parameter affects ports with single 801.1X, multi 802.1X, or MAC based authentication.

If a supplicant or client is denied access, it will be held in an unauthorized state for the hold time.

## RADIUS

The RADIUS assigned QoS is globally enabled by the following ICLI command:

```
(config)# [no] dot1x feature radius-qos
```

The RADIUS assigned VLAN feature is enabled by the following ICLI command:

```
(config)# [no] dot1x feature radius-vlan
```

Both can be enabled by the following ICLI command:

```
(config)# [no] dot1x feature radius-qos radius-vlan
```

## Guest VLAN Enabled

The guest vlan feature is enabled by the following ICLI command:

```
(config)# [no] dot1x feature guest-vlan
```

Any combination of the features guest-vlan, radius-qos, and radius-vlan can be enabled by the following ICLI command:

```
(config)# [no] dot1x feature guest-vlan radius-qos radius-vlan
```

## RADIUS Assigned QoS

This feature is enabled for a port. For more information, see "System Configuration". It can also be enabled by the following ICLI command:

```
(config-if)# [no] dot1x radius-qos
```

where the no variant command disables it.

The feature takes effect when globally enabled by checking the RADIUS-Assigned QoS Enabled option, or by means of the following ICLI command:

```
(config)# [no] dot1x radius-qos
```

On the RADIUS server and entry (per RFC 4675), say:

```
User-Priority-Table = 55555555
```

must exist for the 802.1X entry in question. In this case the user is assigned QoS 5. The valid values are 0,..., 7. The value on the right must contain eight identical numbers.

If the FreeRADIUS (http://freeradius.org) is used, then an entry for user mememe with password itsasecret would look like the following in the user's file.

```
mememe  Cleartext-password := “itsasecret”

User-Priority-Table = 55555555
```

The port state table displays the admin state used, the port authorized, and the QoS class (5), as it was configured on the RADIUS server.

The show dot1x ICLI commands also display status and statistics.

```
# show dot1x status

# show dot1x status interface gi 1/3

The latter shows status to the interface specified:

# show dot1x status interface GigabitEthernet 1/3 GigabitEthernet
1/3 :

---------------------

Admin State           Port State       Last Source      Last ID

------------------   ---------------  --------------   --------

Port-based 802.1X    Authorized    00-23-5a-a8-05-eb    mememe

Current Radius QOS   Current Radius VLAN Current Guest VLAN

------------------   -------------------  ------------------

5
```

## RADIUS Assigned VLAN

This feature is enabled for a port. For more information, see "System Configuration". It can also be enabled by the following ICLI command:

```
(config-if)# [no] dot1x radius-vlan
```

where the no variant disables it.

The feature takes effect when globally enabled by checking the RADIUS-Assigned VLAN Enabled option, or by means of the following ICLI command:

```
(config)# [no] dot1x radius-vlan
```

On the RADIUS server and entry, say:

```
Tunnel-Medium-Type = 6             i.e., IEEE-802

Tunnel-Type = 13                   i.e., VLAN

Tunnel-Private-Group-Id = ”123”    i.e., VID=123
```

must exist for the 802.1X entry in question. In this case, the user is assigned VLAN 123. Refer to RFC 2868, RADIUS Attributes for Tunnel Protocol Support and RFC 3580, IEEE 802.1X Remote Authentication Dial In User Service (RADIUS), Usage Guidelines for further reference.

If the FreeRADIUS (http://freeradius.org) is used, then an entry for user mememe with password itsasecret would look like the following in the user's file.

```
mememe  Cleartext-password := “itsasecret”

User-Priority-Table = 55555555,

Tunnel-Medium = 6,

Tunnel-Type = 13,

Tunnel-Private-Group-ID = 123
```

The QoS = 5 remains from the previous section.

The port state table shows that the port VLAN has been assigned by the RADIUS server.

The show dot1x ICLI command also shows the status information

```
# show dot1x status interface GigabitEthernet 1/3

GigabitEthernet 1/3 :

----------------------

Admin State           Port State    Last Source          Last ID

------------------   -----------   ------------------   -------

Port-based 802.1X     Authorized    00-23-5a-a8-05-eb    mememe

Current Radius QOS    Current Radius VLAN Current Guest VLAN

------------------     -----------------  -------------------

5                     123                  -
```

where VID 123 is found again.

## Guest VLAN Enabled

A guest VLAN is a VLAN into which clients can be placed if the authentication process fails. This applies to cases where the admin state is single 801.1X, multi 802.1X, or MAC based authentication.

A port is enabled to enter the guest VLAN if the Guest VLAN Enabled option is selected. For more information, see "System Configuration". It can also be enabled by the following ICLI command:

```
(config-if)# [no] dot1x guest-vlan
```

Command parameters relate to the last four options.

- Guest VLAN Enabled
- Guest VLAN ID
- Max. Reauth. Count
- Allow Guest VLAN if EAPOL Seen

The ICLI commands for these parameters are as follows:

```
(config)# [no] dot1x feature guest-vlan

(config)# dot1x guest-vlan 44

(config)# dot1x max-reauth-req 33

(config)# [no] dot1x guest-vlan supplicant
```

This command enables the guest vlan globally, sets the VLAN ID to 44, sets the Max. Reauth. Count to 33, and enables Allowed Guest VLAN if EAPOL Seen.

The criteria for entering the guest VLAN is as follows:

After a link-up on a port, the authenticator starts transmitting EAPoL packets towards the supplicant. If Max. Reauth. Count packets are transmitted without receiving an EAPoL packet, then the port will enter the guest VLAN using the following logic:

- Allow Guest VLAN if EAPOL Seen is enabled

or

- Allow Guest VLAN if EAPOL Seen is not enabled:
  - If EAPoL packets have been seen on this port, then continue transmitting EAPoL packets and do not enter guest VLAN
  - If EAPoL packets have not been seen on this port, then enter guest VLAN.

# 16 QoS Configuration

This document gives examples on how to set up Quality of Service (QoS) using the Industrial Command Line Interface (ICLI). The examples used in this document pertain to switch engine.

## 16.1 Understanding QoS

All ingress frames are classified to a QoS level. QoS class is used in the queue system when assigning resources, in the arbitration from ingress to egress queues, and in the egress scheduler when selecting the next frame for transmission.

- Bandwidth control in the queues can be done by using Policers or Shapers.
- Apart from Shapers and Policers, different scheduling mechanisms can be configured on how the different priority queues in the QOS system are handled.
- Weighted Random Early Detection (WRED) can be configured globally to avoid congestion and drop the Yellow Frames (frames with Drop Probability (DP) set to 1) when the queues are filled.
- For controlling the amount of flooded frames entering the switch Storm Policers can be used at the global level.

### QoS Classification

There are two methods of classification to a QoS Class (CoS): Basic and Advanced.

### Basic QoS Classification

Basic QoS classification enables predefined schemes for handling Priority Code Points (PCP), Drop Eligible Indicator (DEI), and Differentiated Service Code Points (DSCP):

- QoS classification based on PCP and DEI for tagged frames. The mapping table of PCP and DEI to QoS class of each port is programmable.
- QoS classification based on DSCP values.
- DSCP Translation.
- DSCP Remarking based on QOS class.
- Per Port QOS class configuration for untagged and non IP Frames.

## Advanced QoS Classification

Advanced QoS classification uses the QoS Control Lists (QCLs), which provide a flexible classification:

- Higher layer protocol fields (Layer 2 through Layer 4) for rule matching.
- Actions include mapping to QOS class and translation of PCP, DEI and DSCP values.

## Policers

Policers limit the bandwidth of received frames exceeding the configurable rates. Policers can be configured at queue level or at a port level. There is also a provision to add policers at the EVC level, although this provision is not discussed in this document.

## Shapers

Egress traffic shaping can be achieved using bandwidth shapers. Shapers can be configured at queue level or at a port level.

## Scheduling Algorithm

Two types of scheduling are possible on the switch at a port level, Strict Priority and Deficit Weighted Round Robin (DWRR).

Strict priority: All queues follow strict priority scheduling.

DWRR: Scheduling is based on the weights configured for each queue. Configuration is present to select the number of queues which can be under DWRR. It is possible to include from 2 to all 8 queues in DWRR mode.

When the number of queues selected for DWRR is less than 8 then the lowest priority queues are put in DWRR and higher priority queues are put in Strict Priority. For example, if number of Queues is 2 for DWRR then Queue 0 and 1 are set in DWRR mode and remaining Queues 2 to 8 are set in Strict Priority.

Weighted Random Early Detection (WRED) can be configured globally to avoid congestion and drop the Yellow Frames (frames with Drop Probability (DP) set to 1) when the queues are filled. For controlling the amount of flooded frames entering the switch Storm Policers can be used at the global level.

## Weighted Random Early Detection (WRED)

Congestion can be avoided in the queue system by enabling and configuring the Weighted Random Early Detection Function (WRED). WRED can discard the frames with Drop Probability set to 1.

Configuration includes enabling WRED per queue (Global settings and not per port) and setting the Minimum and Maximum Threshold. Minimum threshold is the queue fill level at which the WRED. starts discarding the Frames. Maximum threshold can be configured either as Drop Probability or Fill Level. When the Unit is Drop Probability the mentioned threshold would be the Drop Probability with the queue fill level is just about 100%. When the Unit is Fill level, then it represents the Queue fill level where Drop probability is 100%.

### Storm Policing

Storm Policers restrict the amount of flooded frames (Frames coming with SMAC which is not learnt earlier) entering the switch. The configurations are global per switch and not per port. Storm policer can be applied separately on Unicast, Multicast, or Broadcast packets.

CLI example: configure the broadcast rate to 128fps, multicast rate to 256fps and unicast rate to 512bps.

```
(config)# qos storm broadcast fps 128
(config)# qos storm multicast fps 256
(config)# qos storm unicast fps 512
(config)# exit
# show qos storm
qos storm:
==========
Unicast  :  enabled     fps 512
Multicast:  enabled     fps 256
Broadcast:  enabled     fps 128
```

## 16.2 QoS Configuration Examples

This section provides ICLI configuration examples according to the different QoS classifications.

Notes:
To configure any of the following examples, first use the following command to restore system defaults.

```
# reload defaults
#
```

### Port Classification

Basic QoS classification configuration can be done per port. Ingress traffic coming on each port can be assigned to a CoS, PCP, Drop Precedence Level (DPL), and DEI.

### Example

All traffic coming on port 1 is mapped to CoS 2 and PCP is set as 1.

The equivalent ICLI commands are as follows:

```
# configure terminal
(config)# interface GigabitEthernet 1/1
! Set Cos to 2 and PCP to 1
(config-if)# qos cos 2
(config-if)# qos pcp 1
(config-if)# end
```

## Tagged Frame Classification per Port

Ingress port tag classification can be done based on the PCP and DEI values received on the incoming packets. This is done by enabling tag classification for that port.

## Example

Map PCP 0 and DEI 0 to QoS Class 2, Map PCP 0 and DEI 1 to QoS Class 3 on port 2.

The equivalent ICLI commands are as follows:

```
# configure terminal
(config)# interface GigabitEthernet 1/2
! Enable Tag Classification
(config-if)# qos trust tag
! Map PCP 0 and DEI 0 to Qos Class 2
(config-if)# qos map tag-cos pcp 0 dei 0 cos 2 dpl 0
! Map PCP 0 and DEL 1 to Qos Class 3
(config-if)# qos map tag-cos pcp 0 dei 1 cos 3 dpl 1
(config-if)# end
```

## Tag Remarking per Port

Tag remarking on the egress frames can be done in the following three ways.

- Classified: PCP and DEI values on the egress frames are updated with the classified values at the ingress. By default the PCP and DEI values are set to classified values.
- Default: PCP and DEI values on the egress frames are updated to default values defined per port.
- Mapped: PCP and DEI values on the egress frames are updated based on the tag remarking QoS/DPL to PCP/DEI Mapping per port.

PCP and DEI values sent on the egress frames can be mapped to QoS class and DPL values. This configuration can be done per port.

## Example 1

Set Default PCP to 5 and DEI to 0 on port 3.

The equivalent ICLI commands are as follows:

```
# configure terminal
(config)# interface GigabitEthernet 1/3
! Set Default PCP to 5 and DEI to 0
(config-if)# qos tag-remark pcp 5 dei 0
(config-if)# end
```

## Example 2

Map QoS Class 2 and DPL 0 to PCP 3 and DEI 0. Map QoS Class 3 and DPL 1 to PCP 4 and DEI 1.

The equivalent ICLI commands are as follows:

```
# configure terminal
(config)# interface GigabitEthernet 1/2
! Set Tag Remarking to Mapped
(config-if)# qos tag-remark mapped
! Map QoS Class 2 and DPL 0 to PCP 3 and DEI 0
(config-if)# qos map cos-tag cos 2 dpl 0 pcp 3 dei 0
! Map QoS Class 3 and DPL 1 to PCP 4 and DEI 1
(config-if)# qos map cos-tag cos 3 dpl 1 pcp 4 dei 1
(config-if)# end
```

## DSCP Configuration

The following DSCP Configuration settings are present per port for ingress and egress.

