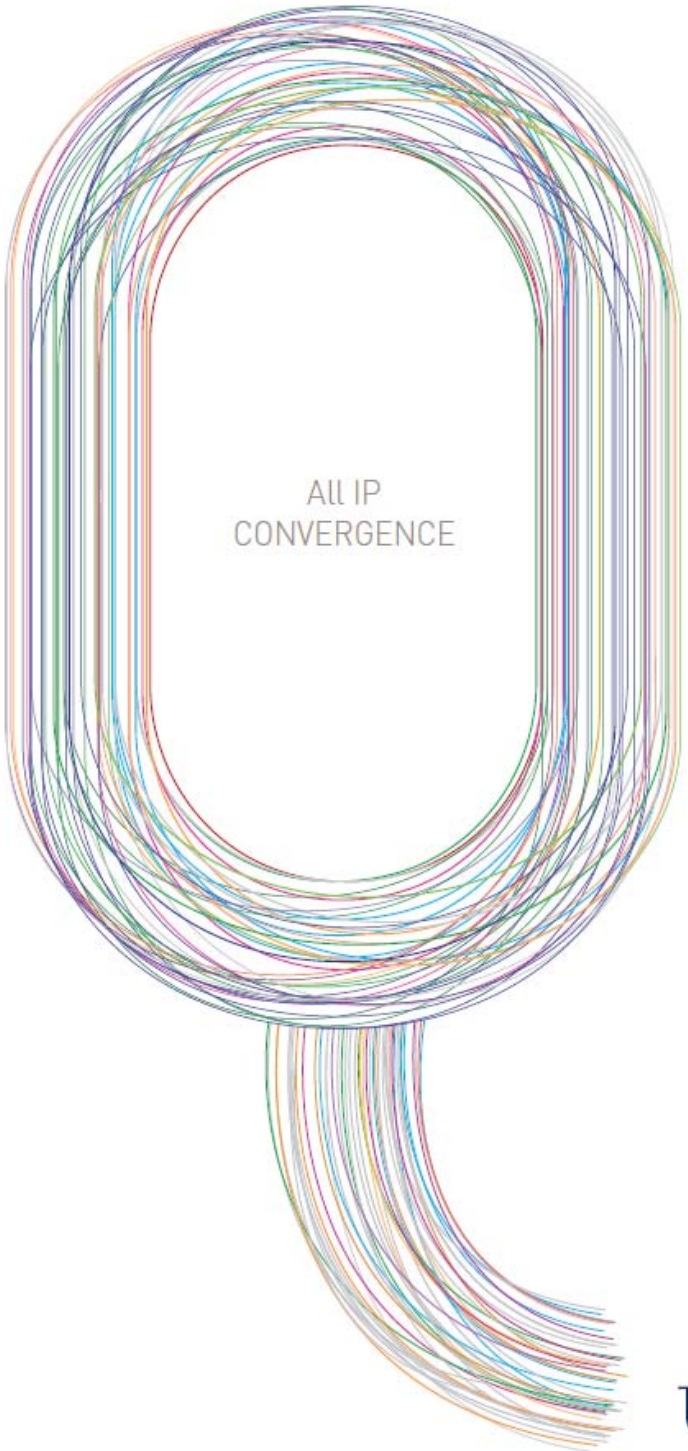
PON
ONU

E3208E

■ User Guide



ubiQuoss

E3208E

■ User Guide

UbiQuoss Inc.
24F Millennium B/D, 467-12 Dogok-Dong
Gangnam-Gu, Seoul 135-700 Korea
TEL: +82-70-8666-5000
FAX: +82-2-2190-3201
E-mail: oversea.team@ubiQuoss.com
www.ubiQuoss.com

Preface

This preface provides the overview of E3208E user guide, which describes guide conventions, and lists other publications that may be useful.

Introduction

This guide is intended to provide the information needed for network environment setup and operation of E3208E ONU.

This guide is for Ethernet-based network operators and involved engineers. Using this guide, network operator will be able to build an optimal network and operate and manage the network more efficiently. Therefore, readers of this guide are assumed to have basic understanding of the following subjects:

- Local Area Networks (LAN) and Metro Area Network (MAN)
- Concepts of Ethernet, high speed Ethernet and Giga-bit Ethernet
- Concept of Ethernet switching and bridging
- Concept of TCP/IP protocol
- Simple Network Management Protocol (SNMP)

Related Documents

For additional information on this equipment, refer to the following manual.

Manual	Contents
Hardware Installation Guide	Hardware installation Initial operating environment configuration

History of Document

Date	Version
2012. 06	First Edition

Symbols in this Guide

The symbols below are used to indicate the product names and notes in the user guide.

Description of Symbols

The installation guide uses the following icons and fonts to indicate special messages for the reader.

	Note	Presents the useful contents related to the user guide, the references and data related to the product use, etc.
	Caution	Describes the situation that data loss and incorrect product operation can occur, and provides the proper actions to take in the situation.
	Warning	Describes the situation that product damage and the user's injury can occur, and provides the proper actions to take in the situation.

Organization

The summary of each part is described below.

Chapter 1. Introduction

This chapter provides the information required for system operator to set up an operating environment and to get started with the E3208E ONU.

Chapter 2. Interface Environment Setup

This chapter describes interface environment configuration.

Chapter 3. VLAN

Virtual LAN (VLAN) logically groups network users and resources connected to the switch ports. VLAN facilitates network management consuming much time and improves efficiency of network through broadcast traffic control.

Chapter 4. IP Environment

This chapter describes how to set IP addresses.

Chapter 5. DHCP Relay and Client

This chapter describes how to set DHCP Relay and DHCP Client.

Chapter