- DSCP based QoS classification
- Selection of trusted DSCP values used for QoS classification
- DSCP Translation: DSCP translation is done based on the DSCP translation table
- Classify (For rewriting if enabled):
  - No DSCP classification
  - Classify only DSCP=0
  - Classify only selected (trusted) DSCP values based on the DSCP classification table
  - Classify all DSCP
- Rewrite (on egress):
  - No egress rewrite
  - Rewrite enabled without remapping
  - Remap DSCP with DP unaware
  - Remap DSCP with DP aware

## Example 1

DSCP (only trusted) to QoS class / DPL classification at ingress on port 2.

The equivalent ICLI commands are as follows:

```
# configure terminal
! Enable DSCP Trust for DSCP at Port 2.
(config)# interface GigabitEthernet 1/2
(config-if)# qos trust dscp
(config-if)# exit
! Map DSCP Values 4 and 5 to QoS Class 6.
(config)# qos map dscp-cos 4 cos 6 dpl 0
(config)# qos map dscp-cos 5 cos 6 dpl 0
(config)# end
```

## Example 2

Translate DSCP at ingress on port 2 and rewrite enabled on port 3.

The equivalent ICLI commands are as follows:

```
# configure terminal
! Enable DSCP Translate at ingress on Port 2
(config)# interface GigabitEthernet 1/2
(config-if)# qos trust dscp
(config-if)# qos dscp-translate
(config-if)# exit
! Enable DSCP Remark at egress on Port 3
(config)# interface GigabitEthernet 1/3
(config-if)# qos trust dscp
(config-if)# qos dscp-remark rewrite
(config-if)# exit
! Create Ingress DSCP Translation Map
(config)# qos map dscp-ingress-translation 1 to 5
(config)# qos map dscp-ingress-translation 2 to 6
(config)# end
```

## Example 3

Classify only DSCP = 0 at ingress on port 2 and rewrite enabled on port 3.

The equivalent ICLI commands are as follows:

```
# configure terminal
```

```
! Enable DSCP=0 Classification and Translation at ingress on Port
2
(config)# interface GigabitEthernet 1/2
(config-if)# qos trust dscp
(config-if)# qos dscp-classify zero
(config-if)# qos dscp-translate
(config-if)# exit
! Create Ingress DSCP Translation Map.
(config)# qos map dscp-ingress-translation 0 to 7
(config)# qos map dscp-ingress-translation 1 to 5
! Note: Only DSCP=0 will be rewritten as these are only classified.
! Enable DSCP Remark at egress on Port 3
(config)# interface GigabitEthernet 1/3
(config-if)# qos trust dscp
(config-if)# qos dscp-remark rewrite
(config-if)# exit
(config)# end
```

## Example 4

Classify Selected DSCP at ingress on port 2, DSCP rewrite enabled on port 3.

The equivalent ICLI commands are as follows:

```
# configure terminal
! Enable DSCP classification for selected DSCP values at ingress
Port 2
(config)# interface GigabitEthernet 1/2
(config-if)# qos trust dscp
(config-if)# qos dscp-classify selected
(config-if)# exit
(config)# qos map dscp-classify 0
(config)# qos map dscp-classify 1
(config)# qos map dscp-classify 2
! Create Ingress DSCP Translation Map.
(config)# qos map dscp-ingress-translation 0 to 7
(config)# qos map dscp-ingress-translation 1 to 5
(config)# qos map dscp-ingress-translation 2 to 8
! Enable DSCP Remark at egress on Port 3
(config)# interface GigabitEthernet 1/3
```

```
(config-if)# qos trust dscp
(config-if)# qos dscp-remark rewrite
(config-if)# exit
(config-if)# end
```

## Example 5

Classify all DSCP values at ingress on port 2, rewrite enabled on port 3.

The equivalent ICLI commands are as follows:

```
# configure terminal
! Enable DSCP classification for all DSCP values at ingress Port
2
(config)# interface GigabitEthernet 1/2
(config-if)# qos trust dscp
(config-if)# qos dscp-classify any
(config-if)# exit
! Enable DSCP Remark at egress on Port 3
(config)# interface GigabitEthernet 1/3
(config-if)# qos trust dscp
(config-if)# qos dscp-remark rewrite
(config-if)# exit
(config)# end
```

## Example 6

QoS/DP to DSCP Classification enabled. Rewrite DSCP with DP Aware at egress on port 3.

Notes

To execute this example PCP/DEI on the incoming packets can be used to direct packets to a particular QoS class and DP value,.

The equivalent ICLI commands are as follows:

```
# configure terminal
! Enable DSCP Classification on all DSCP values on port 2.
(config)# interface GigabitEthernet 1/2
(config-if)# qos trust dscp
(config-if)# qos dscp-classify any
(config-if)# exit
```

```
! Map QoS Class 5, DP = 0 to DSCP 4, QoS Class 5, DP = 1 to DSCP
5
(config)# qos map cos-dscp 5 dpl 0 dscp 4
(config)# qos map cos-dscp 5 dpl 1 dscp 5
! Remap DSCP 4, DP = 0 to DSCP = 8 and DSCP 5, DP = 1 to DSCP =9
on Egress
(config)# qos map dscp-egress-translation 4 0 to 8
(config)# qos map dscp-egress-translation 5 0 to 9
! Enable DSCP rewrite with DSCP Remap DP Aware on Port 3
(config)# interface GigabitEthernet 1/3
(config-if)# qos dscp-remark remap-dp
(config-if)# end
```

## QCLs

Advanced QoS classification can be done by checking fields from Layer 2 to Layer 4 and mapping them to PCP/DEI, QoS class and DSCP values.

## Example 1

Match on a particular destination MAC on port 2 and map these to QoS class 5.

The equivalent ICLI commands are as follows:

```
# configure terminal
! Set the Address mode to Destination on Port 2
(config)# interface GigabitEthernet 1/2
(config-if)# qos qce addr destination
(config-if)# exit
! Create QCL rule for matching particular destination MAC on Port
2
(config)# qos qce 1 interface GigabitEthernet 1/2 dmac
00-00-00-00-00-23 action cos 5
(config-if)# end
```

## Example 2

Match on a particular VLAN Tag and PCP range on port 2 and map these to QoS class 6. Also map these frames to PCP = 6 and DEI = 0.

The equivalent ICLI commands are as follows:

```
# configure terminal
! Create QCL rule for matching particular VLAN ID and range of PCP
values.
```

```
(config)# qos qce 1 interface GigabitEthernet 1/2 tag vid 10 pcp
4-5 action cos 6 pcp-dei 6 (config)# end
```

## Example 3

Match on specific Dest MAC, Source IP, UDP SPort number on port 2. Map these to QoS Class 7, DP = 1 and DSCP value = 9.

The equivalent ICLI commands are as follows:

```
# configure terminal

! Set the QCE address mode to MAC and IP address on Port 2.

(config)# interface GigabitEthernet 1/2

(config-if)# qos qce key mac_ip_addr

(config-if)# exit

! Create QCL rule for matching DMAC, SIP, UDP Sport on Port 2.

(config)# qos qce 1 interface GigabitEthernet 1/2 dmac
00-00-00-00-00-23 frame-type ipv4 proto (config)# end
```

## Policers

## Port Policers

Enable policing at port level on a particular port.

## Example 1

Enable policer on port 2 and set the policer rate to 2000 Kbps. For better performance, optionally enable flow control as well if the policed traffic is TCP traffic.

The equivalent ICLI commands are as follows:

```
# configure terminal

! Enable Policer on Port 2 with a rate set to 2000Kbps

(config)# interface GigabitEthernet 1/2

(config-if)# qos policer 2000 flowcontrol

(config-if)# end
```

## Example 2

Enable policer on port 2 and set the policer rate to 200 fps. The units are frames per second.

The equivalent ICLI commands are as follows:

```
# configure terminal

! Enable Policer on Port 2 with a rate set to 200fps

(config)# interface GigabitEthernet 1/2

(config-if)# qos policer 200 fps (config-if)
```

```
# end
```

## Queue Policers

## Example

Enable policer on queue 2 at port 2. Set the policing rate to 20 Mbps.

The equivalent ICLI commands are as follows:

```
# configure terminal
! Enable Policer on Queue 2 at Port 2 with a rate set to 20 Mbps
(config)# interface GigabitEthernet 1/2
(config-if)# qos queue-policer queue 2 20000
(config-if)# end
```

## Shapers

## Port Shapers

Enable shapers at port level to shape the egress traffic.

## Example

Enable shaper on port 3 and set the shaping rate to 4000 Kbps.

The equivalent ICLI commands are as follows:

```
# configure terminal
! Enable Shaper on Port 3 and set the rate to 4000 Kbps
(config)# interface GigabitEthernet 1/3
(config-if)# qos shaper 4000
(config-if)# end
```

## Queue Shapers

## Example

Enable shaping on Queue 3 and Queue 4 at different rates on Port 3.

The equivalent ICLI commands are as follows:

```
# configure terminal
! Enable Queue Shaper on Queues 3 and 4 on Port 3 and set the rate
to 4000 and 8000 Kbps
(config)# interface GigabitEthernet 1/3
(config-if)# qos queue-shaper queue 3 4000
(config-if)# qos queue-shaper queue 4 8000
(config-if)# end
```

## Schedulers

## DWRR

## Example

Set the scheduling mode to DWRR (for 6 queues) on Port 3 with the following weights: Queue0-40, Queue1-40, Queue2-20, Queue3-20, Queue4-20 and Queue5-20.

The equivalent ICLI commands are as follows:

```
# configure terminal
! Set Scheduler mode to DWRR Priority on Port 3
(config)# interface GigabitEthernet 1/3
(config-if)# qos wrr 40 40 20 20 20 20
(config-if)# end
```

## Weighted Random Early Detection (WRED)

## Example 1

Configuring WRED on Queue 4 with a Minimum Threshold as 10% and Maximum Threshold as 50%. Maximum Threshold unit is Drop Probability.

The equivalent ICLI commands are as follows:

```
# configure terminal
!Set Minimum threshold as 10 and Maximum Threshold as 50 on Queue
4. (config)# qos wred queue 4 min-fl 10 max 50
```

## Example 2

Configuring WRED on Queue 5 with a Minimum Threshold as 10% and Maximum Threshold as 90%. Maximum Threshold unit is Fill Level.

The equivalent ICLI commands are as follows:

```
# configure terminal
!Set Minimum threshold as 10 and Maximum Threshold as 90 on Queue
5.
(config)# qos wred queue 5 min-fl 10 max 90 fill-level
```

## Storm Policing

## Example

Apply a storm policer of 1K fps on Unicast frame type.

The equivalent CLI Command is:

```
# configure terminal
(config)# qos storm unicast kfps 1
```

# 17 Configure the DHCP Client

This document describes basic usage of Industrial Command Line Interface (ICLI) to configure the DHCP client with a switch.

The ICLI is a comprehensive management interface on the device. It is the only management interface accessible on the serial console. Even if there is no network connectivity, the device can still be managed using a serial connection. The following commands assume that the device is powered on and the serial port has a functional connection to a computer console. Serial port setting should be as follows:

- 115200 baud rate
- No parity
- 8 data bits
- 1 stop bit
- No flow control

Use serial cable to connect computer serial port and Console port of the device, and run terminal emulator, such as TeraTerm or PuTTY on Windows, or Minicom on Linux.

The '#' denotes the user prompt.

```
# configure terminal
(config)# hostname Switch
Switch(config)# end
```

## 17.1 DHCP Client

When enabled, the DHCP client within the switch application software sends out requests for IP address configuration. When the requests are received by a DHCP server on the network the server searches through its pool of available IP addresses, allocates one, and returns it to the DHCP client. The returned information typically includes IP address, netmask, and default gateway, but may also contain other information such as Domain Name Service (DNS) server addresses.

Notes

IP addresses can only be assigned to VLAN interfaces.

The interface configuration mode is used to configure the parameters for an interface or a range of interfaces. An interface can be a physical port, VLAN, or other virtual interface. The interface configuration mode is distinguished further according to the type of interface. The command prompt for each type of interface is slightly different.

The VLAN interface configuration mode is used to configure the parameters of a VLAN interface. The following sections describe the commands to access the VLAN interface configuration mode

## Static IP Address

In the application software, VLAN 1 is typically used as the management VLAN. The objective is to assign an IP address to the device on VLAN 1. The following static setup is also the default setup.

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if-vlan)# ip address 192.0.2.1 255.255.255.0
Switch(config-if-vlan)# end
```

## DHCP Address

The application software includes a DHCP client, which must be enabled to automatically obtain an IP address from a DHCP server located on the network.

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if-vlan)# ip address dhcp
Switch(config-if-vlan)# end
```

## DHCP Address with Fallback

It is a good practice to default to an IP address after a timeout period for those instances where there is no DHCP server on the network.

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if-vlan)# ip address dhcp fallback 192.0.2.1
255.255.255.0
Switch(config-if-vlan)# end
```

## Display IP Address

The following output is displayed after the static address has been set up.

```
Switch# show ip interface brief
Interface      Address          Method       Status
```

```
---------      ------------     -------      ------
VLAN 1         192.0.2.1/24     Manual       UP
Switch#
```

When the DHCP negotiation is successful the following response is displayed.

```
Switch# show ip interface brief
Interface      Address          Method       Status
---------      ------------     -------      ------
VLAN 1         10.10.132.82/23  DHCP         UP
Switch#
```

The command show ip interface brief displays configured and active IP interfaces. Active interfaces should show a status of UP. If this status is not seen, there may be no link on any port. The fallback IP of 192.0.2.1 is assigned if the DHCP negotiation fails. The following command displays DHCP session statistics.

```
Switch# show ip dhcp detailed statistics client
GigabitEthernet 1/1 Statistics:
--------------------------------
Rx Discover:                    0   Tx Discover:           4
Rx Offer:                       1   Tx Offer:              0
Rx Request:                     0   Tx Request:            17
Rx Decline:                     0   Tx Decline:            0
Rx ACK:                         17  Tx ACK:                0
Rx NAK:                         0   Tx NAK:                0
Rx Release:                     0   Tx Release:            0
Rx Inform:                      0   Tx Inform:             0
Rx Lease Query:                 0   Tx Lease Query:        0
Rx Lease Unassigned:            0   Tx Lease Unassigned:   0
Rx Lease Unknown:               0   Tx Lease Unknown:      0
Rx Lease Active:                0   Tx Lease Active:       0
Rx Lease Active:                0   Tx Lease Active:       0
Rx Discarded checksum error:    0
Switch#
```

Another way to show the IP address is by displaying the actual VLAN.

```
Switch# show interface vlan 1
VLAN1
  LINK: 00-22-6f-01-01-10 Mtu:1500 <UP BROADCAST RUNNING
MULTICAST>
```

```
IPv4: 192.168.1.254/24 192.168.1.255
```

## Using the Obtained Network Connection

Once the basic system configuration is complete, management connectivity can be verified by issuing a ping command to a known external IP address.

```
Switch# ping ip 10.10.130.66
PING server 10.10.130.66, 56 bytes of data.
64 bytes from 10.10.130.66: icmp_seq=0, time=10ms
64 bytes from 10.10.130.66: icmp_seq=1, time=10ms
64 bytes from 10.10.130.66: icmp_seq=2, time=0ms
64 bytes from 10.10.130.66: icmp_seq=3, time=0ms
64 bytes from 10.10.130.66: icmp_seq=4, time=0ms
Sent 5 packets, received 5 OK, 0 bad
Switch#
```

If the ping is successful, network logins can now be performed using ssh to the address on VLAN interface 1.

## Saving the Configuration to FLASH

The current configuration of the device does not survive across reboots. Use the following commands to save running-config to FLASH storage under the name startup-config.

```
Switch# copy running-config startup-config Building configuration...
% Saving 1223 bytes to flash:startup-config
Switch#
```

The startup-config file is read and executed on every boot. It is also used to restore the running configuration of the system to the last saved state.

## Specify MAC Address

Obtaining an IP address is not successful when two switches have the same MAC address. A MAC address must be unique because the DHCP server binds the MAC address and the IP address. Use the following steps to specify a unique MAC address to get an IP address from the network.

```
Switch# platform debug allow
Switch# debug board
Board MAC Address: 00-22-6f-01-01-10
Board ID        : 1234
Board Type Conf  : 0
Board Type Active : Luton26 (5)
```

```
Product Type     : IES6300-8GT2HS
Product hwrev     : Need to fill in!
Switch# debug board mac 00-22-6F-00-b1-20
Board set operation success
```

# 18 IP Multicast Configuration

This document provides steps for deploying the IPMC profile, IGMP/MLD snooping and proxy, and MVR to manage IPMC traffic forwarding using ICLI commands. It requires familiarity with IP/HTTP technology and experience in setting up an OS application service.

A network equipment device running software is managed on a platform that may be a computer running an IP-capable OS (for example, FreeBSD®, Linux® or WINDOWS®).

To use ICLI as the management interface, requires a serial console connection between the device and the management platform. No network connection is required to use ICLI, but the terminal emulator software has to be installed.

## 18.1 IGMP/MLD Snooping

IP multicast reduces the IP broadcasting data traffic efforts by forwarding the data frames to only those network equipments that expect the designated frames proposing group registration. It is commonly deployed for triple play services (data, voice, and video) such as network conference system and video on demand.

SWITCH IPMC, which includes IGMP and MLD protocol support, manages the IP multicast group registration. Snooping works at the Layer2 MAC level but it actually handles (Layer3) IP IGMP control messages to dedicate Layer2 MAC forwarding table.

For IPMC snooping the system needs to be in Router mode where the following two roles are defined.

- Querier transmits IPMC queries and is responsible for triggering multicast address determination.
- Non-Querier routers not selected as Querier in the same broadcast domain, such as VLAN.

## 18.2 IGMP/MLD Proxy

To be an IPMC proxy, the system acts as a Host/Node in reporting the joins or leaves of multicast groups towards routers. On the other hand, the system acts as a Router that collects the expected multicast group registration information from the connected hosts/nodes. In this manner IPMC control messages restrict and manage loading of the connected routers in running protocol control.

## 18.3 IPMC Profile

In addition to multicast group registration that is driven by IGMP/MLD control messages, IPMC provides IPMC profile, an access control on registration. IPMC profile manages permissions in multicast registration for group tables.

An IPMC profile provides the rules for specific group addresses to decide whether or not the multicast registration should happen. The concept of an IPMC profile is similar to that of an ACL that gives permission by checking the given rules in a specific order. An IPMC profile is constructed with address range rules where the first matching condition takes effect.

## 18.4 IPMC Traffic Forwarding

By using IPMC snooping or proxy, SWITCH is able to do IPv4 and/or IPv6 multicast forwarding that saves bandwidth across the network. It is also able to do access management on multicast registration by deploying the IPMC profile either in filtering utility or in throttling control. MVR deployment selects the expected group address dedicated by the IPMC profile when it is expected to restrict and prioritize certain multicast streams as they are forwarded in a proprietary VLAN trunk.

IPMC snooping/proxy and MVR can coexist to provide IPv4 and/or IPv6 multicast group registration services. However, there is priority in choosing the group address for registration between IPMC snooping/proxy and MVR.

MVR has higher priority in choosing the group address for registration because MVR should be treated as a static VLAN deployment in which the user administration must get involved. When a group address is acquired by MVR the control message regarding the specific group address is not advertised in IPMC snooping/proxy VLANs.

### Limitations for IPMC Snooping, Proxy and Profile

1 IP and MAC hash: By using the MAC address table for forwarding IP multicast data, it is possible that two different IPMC group addresses map to the same MAC forwarding entry.
2 Unregistered Flooding Control: When the group table is full, unregistered multicast data traffic will be blocked by the unregistered flooding setting. Keep the unregistered flooding control enabled to deal with this situation.
3 Proxy for IGMPv3/MLDv2: transmits IGMPv1/IGMPv2/MLDv1 control messages

upstream while the proxy is enabled. While downstream, it is able to fully handle IPMC group registration upon receiving IGMPv1/IGMPv2/IGMPv3/MLDv1/MLDv2 control messages. SWITCH does not yet fully support IGMPv3/MLDv2 in IPMC proxy.

4 Not all platforms support SSM forwarding: To consider the access control resources used in chip forwarding, SSM registration information is valid on software level only.

# 18.5 IGMP/MLD Snooping Operation and Configuration

IPMC (IGMP/MLD) snooping is used to perform generic IP multicast group registration upon receiving IGMP/MLD control messages. IPMC protocol implementations are compliant with IGMPv3 and MLDv2 standards that are capable of handling all kinds of IPMC control messages from a connected network equipment.

To start snooping, both the global and per (IP) VLAN interface administrative controls have to be enabled. Depending on the querier election result on the VLAN, the active querier begins advertising query control messages. The hosts/nodes then respond with the join messages that include the expected group address. After the join messages are received, routers/ switches program the group table according to the collected information with a proper forwarding map. When a multicast data stream is broadcast, devices with IPMC snooping capability forward the data frame to registered group member(s) only.

## IPMC Snooping

Each multicast listener reports the expected join group upon receiving the query from querier. The device is then aware of the destination port interface(s) with respect to the registered group address. When multicast data is broadcast from the server, the device only forwards the specific frame destined to the known group for the registered member(s).

The SWITCH supports both the IPv4 (IGMP) and IPv6 (MLD) multicast group registration protocols, as described in the following sections.

## IGMP Snooping

IGMP is a protocol for IPv4 multicast group registration. IGMP snooping provides global administrative control and per (IP) VLAN interface management. An IGMP VLAN needs to be created and the specific IGMP VLAN enabled to start snooping IGMP control messages. The following are additional configurable IGMP VLAN interface settings regarding protocol controls.

- Querier Election defined in IGMP. When this option is disabled, the device will always be a Non-Querier.
- Querier Address IPv4 address defined as the source address used in the IP header for IGMP Querier election. When the Querier address is not set, the system uses IPv4 management address of the IP interface associated with this VLAN. When the IPv4 management address is not set, the system uses the first

available IPv4 management address. Otherwise, the system uses a default value, 192.0.2.1.

- Compatibility is maintained by hosts and routers taking appropriate actions depending on the versions of IGMP operating on hosts and routers within a network.
- Priority of interface indicates the IGMP control frame priority level generated by the device. It can be used to prioritize the different classes of traffic.
- RV the robustness variable allows tuning for the expected packet loss on a network.
- QI the query interval is the interval between general queries sent by the querier.
- QRI The maximum response delay used to calculate the maximum response code inserted into the periodic general queries. This depends on the maximum response code given. The connected host/node has to respond within this interval.
- LMQI the last member query interval is used to guarantee the group de-registration that no more host/node requires the specific multicast address. It is also used as the contributor for protocol built-in fast leaving mechanism.
- URI The unsolicited report interval is the time between repetitions of a host's initial report of membership in a group. It is used to suppress the join/report sent by the host/node.

The following table shows the basic IGMP snooping parameters and their corresponding descrip- tions.

Table 1 • IGMP Snooping Parameters

| Parameters | Description |
|---|---|
| Global IGMP Snooping | Enable/Disable the global IGMP snooping. System starts to receive IGMP control frame when the global IGMP snooping is enabled. |
| Unregistered Flooding | Enable/Disable the flooding of frame destined to unregistered IPv4 group address. The flooding control takes effect only when IGMP snooping is globally enabled. When IGMP snooping is disabled, unregistered traffic flooding is always active in spite of this setting. |
| IGMP SSM Range | Allows the SSM-aware hosts and routers to run the SSM service model for the groups in the address range. Group address in the SSM range will not allow to be advertised with EXCLUDE/BLOCK registration message. |
| VLAN ID | ID of the specific IGMP VLAN interface. |
| VLAN IGMP Snooping | Enable/Disable per (IP) VLAN IGMP snooping. System starts IGMP and does group table maintenance when per VLAN IGMP snooping is enabled. |
| Join Querier Election | Enable/Disable to join the IGMP querier election of the specific IGMP VLAN interface. |
| Querier Address | Specify the IP address used as the source address in frames generated by the device itself. |
| Compatibility | Specify the IGMP VLAN interface's compatibility. The options are: IGMP-Auto, Forced IGMPv1, Forced IGMPv2, and Forced IGMPv3. |

| Parameters | Description |
|---|---|
| Priority | Specify the CoS priority for IGMP VLAN tagged control frame. |
| RV | Used as the tolerance for IGMP control frame loss. |
| QI | Used for the routers sending periodical general query message. |
| QRI | Used for the hosts as the time limit in responding the query message. |
| LMQI | Used for the routers to determine if any hosts expect the group address by sending specific query messages in this period of time. |
| URI | Used for the hosts not sending too many join/report messages in this period of time. |

IGMP snooping works well with the default parameters once it is globally enabled with the created and enabled VLAN interface. The rest of the functionality follows the protocol to achieve the group registration and forwarding table programming.

SWITCH IGMP snooping is disabled by default without any IGMP VLAN interface. Create and enable the IGMP VLAN interface and global administrative control to start IGMP snooping. Because IGMP snooping logical interface relies on the existing physical VLAN setting to receive and transmit protocol frames, it is important to properly configure the associated VLAN. IGMP behavior is configured by protocol parameters. Modifying these parameters requires familiarity with the IGMP standard.

The following is a quick summary of the steps.

1 Confirm unregistered flooding control is set as expected.
2 Confirm the SSM address range if it is expected to run IGMPv3 snooping for SSM capable services.
3 Create an IGMP VLAN interface and enable this interface.
4 Configure Querier Address if needed.
5 Set up Compatibility and/or Join Querier Election to force IGMP snooping in static operation (IGMPv1/IGMPv2/ IGMPv3 and/or Non-Querier) mode.
6 Set up protocol attributes (RV / QI / QRI / LMQI / URI) for IGMP to adjust protocol behaviors.
7 Assign the CoS priority for sending tagged control frames, if needed.
8 Repeat Step-3 to Step-7 for IGMP VLAN interface management.
9 Set up global IGMP snooping administrative control, if needed.
10 Save the configuration, if needed.

## Default Setting and Configurable Value Range

The following table shows the default IGMP snooping settings and their configurable value range.

Table 2 • IGMP Snooping Settings

| Configuration | Default Value | Configurable Value Range |
|---|---|---|
| Global IGMP Snooping | Disabled | Enabled or Disabled |

| Configuration | Default Value | Configurable Value Range |
|---|---|---|
| Unregistered Flooding | Enable | Enabled or Disabled |
| IGMP SSM Range | 232.0.0.0 / 8 | Valid IPv4 multicast prefix and prefix length |
| VLAN ID for IGMP Interface | Empty | 1 ~ 4095 VLAN ID. At maximum 32 IGMP VLAN interface can be created. |
| VLAN IGMP Snooping | Disabled | Enabled or Disabled |
| Join Querier Election | Enable | Enabled or Disabled<br>When Disabled, the specific interface always acts as Non-Querier. |
| Querier Address | 0.0.0.0. | Valid IPv4 unicast address |
| Compatibility | Auto | Auto / IGMPv1 / IGMPv2 / IGMPv3<br>Auto: Compatible with IGMPv1/IGMPv2/IGMPv3<br>IGMPv1:Forced IGMPv1<br>IGMPv2:Forced IGMPv2<br>IGMPv3:Forced IGMPv3 |
| Priority | 0 | 0 ~ 7 CoS value. |
| RV | 2 | Packet loss tolerance count from 1 to 255 |
| QI | 125 | 1 - 31744 seconds |
| QRI | 100 | 0 - 31744 tenths of seconds |
| LMQI | 10 | 0 - 31744 tenths of seconds |
| URI | 1 | 0 - 31744 seconds |

## IGMP Snooping Setup using ICLI

The following table shows the steps used to set up IGMP snooping using ICLI.

Table 3 • Setting up IGMP Snooping Using ICLI

| Step | Command or Action | Purpose |
|---|---|---|
| 1 | **configure terminal**<br>Example<br>**# configure terminal**<br>**(config)#** | Enter Configure Mode |
| 2 | **ip igmp { ssm-range <ipv4_mcast> \| unknown-flooding }**<br>Example<br>**(config)# ip igmp unknown-flooding**<br>**(config)#** | (Optional)<br>Sets up unknown flooding or SSM range or IPv4 multicast data forwarding. |
| 3 | **ip igmp snooping vlan <vlan_list>**<br>Example<br>**(config)# ip igmp snooping vlan 1**<br>**(config)#** | Creates IGMP VLAN interface(s) with specific VLAN ID or list. |

| Step | Command or Action | Purpose |
|---|---|---|
| 4 | **interface vlan <vlan_list>**<br>Example<br>**(config)# interface vlan 1**<br>**(config-if-vlan)#** | Enters (IP) VLAN interface configuration mode with the specific VLAN ID or list. |
| 5 | **ip igmp snooping**<br>Example<br>**(config-if-vlan)# ip igmp snooping**<br>**(config-if-vlan)#** | Enables the designated (IP) VLAN interface MLD snooping function. |
| 6 | **ip igmp snooping**<br><br>**{**<br>**compatibility { auto \| v1 \| v2 \| v3 }**<br>**\| last-member-query-interval <0-31744> \|**<br>**priority <0-7> \|**<br>**querier address <ipv4_ucast> \|**<br>**querier election \|**<br>**query-interval <1-31744> \|**<br>**query-max-response-time <0-31744> \|**<br>**robustness-variable <1-255> \|**<br>**unsolicited-report-interval <0-31744>**<br>**}**<br>Example<br>**(config-if-vlan)# ip igmp snooping querier election**<br>**(config-if-vlan)#** | (Optional)<br>Sets up IGMP VLAN interface specific configurations. |
| 7 | **exit**<br>Example<br>**(config-if-vlan)# exit**<br>**(config)#** | Exits from interface configuration mode and returns to global configuration mode |
| 8 | **ip igmp snooping**<br>Example<br>**(config)# ip igmp snooping**<br>**(config)#** | Enables the global MLD snooping function. |
| 9 | **end**<br>Example<br>**(config)# end**<br>**#** | Returns to privileged EXEC mode |
| 10 | **copy running-config startup-config**<br>Example<br>**# copy running-config startup-config**<br>**#** | (Optional)<br>Saves settings in the configuration file |

## MLD Snooping

MLD is a protocol for IPv6 multicast group registration. MLD snooping provides global administrative control and per (IP) VLAN interface management. Except for the Querier Address, it is almost the same as "IGMP Snooping".

The querier address used in MLD is always the IPv6 link-local address of the specific (IP) VLAN interface because MLD is a local scope protocol running for IPv6 multicast group registration. If the corresponding IP interface is not configured in the system, MLD snooping uses EUI-64 to determine the source address used in the IP header for generating MLD control messages.

The following table shows the basic MLD snooping parameters and their corresponding descriptions.

Table 4 • MLD Snooping Parameters

| Parameters | Description |
|---|---|
| Global MLD Snooping | Enable/Disable the global MLD snooping.<br>The system starts to receive MLD control frame when the global MLD snooping is enabled. |
| Unregistered Flooding | Enable/Disable the flooding of frame destined to unregistered IPv6 group address. The flooding control takes effect only when MLD snooping is globally enabled. When MLD snooping is disabled, unregistered traffic flooding is always active in spite of this setting. |
| MLD SSM Range | Allows the SSM-aware hosts and routers to run the SSM service model for the groups in the address range. |
| VLAN ID | ID of the specific MLD VLAN interface. |
| VLAN MLD Snooping | Enable/Disable per (IP) VLAN MLD snooping.<br>The system starts MLD and performs group table maintenance when per VLAN MLD snooping is enabled. |
| Join Querier Election | Enable/Disable to join the MLD querier election of the specific MLD VLAN interface. |
| Compatibility | Specify the MLD VLAN interface's compatibility. The options are: MLD-Auto, Forced MLDv1, and Forced MLDv2. |
| Priority | Specify the CoS priority for MLD VLAN tagged control frame. |
| RV | Used as the tolerance for MLD control frame loss. |
| QI | Used for the routers sending periodical general query message. |
| QRI | Used for the hosts as the time limit in responding the query message. |
| LMQI | Used for the routers to determine if any hosts expect the group address by sending specific query messages in this period of time. |
| URI | Used for the hosts not sending too many join/report messages in this period of time. |

MLD snooping works well with the default parameters once it is globally enabled with created and enabled VLAN interface. The rest of the functionality follows the protocol to achieve the group registration and forwarding table programming.

Unregistered Flooding control needs to be enabled always for MLD snooping because IPv6 relies on multicast message exchanges for interface initialization. If these important messages are filtered (not to be flooded), then the connected IPv6 nodes will not function properly.

MLD snooping is disabled by default without any MLD VLAN interface. Create and enable the MLD VLAN interface and global administrative control to start MLD snooping. Because the MLD snooping logical interface relies on an existing physical VLAN setting to receive and transmit protocol frames, it is important to properly configure the associated VLAN. MLD behavior is configured by protocol parameters. Modifying these parameters requires familiarity with the MLD standard.

The following is a quick summary of the steps.

1 Confirm unregistered flooding control is set as expected. It is strongly recommended to enable unregistered flooding control for IPv6 multicast traffic.
2 Confirm SSM address range if it is expected to run MLDv2 snooping for SSM capable services.
3 Create an MLD VLAN interface and enable this interface.
4 Set up Compatibility and/or Join Querier Election to force MLD snooping in static operation (MLDv1/MLDv2 and/or Non-Querier) mode.
5 Set protocol attributes (RV/QI/QRI/LLQI/URI) for MLD to adjust protocol behaviors.
6 Assign the CoS priority for sending tagged control frames, if needed.
7 Repeat Step-3 to Step-6 for MLD VLAN interface management.
8 Set up global MLD snooping administrative control, if needed.
9 Save the configuration, if needed.

## Default Setting and Configurable Value Range

The following table shows the default MLD snooping settings and their configurable value range.

Table 5 • Default MLD Snooping Settings

| Configuration | Default Value | Configurable Value Range |
|---|---|---|
| Global MLD Snooping | Disabled | Enabled or Disabled |
| VLAN ID for MLD Interface | Enable | Enabled or Disabled |
| MLD SSM Range | ff3e::/ 96 | Valid IPv6 multicast prefix and prefix length |
| VLAN ID for MLD Interface | Empty | 1 ~ 4095 VLAN ID. At maximum 32 MLD VLAN interface can be created. |
| VLAN MLD Snooping | Disabled | Enabled or Disabled |
| Join Querier Election | Enable | Enabled or Disabled<br>When Disabled, the specific interface always acts as Non-Querier. |

| | | |
|---|---|---|
| Compatibility | Auto | Auto / MLDv1 / MLDv2<br>Auto: Compatible with MLDv1/MLDv2MLDv1: Forced MLDv1<br>MLDv2:Forced MLDv2 |
| Priority | 0 | 0 ~ 7 CoS value. |
| RV | 2 | Packet loss tolerance count from 1 to 255 |
| QI | 125 | 1 - 31744 seconds |
| QRI | 100 | 0 - 31744 tenths of seconds |
| LLQI | 10 | 0 - 31744 tenths of seconds |
| URI | 1 | 0 - 31744 seconds |

## MLD Snooping Setup Using ICLI

The following table shows the steps used to set up MLD snooping using ICLI.

Table 6 • Setting up MLD Snooping using ICLI

| Step | Command or Action | Purpose |
|---|---|---|
| 1 | **configure terminal**<br>Example<br>**# configure terminal (config)#** | Enter Configure Mode |
| 2 | **ipv6 mld { ssm-range <ipv6_mcast> \| unknown-flooding }**<br>Example<br>**(config)# ipv6 mld unknown-flooding**<br>**(config)#** | (Optional)<br>Sets up unknown flooding or SSM range or IPv6 multicast data forwarding. |
| 3 | **ipv6 mld snooping vlan <vlan_list>**<br>Example<br>**(config)# ipv6 mld snooping vlan 1**<br>**(config)#** | Creates MLD VLAN interface(s) with specific VLAN ID or list. |
| 4 | **interface vlan <vlan_list>**<br>Example<br>**(config)# interface vlan 1**<br>**(config-if-vlan)#** | Enters (IP) VLAN interface configuration mode with the specific VLAN ID or list. |
| 5 | ipv6 mld snooping<br>Example<br>**(config-if-vlan)# ipv6 mld snooping**<br>**(config-if-vlan)#** | Enables the designated (IP) VLAN interface MLD snooping function. |

| Step | Command or Action | Purpose |
|---|---|---|
| 6 | **ipv6 mld snooping**<br><br>**{**<br>**compatibility { auto \| v1 \| v2 } \|**<br>**last-member-query-interval**<br>**<0-31744> \|**<br>**priority <0-7> \|**<br>**querier election \|**<br>**query-interval <1-31744> \|**<br>**query-max-response-time <0-31744>**<br>**\|**<br>**robustness-variable <1-255> \|**<br>**unsolicited-report-interval**<br>**<0-31744>**<br>**}**<br>Example<br>**(config-if-vlan)# ipv6 mld snooping querier election**<br>**(config-if-vlan)#** | (Optional)<br>Sets up MLD VLAN interface specific configurations. |
| 7 | **exit**<br>Example<br>**(config-if-vlan)# exit**<br>**(config)#** | Exits from interface configuration mode and returns to global configuration mode |
| 8 | **ipv6 mld snooping**<br>Example<br>**(config)# ipv6 mld snooping**<br>**(config)#** | Enables the global MLD snooping function. |
| 9 | **end**<br>Example<br>**(config)# end**<br>**#** | Returns to privileged EXEC mode |
| 10 | copy running-config startup-config<br>Example<br>**# copy running-config startup-config**<br>**#** | (Optional)<br>Saves settings in the configuration file<br>file |

## 18.6 IGMP/MLD Proxy Operation and Configuration

IPMC (IGMP/MLD) proxy is used to reduce message exchanges from the IPMC control plane. IPMC proxy speaks for a set of hosts in a reporting group and it communicates with the hosts as a generic IPMC router to collect group registration information. The key idea in proxy operation is that the device will actively report the

join only for the first registration (New) of a group, and the leave only for the last de-registration (Removal) of a group. The following tasks start the IPMC proxy operation.

- Enable both the global and expected (IP) VLAN interface snooping.
- Turn on proxy administrative control.
- Turn off the Join Querier Election capability on the (IP) VLAN interface.

On boot-up, the device collects the group registrations and reports the entries in the group table when the timer for the latest event reporting expires, or when the device receives a query message from querier. In other words, the device plays the role of both a host and a router at the same time. The following steps describe protocol message exchanges.

1 When 1 boots up, it reports the join for 225.5.5.5 and 228.8.8.8 to register them in the device's group table. After a while, the device sends the join for 225.5.5.5 and 228.8.8.8 group addresses.
2 Assume 2 and 3 boot up almost at the same time, but the messages from 2 come first. The new group registrations for addresses 226.6.6.6 and 227.7.7.7 are collected and registered in the device's group table. When messages from 3 arrive, the device updates the existing group registrations. After a while, the device sends the join only for 226.6.6.6 and 227.7.7.7 group addresses.
3 When 4 boots up and it sends join messages, the device updates only the existing group registrations and does not advertise the reports for join.
4 When 5 boots up and it sends join messages, the device updates only the existing group registrations and does not advertise the reports for join.
5 When the general query timer (QI) expires on a querier all the hosts receive the general query frame and respond with reports of join. The device processes the received joins from the connected listeners but filters the control frames by not forwarding them. The device also reports the joins for the recorded groups (225.5.5.5, 226.6.6.6, 227.7.7.7,and 228.8.8.8) in a local database instead.

## IGMP Proxy

The IGMP proxy delegates IPv4 multicast group registration, provides global administrative controls, and cooperates with

The following table shows the basic IGMP proxy parameters and their corresponding descriptions.

Table 7 • IGMP Proxy Parameters

| Parameters | Description |
|---|---|
| IGMP Host Proxy | Enable/Disable the global IGMP proxy.<br>The system stops forwarding control messages to upstream directly, but when the IGMP proxy is enabled, it actively sends the group address report instead. |
| IGMP Leave Proxy | Enable/Disable the IGMP proxy only for group de-registration.<br>This capability only works on IGMPv2 that provides the LEAVE message type. |

Note:

When global IGMP proxy is enabled, the system does proxy for both group registration and de-registration regardless of the setting for IGMP leave proxy.

## MLD Proxy

The MLD proxy delegates the IPv6 multicast group registration, provides global administrative controls, and cooperates with MLD snooping. The following table shows the basic MLD proxy parameters and their corresponding descriptions.

Table 8 • MLD Proxy Parameters

| Parameters | Description |
|---|---|
| MLD Host Proxy | Enable/Disable the global MLD proxy.<br>The system stops forwarding control messages to upstream directly, but when the MLD proxy is enabled, it actively sends the group address report instead. |
| MLD DONE Proxy | Enable/Disable the MLD proxy only for group de-registration.<br>This capability only works for MLDv1 that provides the DONE message type. |

Note:
When global MLD proxy is enabled, the system does proxy for both group registration and de-registration regardless of the setting for MLD leave proxy.

## Configuring IGMP/MLD Proxy

Set up IPMC Snooping before turning on IGMP/MLD proxy on SWITCH. The following options are available for IGMP/MLD proxy:

- Leave Proxy Proxy for IGMPv2/MLDv1 leave messages only.
- Host Proxy Proxy for all kinds of IGMP/MLD control messages.

When host proxy is chosen, leave proxy is covered, but even though leave proxy becomes a redundant setting, it is still kept in configuration.

The following is a quick summary of the steps.

1 Determine whether IGMP or MLD proxy is expected.
2 If IGMP proxy is expected, set up IGMP snooping first. If MLD proxy is expected, set up MLD snooping first.
3 Select preferred proxy option: host proxy or leave proxy.
4 Enable the specific proxy administrative control.
5 Save the configuration, if needed.

## Default Setting and Configurable Value Range

The following table shows the default IGMP/MLD proxy settings and their configurable value range.

Table 9 • IGMP/MLD Proxy Settings

| Configuration | Default Value | Configurable Value Range |
|---|---|---|
| IGMP Host Proxy | Disabled | Enabled or Disabled |

| | | |
|---|---|---|
| IGMP Leave Proxy | Disabled | Enabled or Disabled |
| MLD Host Proxy | Disabled | Enabled or Disabled |
| MLD Leave Proxy | Disabled | Enabled or Disabled |

### IGMP/MLD Proxy Setup Using ICLI

The following table shows the steps used to set up IGMP/MLD proxy using ICLI.

Table 10 • Setting up IGMP/MLD Proxy Using ICLI

| Step | Command | Purpose |
|---|---|---|
| 1 | **Configure terminal.**<br>Example<br>**# configure terminal**<br>**(config)#** | Enter Configure Mode |
| 2 | **ip igmp host-proxy [ leave-proxy ]**<br>Example<br>**(config)# ip igmp host-proxy leave-proxy**<br>**(config)#** | (Optional)<br>Enables IGMP host proxy or leave proxy. |
| 3 | **ipv6 mld host-proxy [ leave-proxy ]**<br>Example<br>**(config)# ipv6 mld host-proxy**<br>**(config)#** | (Optional)<br>Enables MLD host proxy or leave proxy. |
| 4 | **end**<br>Example<br>**(config)# end**<br>**#** | Returns to privileged EXEC mode. |
| 5 | **copy running-config startup-config**<br>Example<br>**# copy running-config startup-config**<br>**#** | (Optional)<br>Saves settings in the configuration file. |

## 18.7 IPMC Profile Operation and Configuration

IPMC profiling functions as an administrative forwarding map for IP multicasting. When a group address does not match any rule in an IPMC profile, it is dropped from multicast registration. As a result, it is important to determine the expected groups for registration in advance.

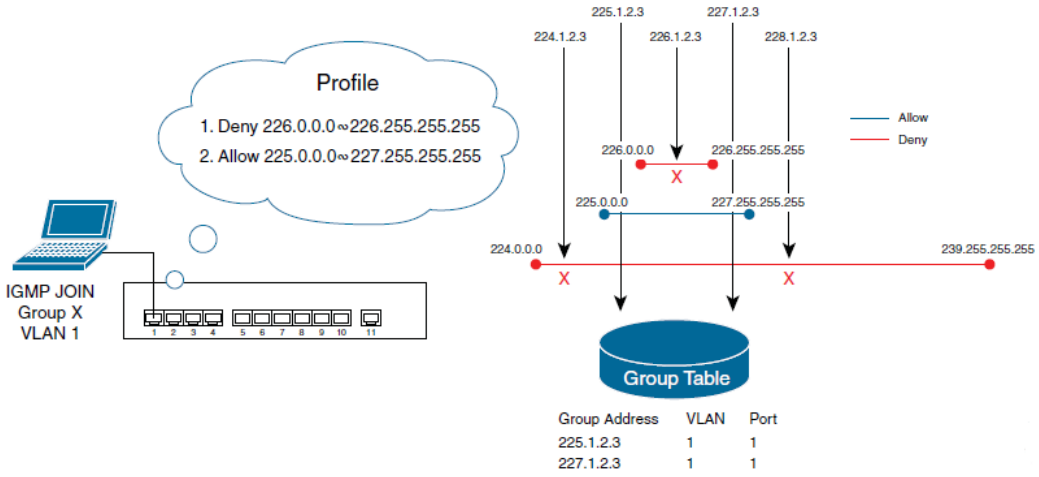
IPMC profile configuration consists of profile settings and address ranges. A profile contains filtering rules by referring to the selected address range. An address range, which may belong to different profiles, provides a set of contiguous IP multicast groups that are used for address matching.

To start using IPMC profile, the following conditions have to be met:

- The global IPMC profile administrative control has to be enabled.
- Define the address ranges for profiling. An address range can be either IPv4 multicast address or IPv6 multicast address but not a hybrid (IPv4 and IPv6 mixed) multicast address.
- Define the rules for a single profile by selecting the existing address ranges and giving corresponding actions. Smaller rule index number indicates higher priority in matching. A profile can perform access control in hybrid matching but obeys the priority order to dedicate final filtering results.
- Associate the profile with the expected application, IPMC filtering utility, and/or MVR. Overlapping address tolerance depends on the application's design perspective: IPMC filtering utility even allows the same IPMC profile being applied on different ports, but MVR does not allow the different MVR VLANs managing the overlap groups.

When the profile is set and ready to perform filtering, every group registration request (triggered by receiving IPMC control message) starts matching to decide registration result. By inspecting the rules in the designated profile, the first matched result will be the final decision. The following figure shows the IPMC profiling operation with respect to IGMP.

Figure IPMC Profiling Operation for IGMP




In this example, the specific profile expects to permit only the group address from 225.0.0.0 to 225.255.255.255 and 227.0.0.0 to 227.255.255.255. The first rule (index is 1) should deny group address ranges from 226.0.0.0 to 226.255.255.255, and the second rule (index is 2) should permit group address ranges from 225.0.0.0 to 227.255.255.255.

Upon receiving the JOIN message, SWITCH starts matching the input group address with the existing rules, as shown in the following examples.

1 When 224.1.2.3 is seen, both rules are not matched so the group address is not programed into the group table.
2 When 225.1.2.3 is seen, the first rule is not matched but the second rule is matched so the group address is programed into the group table.
3 When 226.1.2.3 is seen, the first rule is matched and thus the operation stops. The first rule denies registration so the group address is not programed into the

group table.

4 When 227.1.2.3 is seen, the first rule is not matched but the second rule is matched. The second rule permits registration and so the group address is programed into the group table.

5 When 228.1.2.3 is seen, both rules are not matched so the group address is not programed into the group table.

IPMC profile provides the configurable parameters used for managing profile, profile rule, and address range. The following table shows the basic IPMC profile parameters and their corresponding descriptions.

Table 14 • IPMC Profile Parameters

| Parameters | Description |
|---|---|
| Global Profile Mode | Enable/Disable the global IPMC profile.<br>System starts to filter based on profile settings only when the global profile mode is enabled. |
| Address Range Name | The name used for indexing the address entry table, and each entry has the unique name. |
| Start Address | The starting IPv4/IPv6 multicast group address that will be used as an address range. |
| End Address | The ending IPv4/IPv6 multicast group address that will be used as an address range. |
| Profile Name | The name used for indexing the profile table, and each entry has the unique name. |
| Profile Description | Additional description about the profile. |
| Rule Entry Name | The name used in specifying the address range for a rule. Only the existing address range entries will be chosen. |
| Rule Action | Indicates the learning action upon receiving the Join/Report frame that has the group address matches the address range of the rule.<br>Permit Group address matches the range specified in the rule will be learned. Deny Group address matches the range specified in the rule will be dropped. |
| Log for Rule | Indicates the logging preference upon receiving the Join/Report frame that has the group address matches the address range of the rule.<br>Enable Corresponding information of the group address, that matches the range specified in the rule, will be logged.<br>Disable Corresponding information of the group address, that matches the range specified in the rule, will not be logged. |
| Next Rule | Specify next rule entry used in the same profile. When the next rule is not specified, the designated rule is added as the last entry in the profile by default. In brief, it is used to assign the priority order for rule in profile |

Note:
IPMC profile starts operation passively. It only provides the access control upon receiving an

IPMC control message that relies on snooping, proxy, and MVR administration.

Without any profile, address range, and rule entry, the IPMC profile is disabled by default. Create address ranges and profiles, and associate expected ranges as rules used in a specific profile to set up an IPMC profile. When IPMC access control is required, enable global IPMC profile to start filtering. The following is a quick summary of the steps.

1 Create address range with proper entry name.
2 Repeat Step-1 for expected address range management.
3 Create profile with proper entry name.
4 Set up additional descriptions for designated IPMC profile entry, if necessary.
5 Associate an address range entry with designated IPMC profile entry as a profile rule.
6 Set up action and log preference for the rule.
7 Assign the priority order of the rule in the designated IPMC profile entry, if necessary.
8 Repeat Step-3 ~ Step-7 for profile management.
9 Set up global IPMC profile administrative control, if necessary.
10 Save the configuration, if needed.

Always check the precedence of rules in a profile before applying the specific profile.

## Default Setting and Configurable Value Range

The following table shows the default IPMC profile settings and their configurable value range.

Table 15 • IPMC Profile Settings

| Configuration | Default Value | Configurable Value Range |
|---|---|---|
| Global Profile Mode | Disabled | Enabled or Disabled. |
| Address Range Name | Null string | At maximum 16 printable characters are accepted. The name string has to be unique per system. There are at most 128 address range entries to be created. |
| Start Address | Empty | Valid IPv4 or IPv6 multicast address. It has to be the same version address as ‘End Address’ |
| End Address | Empty | Valid IPv4 or IPv6 multicast address. It has to be the same version address as ‘Start Address’ |
| Profile Name | Null string | At maximum 16 printable characters are accepted. The name string has to be unique per system. There are at most 64 profile entries to be created. |
| Profile Description | Null string | At maximum 64 printable characters are accepted. |
| Rule Entry Name | Null string | Any existing address range configured in the system. |
| Rule Action | Deny | Permit or Deny |

| Configuration | Default Value | Configurable Value Range |
|---|---|---|
| Log for Rule | Disabled | Enabled or Disabled |
| Next Rule | Least priority (Last rule in profile) | Any existing rule in the specific IPMC profile. |

## IPMC Profile Setup using ICLI

The following table shows the steps used to set up IPMC profile using ICLI.

Table 16 • Setting up IPMC Profile Using ICLI

| Step | Command | Purpose |
|---|---|---|
| 1 | **Configure terminal.**<br>Example<br>**# configure terminal (config)#** | Enter configure mode. |
| 2 | **ipmc profile**<br>Example<br>**(config)# no ipmc profile**<br>**(config)#** | (Optional)<br>Enable/Disable global IPMC profiling function. |
| 3 | **ipmc range range-name start-ip-multicast-address end-ip-multicast-address**<br>Example<br>**(config)# ipmc range Video 227.3.3.3 228.123.123.123**<br>**(config)# ipmc range Data 238.0.0.0 239.255.255.255**<br>**(config)# ipmc range Audio 225.1.1.1 225.222.222.222**<br>**(config)# ipmc range Game 226.0.0.0 226.255.255.255**<br>**(config)#** | Define the expected address ranges. |
| 4 | **ipmc profile profile-name**<br>Example<br>**(config-if)# ipmc profile AN1135**<br>**(config-if)#** | Specifies the name of IPMC profile entry on which access control is enabled, and enters IPMC profile configuration mode. |
| 5 | **description**<br>Example<br>**(config-ipmc-profile)# description Demonstration for Configuration Guides AN1135 (config-ipmc-profile)#** | (Optional)<br>Add additional notes for describing the specific profile. |

| Step | Command | Purpose |
|---|---|---|
| 6 | **range range-name {deny \| permit} [log] [next range-name]**<br>Example<br>**(config-ipmc-profile)# range Audio permit log (config-ipmc-profile)# range Data permit**<br>**(config-ipmc-profile)# range Video permit next Data**<br>**(config-ipmc-profile)#** | Arrange and configure rules for the specific profile. |
| 7 | **end**<br>Example<br>**(config-ipmc-profile)# end**<br>**#** | Returns to privileged EXEC mode. |
| 8 | **show ipmc profile [profile-name] [detail]**<br>Example<br>**# show ipmc profile**<br>**IPMC Profile is currently disabled, please enable profile to start filtering. Profile:AN1135 (In IGMP Mode)**<br>**Description:Demonstration for Configuration Guides AN1135**<br>**HEAD-> Audio (Permit the following range and log the matched entry) Start Address:225.1.1.1**<br>**End Address:225.222.222.222**<br>**NEXT-> Video (Permit the following range) Start Address:227.3.3.3**<br>**End Address:228.123.123.123**<br>**NEXT-> Data (Permit the following range) Start Address:238.0.0.0**<br>**End Address:239.255.255.255**<br>**#** | Confirm the configured IPMC profile filtering conditions. |
| 9 | **copy running-config startup-config**<br>Example<br>**# copy running-config startup-config**<br>**#** | (Optional)<br>Saves settings in the configuration file. |

Notes

Use no command to negate configured settings. Use the show ipmc profile detail command to display the matching conditions in detail to help in understanding the filtering result of a specific address.

# 18.8 IGMP/MLD Utility Operation and Configuration

The IPMC provides four additional utilities for static controls on "IPMC Snooping".

1 Filtering restricts group registration based on the given profiling access control. Only the allowed groups will be registered. For information about profiling access controls, see "IPMC Profile Operation and Configuration".
2 Throttling limits the number of groups registered, based upon the throttling value.
3 Fast Leave deletes the MAC forward entry regardless of the protocol confirmation when a message for leaving a group is received.
4 Router Port statically configures a specific port as upstream, which means it connects to another IPMC router(s).

The following table shows the basic IPMC utility parameters and their corresponding descriptions.

Table 17 • IPMC Utility Parameters

| Parameters | Description |
|---|---|
| Filtering Profile | Specify the profile to be used in filtering group registration. |
| Throttling Value | Specify the maximum number of group registrations. |
| Fast Leave | Performs deleting MAC forward entry immediately upon receiving message for group de-registration. |
| Router Port | Specify the interface is connected with another IPMC router(s). |

Each utility need to be configured per-port because they are used to enhance IGMP/MLD snooping and IPMC performs Layer2 snooping. The following are some examples of typical use.

- The filtering utility can be used to limit the multicast address forwarding for a specific port.
- The throttling utility can be used to restrict the amount of multicast address registration on a certain port to save group table resource.
- The fast leave utility can be used to speed up the group purging for a better multicast streaming experience.
- The router port utility can be used to manually specify the upstream for IPMC control plane.

The following is a quick summary of the steps.

1 Define the purpose and investigate the possible results of applying these utilities.
2 Set up the IPMC profile first to use the filtering utility. For more information, see "IPMC Profile Operation and Configuration".
3 Associate the expected IPMC profile to be filtered on a specific port, if required.
Note:
Filtering from a hybrid mode profile applied on either IGMP or MLD snooping port(s) is possible, but not filtering from a pure IGMP profile applied on a MLD snooping port and vice versa.
4 Assign the throttling number to limit the amount of group registration on a specific

port, if required.

5 Enable the fast leave for immediate purging MAC forwarding entry on a specific port, if required.

6 Select the upstream connection (where a multicast router is attached) on a specific port, if required.

7 Save the configuration, if needed.

## Default Setting and Configurable Value Range

The following table shows the default IPMC utility settings and their configurable value range.

Table 18 • IPMC Utility Settings

| Configuration | Default Value | Configurable Value Range |
|---|---|---|
| Filtering Profile | Empty | Existing IPMC profile entry. |
| Throttling Value | Unlimited | 1-10 number of group registration. |
| Fast Leave | Disabled | Enabled or Disabled. |
| Router Port | Disabled | Enabled or Disabled. |

## IGMP/MLD Utility Setup Using ICLI

The following table shows the steps used to set up IGMP/MLD utilities using ICLI.

Table 19 • Setting up IGMP/MLD Utilities Using ICL

| Step | Command | Purpose |
|---|---|---|
| 1 | **configure terminal**<br>Example<br>**# configure terminal (config)#** | Enter configure mode. |
| 2 | **interface interface-id**<br>Example<br>**(config)# interface GigabitEthernet 1/4 (config-if)#** | Specifies the interface on which you are using the IPMC utility, and enters interface configuration mode. |
| 3 | **ip igmp snooping filter <word16>**<br>**ipv6 mld snooping filter <word16>**<br>Example<br>**(config-if)# ip igmp snooping filter AN1135 (config-if)#** | (Optional)<br>Set up filtering feature. |
| 4 | **ip igmp snooping max-groups <1-10>**<br>**ipv6 mld snooping max-groups <1-10>**<br>Example<br>**(config-if)# ipv6 mld snooping max-groups 3 (config-if)#** | (Optional)<br>Set up throttling feature. |

| Step | Command | Purpose |
|---|---|---|
| 5 | **ip igmp snooping immediate-leave**<br>**ipv6 mld snooping immediate-leave**<br>Example<br>**(config-if)# ipv6 mld snooping immediate-leave**<br>**(config-if)#** | (Optional)<br>Set up fast leave feature. |
| 6 | **ip igmp snooping mrouter ipv6 mld snooping mrouter**<br>Example<br>**(config-if)# ip igmp snooping mrouter**<br>**(config-if)# ipv6 mld snooping mrouter**<br>**(config-if)#** | (Optional)<br>Set up router port feature |
| 7 | **end**<br>Example<br>**(config-if)# end #** | Returns to privileged EXEC mode. |
| 8 | **copy running-config startup-config**<br>Example<br>**# copy running-config startup-config**<br>**#** | (Optional)<br>Saves settings in the configuration file<br>file. |

# 18.9 IPMC Configuration Examples

Complete the following tasks to be able to start managing the IPMC functionality.

1 Prepare a computer

Ensure the computer is equipped with a (USB) RS-232 connector and NIC card.

- Install Linux OS uBuntu LTS version on this computer. For information about installation steps, see http://www.ubuntu.com/download/desktop/install-ubuntu-desktop.
- Add the minicom software package

```
$ sudo apt-get install minicom
```

- Configure the minicom software

```
(Find out the expected group to access the expected serial adapter in the computer. In this case, 'dialout' is the group name and there are at least two serial adapters available:'ttyS0' and ' ttyUSB0'.)

$ ls -alp /dev | grep tty

…

crw-rw----1 root dialout4,64 Nov 13 19:17 ttyS0

…
```

```
crw-rw----1 root dialout4,73 Nov 1 15:53 ttyS9 crw-rw----1 root
dialout 188, 0 Nov 1 15:53 ttyUSB0

…

(Use command "usermod" to add your Ubuntu user as a member of group
'dialout' if user is not in the specific group. To check whether
user belongs to the group 'dialout', use command "id" to identify.)

$ id Switch

uid=2000 gid=1000 groups=1000

$ sudo usermod -a -G dialout Switch

$ id Switch

uid=2000 gid=1000 groups=1000,20(dialout

)

(Setup USB RS-232 adaptor as minicom's default connection, for
example.)

$ sudo minicom -s

(Select 'Serial port setup' after executing command.)

+-----[configuration]------+

| Filenames and paths|

| File transfer protocols|

| Serial port setup|

| Modem and dialing|

| Screen and keyboard|

| Save setup as dfl|

| Save setup as..|

| Exit|

| Exit from Minicom|

+--------------------------+

(Change the serial port setting as below to meet the serial
configuration.)

+ ----------------------------------------------------------

--------+

| A-Serial Device:/dev/ttyUSB0

|

| B -Lockfile Location:/var/lock

|

| C-Callin Program:

|
```

```
| D-Callout Program:
|
| E-Bps/Par/Bits:115200 8N1
|
| F -Hardware Flow Control :No
|
| G -Software Flow Control :No
|
|
|
| Change which setting?
|
+ ------------------------------------------------------------
--------+
| Screen and keyboard|
| Save setup as dfl|
| Save setup as..|
| Exit|
| Exit from Minicom|
+---------------------------+


(Select 'Save setup as dfl' after changing serial port setting is
done.)
```

2 Prepare a network equipment that supports IPMC Profile/Snooping/Proxy and MVR.

3 Connect the computer and the equipment with serial cable and network cable, and ensure both of them are running.

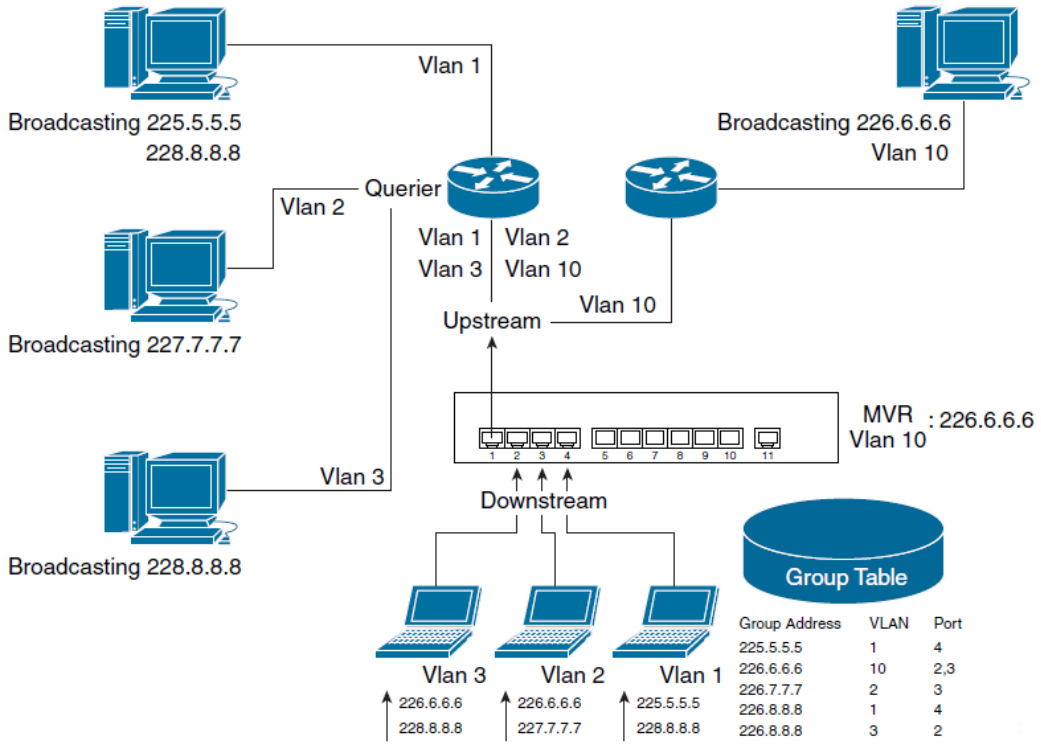
4 Confirm or set up IP configuration of equipment by using the minicom application, and then make sure the IP communication is active between equipment and computer by using PING.
(In this case, the IP address of the computer is '192.0.2.88' while the IP address of the equipment is '192.0.2.1'.)

```
$ ifconfig
eth0Link encap:EthernetHWaddr 00:10:60:76:b4:a5
inet addr:192.0.2.88 Bcast:192.0.2.255Mask:255.255.255.0 inet6
addr:fe80::210:60ff:fe76:b4a5/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500Metric:1
RX packets:793 errors:0 dropped:0 overruns:0 frame:0
```

```
TX packets:791 errors:1 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000

RX bytes:89148 (89.1 KB)TX bytes:89606 (89.6 KB)

$ minicom

Welcome to minicom 2.7

OPTIONS:I18n

Compiled on Jan 1 2014, 17:13:19. Port /dev/ttyUSB0 Press CTRL-A
Z for help on special keys

Username:admin

Password:

# show interface vlan

VLAN1

LINK:00-22-6f-00-c2-70 Mtu:1500 <UP BROADCAST RUNNING MULTICAST>
IPv4:192.0.2.1/24 192.0.2.255

IPv6:fe80::201:c1ff:fe00:c270/64 <UP RUNNING>

# ping ip 192.0.2.88

PING server 192.0.2.88, 56 bytes of data.

64 bytes from 192.0.2.88:icmp_seq=0, time=10ms

64 bytes from 192.0.2.88:icmp_seq=1, time=0ms

64 bytes from 192.0.2.88:icmp_seq=2, time=0ms

64 bytes from 192.0.2.88:icmp_seq=3, time=0ms

64 bytes from 192.0.2.88:icmp_seq=4, time=0ms Sent 5 packets,
received 5 OK, 0 bad

#
```

The following topology illustration is used to demonstrate the examples, which assume the device boots up with its default configuration. It also demonstrates the final group registration results after completing the examples.

Figure IPMC Configuration Example Topology




## Deploy IPMC Profile for Filtering Multimedia Stream

The IPMC profile is set primarily to provide the access control in multicast learning and thus managing forwarding. Therefore we expect only the address ranges from 225.0.0.0 to 228.255.255.255 will be handled by SWITCH. We will then create an IPMC profile and use this profile for filtering IGMP group registration.

```
# configure terminal

(config)# ipmc range SuperSet 225.0.0.0 228.255.255.255 (config)#
ipmc profile Demonstration

(config-ipmc-profile)#     range     SuperSet     permit     log
(config-ipmc-profile)# exit

(config)# ipmc profile

(config)# do show ipmc profile detail

IPMC    Profile    is    now    enabled    to    start    filtering.
Profile:Demonstration (In IGMP Mode) Description:

HEAD-> SuperSet (Permit the following range and log the matched
entry) Start Address:225.0.0.0

End Address:228.255.255.255

IGMP    will    deny    matched    address    between    [224.0.0.0    <->
224.255.255.255] IGMP will permit and log matched address between
[225.0.0.0 <-> 228.255.255.255]

IGMP    will    deny    matched    address    between    [229.0.0.0    <->
239.255.255.255] MLD will deny matched address between [ff00::<->
ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff]
```

```
(config)# interface *

(config-if)# ip igmp snooping filter Demonstration

(config-if)# exit

(config)# ip igmp snooping vlan 1 (config)# interface vlan 1
(config-if-vlan)# ip igmp snooping

(config-if-vlan)# exit (config)# ip igmp snooping

(config)# do show ip igmp snooping detail

IGMP Snooping is enabled to start snooping IGMP control plane.
Multicast streams destined to unregistered IGMP groups will be
flooding.

Switch-1 IGMP Interface Status

IGMP snooping VLAN 1 interface is enabled.

Querier status is ACTIVE (Administrative Control:Join
Querier-Election)

Startup Query Interval:25 seconds; Startup Query Count:1

Querier address is not set and will use system's IP address of this
int erface. Active IGMP Querier Address is 0.0.0.0

PRI:0 / RV:2 / QI:125 / QRI:100 / LMQI:10 / URI:1

RX IGMP Query:0 V1Join:0 V2Join:0 V3Join:0 V2Leave:0 TX IGMP Query:0
/ (Source) Specific Query:0

IGMP RX Errors:0; Group Registration Count:0

Compatibility:IGMP-Auto / Querier Version:Default / Host
Version:Default

Older Version Querier Present Timeout:0 second Older Version Host
Present Timeout:0 second (config)# end

#
```

## Snooping IPv4 Multicast Registration in Different VLAN

Assume that the connected hosts separate into different VLAN for management purposes. VLAN configuration and IGMP snooping need to be set up at the same time.

```
# configure terminal

(config)# vlan 2

(config-vlan)# exit (config)# vlan 3 (config-vlan)# exit

(config)# interface GigabitEthernet 1/4 (config-if)# switch mode
access (config-if)# switch access vlan 1

(config-if)# interface GigabitEthernet 1/3 (config-if)# switch
mode access (config-if)# switch access vlan 2

(config-if)# interface GigabitEthernet 1/2 (config-if)# switch
mode access (config-if)# switch access vlan 3
```

```
(config-if)# interface GigabitEthernet 1/1 (config-if)# switch mode trunk (config-if)# switch trunk native vlan 1

(config-if)# swtich trunk allowed vlan 1,2,3 (config-if)# exit

(config)# ip igmp snooping vlan 2 (config)# ip igmp snooping vlan 3 (config)# interface vlan 1-3 (config-if-vlan)# ip igmp snooping (config-if-vlan)# exit (config)# ip igmp snooping

(config)# do show ip igmp snooping detail

IGMP Snooping is enabled to start snooping IGMP control plane. Multicast streams destined to unregistered IGMP groups will be flooding.

Switch-1 IGMP Interface Status

IGMP snooping VLAN 1 interface is enabled.

Querier status is ACTIVE (Administrative Control:Join Querier-Election

)

Querier Up time:3190 seconds; Query Interval:91 seconds

Querier address is not set and will use system's IP address of this int erface. Active IGMP Querier Address is 10.9.52.198

PRI:0 / RV:2 / QI:125 / QRI:100 / LMQI:10 / URI:1

RX IGMP Query:0 V1Join:0 V2Join:0 V3Join:0 V2Leave:0

TX IGMP Query:3 / (Source) Specific Query:0

IGMP RX Errors:0; Group Registration Count:0

Compatibility:IGMP-Auto / Querier Version:Default / Host Version:Default Older Version Querier Present Timeout:0 second Older Version Host Present Timeout:0 second IGMP snooping VLAN 2 interface is enabled.

Querier status is ACTIVE (Administrative Control:Join Querier-Election

)


Startup Query Interval:24 seconds; Startup Query Count:1

Querier address is not set and will use system's IP address of this int erface. Active IGMP Querier Address is 0.0.0.0

PRI:0 / RV:2 / QI:125 / QRI:100 / LMQI:10 / URI:1

RX IGMP Query:0 V1Join:0 V2Join:0 V3Join:0 V2Leave:0 TX IGMP Query:1 / (Source) Specific Query:0

IGMP RX Errors:0; Group Registration Count:0

Compatibility:IGMP-Auto / Querier Version:Default / Host Version:Default
```

```
Older Version Querier Present Timeout:0 second Older Version Host Present Timeout:0 second IGMP snooping VLAN 3 interface is enabled.

Querier status is ACTIVE (Administrative Control:Join Querier-Election

)

Startup Query Interval:24 seconds; Startup Query Count:1

Querier address is not set and will use system's IP address of this int erface. Active IGMP Querier Address is 0.0.0.0

PRI:0 / RV:2 / QI:125 / QRI:100 / LMQI:10 / URI:1

RX IGMP Query:0 V1Join:0 V2Join:0 V3Join:0 V2Leave:0 TX IGMP Query:1 / (Source) Specific Query:0

IGMP RX Errors:0; Group Registration Count:0

Compatibility:IGMP-Auto / Querier Version:Default / Host Version:Default Older Version Querier Present Timeout:0 second Older Version Host Present Timeout:0 second (config)# end

#
```

## Deploy MVR and IGMP Snooping at The Same Time

Create another IPMC profile and a new MVR VLAN to deploy an MVR VLAN over the existing network with permitting gaming group in range 226.0.0.0/8 (226.0.0.0 ~ 226.255.255.255). In this example, MVR VLAN ID is set as 10 and this MVR VLAN only forwards the multicast stream in the channel to subscribers.

```
# configure terminal

(config)# ipmc range Game 226.0.0.0 226.255.255.255 (config)# ipmc profile Game (config-ipmc-profile)# range Game permit log

(config-ipmc-profile)# exit

(config)# ipmc profile

(config)# do show ipmc profile detail


IPMC Profile is now enabled to start filtering. Profile:AN1135 (In IGMP Mode) Description:Demonstration for Configuration Guides AN1135

HEAD-> Audio (Permit the following range and log the matched entry) Start Address:225.1.1.1

End Address :225.222.222.222

NEXT-> Video (Permit the following range) Start Address:227.3.3.3 End Address :228.123.123.123

NEXT-> Data (Permit the following range) Start Address:238.0.0.0 End Address :239.255.255.255

IGMP will deny matched address between [224.0.0.0 <-> 225.1.1.0]
```

```
IGMP will permit and log matched address between [225.1.1.1 <->
225.222.222.222]

IGMP will deny matched address between [225.222.222.223 <->
227.3.3.2] IGMP will permit matched address between [227.3.3.3 <->
228.123.123.123

]

IGMP will deny matched address between [228.123.123.124 <->
237.255.255.255]

IGMP will permit matched address between [238.0.0.0 <->
239.255.255.255

]

MLD will deny matched address between [ff00::<->
ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff]

Profile:Demonstration (In IGMP Mode) Description:

HEAD-> SuperSet (Permit the following range and log the matched
entry) Start Address:225.0.0.0

End Address :228.255.255.255

IGMP will deny matched address between [224.0.0.0 <->
224.255.255.255] IGMP will permit and log matched address between
[225.0.0.0 <-> 228.255.255.255]

IGMP will deny matched address between [229.0.0.0 <->
239.255.255.255] MLD will deny matched address between [ff00::<->
ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff]

Profile:Game (In IGMP Mode) Description:

HEAD-> Game (Permit the following range and log the matched entry)
Start Address:226.0.0.0

End Address :226.255.255.255

IGMP will deny matched address between [224.0.0.0 <->
225.255.255.255] IGMP will permit and log matched address between
[226.0.0.0 <-> 226.255.255.255]

IGMP will deny matched address between [227.0.0.0 <->
239.255.255.255] MLD will deny matched address between [ff00::<->
ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff]

(config)# mvr vlan 10 name Game (config)# mvr name Game channel
Game (config)# mvr

(config)# do show mvr detail

MVR is now enabled to start group registration. Switch-1 MVR-IGMP
Interface Status

IGMP MVR VLAN 10 (Name is Game) interface is enabled. Querier status
is IDLE ( Forced Non-Querier )

Querier Expiry Time:255 seconds
```

```
IGMP address is not set and will use system's IP address of this
interf ace. Control frames will be sent as Tagged

PRI:0 / RV:2 / QI:125 / QRI:100 / LMQI:5 / URI:1

RX IGMP Query:0 V1Join:0 V2Join:0 V3Join:0 V2Leave:0 TX IGMP Query:0
/ (Source) Specific Query:0

IGMP RX Errors:0; Group Registration Count:0 Port Role Setting:

Inactive Port:Gi 1/1,Gi 1/2,Gi 1/3,Gi 1/4,Gi 1/5,Gi 1/6,Gi 1/7,Gi
1/8, Gi 1/9,2.5G 1/1,2.5G 1/2

Interface Channel Profile:Game (In IGMP Mode) Description:

HEAD-> Game (Permit the following range and log the matched entry)
Start Address:226.0.0.0

End Address:226.255.255.255 Switch-1 MVR-MLD Interface Status

MLD MVR VLAN 10 (Name is Game) interface is enabled. Querier status
is IDLE ( Forced Non-Querier )

Querier Expiry Time:255 seconds

MLD address will use Link-Local address of this interface. Control
frames will be sent as Tagged

PRI:0 / RV:2 / QI:125 / QRI:100 / LMQI:5 / URI:1

RX MLD Query:0 V1Report:0 V2Report:0 V1Done:0 TX MLD Query:0 /
(Source) Specific Query:0 MLD RX Errors:0; Group Registration
Count:0 Port Role Setting:

Inactive Port:Gi 1/1,Gi 1/2,Gi 1/3,Gi 1/4,Gi 1/5,Gi 1/6,Gi 1/7,Gi
1/8, Gi 1/9,2.5G 1/1,2.5G 1/2

Interface Channel Profile:Game (In IGMP Mode) Description:

HEAD-> Game (Permit the following range and log the matched entry)
Start Address:226.0.0.0

End Address:226.255.255.255 (config)# end

#
```

Notes

In this topology, group address destined to addresses not included in the SuperSet will be flooding. Data destined to 225.5.5.5 from VLAN 1 will be forwarded to port 4. Data destined to 226.6.6.6 from VLAN 10 will be forwarded to port 2 & 3. Data destined to from VLAN 2 will be forwarded to port 3. Data destined to 228.8.8.8 from VLAN 1 will be forwarded to port 4. Data destined to 228.8.8.8 from VLAN 3 will be forwarded to port 2.

# 19 HTTPS Setting

This document demonstrates how to set up HTTPS for secure communication between http client (usually a web browser) and http server using ICLI commands.

Using ICLI as the management interface requires a serial console connection between the device and management platform. No network connection is required to use ICLI, but the terminal emulator software has to be installed.

The HTTPS functionality is meant for secure communication between a browser (management console) and a web server (switch). The included self-signed certificate may trigger a browser warning that the certificate is not issued by a trusted source. The certificate upload mechanism in the switch software enables use of a trusted third-party certificate.

## 19.1 Understanding HTTPS

HTTPS (Hypertext Transfer Protocol Secure) is a method for securing HTTP data transfer over a TCP/IP network. It adds the security capabilities of SSL/TLS to standard HTTP communications between an HTTP client (usually a web browser) and an HTTP server (usually a web server). The main motivation for HTTPS is to prevent man-in-the-middle attacks or eavesdropping.

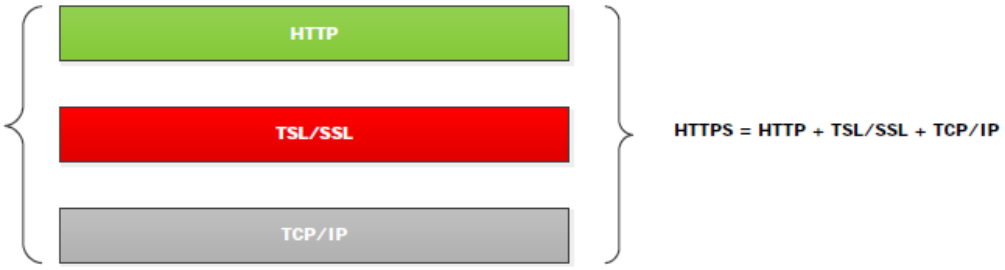
### Restrictions for HTTPS

Per HTTP communication models, the host (web server) addresses and port numbers are necessarily part of the underlying TCP/IP protocols. HTTPS cannot protect their disclosure but encrypts the content of the HTTP data (payload)- that means an eavesdropper can infer the IP address, domain name, and port number of the web server but not the content of the applications.

### HTTPS Working Model

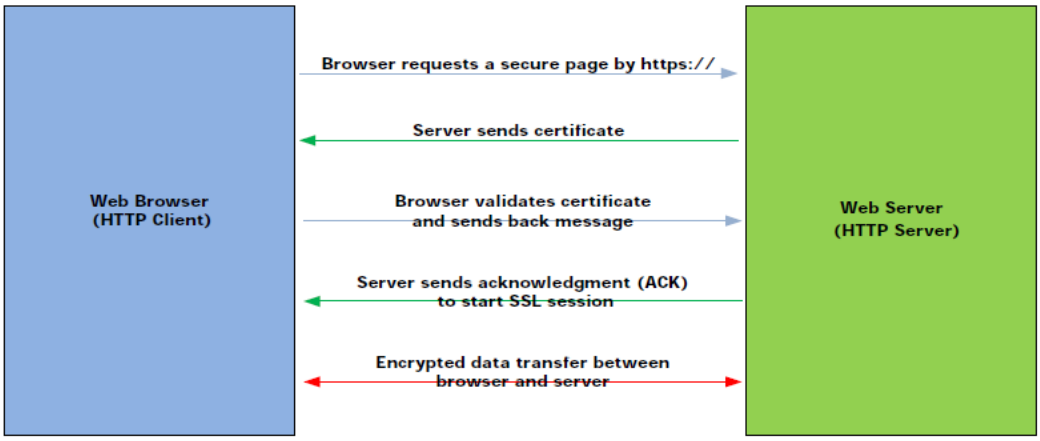
- Protocol layering: HTTPS is a mechanism to layer HTTP on top of SSL/TLS and to add securities capabilities to HTTP application.

Figure 1 • Protocol Layering




- Authentication: The web browser requires a server certificate from the web server before an SSL/TLS connection is established. An SSL/TSL connection is required before HTTPS data transfer can commence.
- Encryption: Once an SSL connection is established, data transfer is encrypted with a public key provided by a security certificate.

Figure 2 • Encryption




## 19.2 Configuration Prerequisites

This section lists the prerequisites for configuring and/or monitoring operations on devices using the management platform.

- Computer with (USB) RS-232 connector and NIC card
- Terminal emulator software that supports the serial port
- Serial port parameters, as follows:
  - Baud rate 115200
  - Data bit: 8 bits
  - Stop bit: 1 bit
  - Flow control: deny
  - parity check: no

## 19.3 Configuring HTTPS

HTTPS is enabled by default in SWITCH. A web browser can access a switch at https://ip-address-of-switch/. This section provides guidelines for changing configurations for a switch booted-up using the default settings.

To configure HTTPS using ICLI, connect a serial RS-232 cable with the switch while the terminal console software is running on host.

## HTTPS Default Setting and Configurable Value Range

The following table provides details of the HTTPS default setting and configurable value range.

Table 1 • HTTPS Default Setting and Configurable Value Range

| Configuration | Default Value | Configurable Value |
|---|---|---|
| Mode | Enable | Enabled, Disabled |
| Automatic Redirect | Disabled | Enabled, Disabled |
| Certificate Maintain | None | None, Delete, Upload, Generate |
| Certificate Algorithm | RSA | RSA |
| PassPhrase | None | A string pattern |
| Certificate Upload | Browser | Web Browser, URL |
| Certificate Status | N/A | Non-configurable |

## Setting up HTTPS Using ICLI

Setting up HTTPS is a multi step process, as described.

## Enable HTTPS

```
!  Enters global configuration mode

!  configure terminal

!  Enables the HTTPS

(config)# ip http secure-server

HTTPS mode is enabled and the browser can request a secure data
via https://
```

## Automatically Redirecting the Web Browser to the HTTPS Mode

```
Enters global configuration mode

# configure terminal

Enables automatic redirect

(config)# ip http secure-redirect

HTTPS automatic redirect is enabled
```

## Maintaining Certificate

```
Disable HTTPS

(config)# no ip http secure-server

Delete HTTPS certificate

(config)# ip http secure-certificate delete
```

```
HTTPS certificate is now deleted
```

## Generating a New Certificate to Replace the Current Certificate

```
Disable HTTPS
(config)# no ip http secure-server
Generate HTTPS certificate with RSA or DSA
To generate certificate with RSA algorithm:
(config)# ip http secure-certificate generate RSA
or
To generate certificate with DSA algorithm.
(config)# ip http secure-certificate generate DSA
HTTPS certificate is now generated
```

## Uploading a Third-Party Certificate Externally to Replace the Current One

```
Disable HTTPS
(config)# no ip http secure-server
Upload certificate from tftp or http servers, below is an example for uploading a named 3rd-party certificate, https_server_certificate.pem from tftp server whose IP address is 10.0.0.123
(config)# ip http secre-certificate upload \
tftp://10.0.0.123/https_server_certificate.pem
 HTTPS certificate is now uploaded
```

Notes

Disable HTTPS before uploading, generating, or deleting a certificate. Enable HTTPS after completing the process.

# 20 Appendix One: Safety Reinforcement Configuration

## 20.1 Storm Suppression

### Risk Statement

The switch receives all data frames on the network segment, learns according to the source MAC addresses in the data frames, builds a MAC address table, and stores the corresponding relationship between MAC addresses and ports. For the received data frames, if the switch can find the destination MAC address in the MAC address table, it will forward the frames at Layer 2 based on the destination MAC address, thus isolating the collision. If the destination address is not in the MAC address table, the switch will send broadcast to all ports except the receiving port, which may lead to broadcast storm in the network.

### Solution

In most scenarios of Layer 2 networks, unicast traffic should be much larger than broadcast traffic, which is also a prerequisite for using switches for networking. However, if broadcast traffic is not restricted, when broadcast traffic exists in large quantities, it will consume a lot of network bandwidth, resulting in the decline of network performance and even communication interruption. If the broadcast traffic generated is restricted in the switch, it can still ensure that the device can leave a part of bandwidth for ordinary unicast forwarding when the broadcast traffic surges.

### Configuration Instance

Set the suppression value of broadcast, multicast and unknown unicast to 16kfps.

```
(config)# qos storm broadcast fps 16
(config)# qos storm multicast fps 16
(config)# qos storm unicast fps 16
```

Save configuration

```
(config)# exit
```

```
# copy running-config startup-config
```

# 20.2 Rate Limit of Reported CPU Message

## Risk Statement

In the network, there will be a large number of messages that need to be sent to the CPU for processing, some of which are malicious attack messages against the CPU; When the network loop causes broadcast storm, some layer 2 protocol messages form storm in the network, and these protocol messages need to be reported to CPU for processing. Too many messages are reported to CPU, which will lead to high CPU occupancy rate, performance degradation and affect normal services. Malicious attack messages against CPU (frequently sending messages) will lead to CPU overload, which will affect the normal operation of other services and even lead to system interruption.

## Solution

Filter the reported messages and limit its rate to avoid CPU overload. Discard the messages that do not conform to the rules, and limit the speed of protocol messages that conform to the rules on the CPU interface (such as port speed limit and speed limit of queue level ). At the same time, ACL can be used to finely control some special protocol flows, thus ensuring the CPU's processing of normal services.

## Configuration Instance

The corresponding rate and flow control has been configured by default on the CPU interface and its 8 queues by reported CPU messages, and no manual configuration is required; For encryption and decryption protocol messages (HTTPS, SSH, etc.) that require CPU to perform extra high-burden calculation, traffic control can be performed through ACL.

Configure the rate of rate-limiter 1 to 500pps.

```
(config)# access-list rate-limiter 1 pps 500
```

ace1 limits the https message rate to 500pps.

```
(config)# access-list ace 1 frame-type ipv4-tcp dip
192.168.1.254/32 dport 443 rate-limiter 1
```

Save configuration

```
(config)# exit

# copy running-config startup-config
```

# 20.3 Isolate the Management Plane from the User Plane

## Risk Statement

In order to improve compatibility and management convenience, the user plane and management plane of the switch are not isolated by default. Users can log in and manage devices through the service interface, which objectively increases the possibility of being attacked, and attackers can easily try to attack the management plane through the service interface.

## Solution

Users can isolate the user plane and the management plane by configuring ACL to protect the management plane from external attacks.

## Configuration Instance

Isolation between in-band management and user plane can be realized by ACL configuration:

- For in-band management VLAN: only management data (HTTPS, SSH, SNMP) are allowed to access by configuring ACL entries, while other data are denied access.
- For the user plane VLAN: configure ACL entries to deny the user VLAN access to the management data of the device (HTTPS, SSH, SNMP).

for example: The management plane is VLAN 1, the device management IP is 192.168.1.254, and the user plane is VLAN 2.

- Complete the following configurations in order: configure VLAN 1 to access devices via HTTPS
- Configure VLAN 1 to access devices via SSH
- Configure VLAN 1 to access devices via SNMP.
- Configure other data of VLAN 1 not to access devices.
- Configure VLAN 2 not to access devices via HTTPS.
- Configure VLAN 2 not to access devices via SSH.
- Configure VLAN 2 not to access devices via SNMP.
- Save configuration

```
(config)# access-list rate-limiter 1 100kbps 5

(config)# access-list ace 1 next 2 vid 1 frame-type ipv4-tcp dport
443

(config)# access-list ace 2 next 3 vid 1 frame-type ipv4-tcp dport
22

(config)# access-list ace 3 next 4 vid 1 frame-type ipv4-udp dport
161

(config)# access-list ace 4 next 5 vid 1 action deny
```

```
(config)# access-list ace 5 next 6 vid 2 frame-type ipv4-tcp dip
192.168.1.254/32 dport 443 action deny

(config)# access-list ace 6 next 7 vid 2 frame-type ipv4-tcp dip
192.168.1.254/32 dport 22 action deny

(config)# access-list ace 7 vid 2 frame-type ipv4-udp dip
192.168.1.254/32 dport 161 action deny

(config)# exit

# copy running-config startup-config
```


Notice

According to ACL priority, the location of entry that deny access by VLAN1 should be arranged after the entires of HTTPS, SSH and SNMP that allow access by VLAN1.

# 20.4 SNMP

## Risk Statement

The management protocols of plaintext transmission, such as SNMPv1 and SNMPv2, have the risk of information leakage in use.

## Solution

Use the secure encryption management protocol SNMPv3.

## Security Configuration

SNMP is a protocol used for network device management. Only SNMP v3 version is currently supported. SNMPv3 supports the security mechanism of USM (User-based Security Model). By authenticating and encrypting the communication data, SNMP v3 can prevent messages from being disguised, tampered and leaked. For security reasons, it is recommended to configure authenticated and encrypted v3 users and use v3 authentication encryption to manage switches. The access right of users are restricted by associating ACL and MIB views with users.


Notes

The length of the authentication password and privacy password string must be greater than or equal to 8 and be composed of two or more of uppercase letters, lowercase letters, numbers and special characters.

## Configuration Instance

Step 5 Create V3 user user1; Set the authentication mode to MD5 and the authentication password to admin123; Set the encryption mode to AES and the privacy password to admin345

```
mydevice(config)# snmp user user2 engine-id 800007e5017f000003 md5
priv aes


Auth Password Set
   Please enter the new Password:
   Enter the Password again:


Private Password Set
   Please enter the new Password:
   Enter the Password again:
The MD5 and AES protocol has security risks. Please use it caution.
```

Step 6 Create V3 user group, as shown in the following figure.

```
(config)# snmp  security-to-group model v3 name user1 group group1
```

Step 7 Create the view node view1.

```
(config)# snmp view  view1 .1.3.6.1 include
```

Step 8 Configure V3 user group access view, as shown in the following figure.

```
(config)# snmp access group1 model v3 level priv read view1 write
view1
```

Step 9 Save configuration

```
(config)# end
# copy running-config startup-config
Building configuration...
% Saving 5615 bytes to flash:startup-config
```

Step 10 End.

# 20.5 Login to Switch via WEB Network Management

## Risk Statement

As a management protocol for plaintext transmission, HTTP has the risk of information leakage when users use this protocol.

## Solution

Use the secure encryption management protocol HTTPS.

## Security Configuration

Device provides secure transmission services to prevent the transmitted data from being intercepted. Due to the security risk of HTTP, this device does not support

logging in to the WEB network management through HTTP. A switch only supports logging in to the Web management via secure HTTP ( that is HTTPS), but does not support logging in to the Web management via HTTP. The HTTPS server receives login connection requests from all interfaces by default, which poses security risks. It is recommended to use access management to restrict access to customers. After successfully specifying the access IP of HTTPS server, only the specified IP address is allowed to log in to the device, and the access of other addresses will be rejected.

## Configuration Instance: Access Control Configuration

According to the access control configuration, the IP address of the client accessing the device is restricted to 192.168.1.100-192.168.1.110, and the client can access the device through HTTPS, SNMP, SSH, etc.

```
(config)# access management 1 1 192.168.1.100 to 192.168.1.110 all
(config)# end
# copy running-config startup-config
Building configuration...
% Saving 5615 bytes to flash:startup-config
```

## Configuration Instance: Enable HTTPS

Enable HTTPS with the following command.

```
(config)# ip http secure-server
```

Save configuration with the following command.

```
(config)# exit
# copy running-config startup-config
Building configuration...
% Saving 5376 bytes to flash:startup-config
```

3onedata


3onedata Co., Ltd.
Headquarter address: 3/B, Zone 1, Baiwangxin High Technology Industrial Park, Song Bai Road, Nanshan District, Shenzhen, 518108, China
Technical support: tech-support@3onedata.com
Service hotline: +86-400-880-4496
Official Website: http://www.3onedata.com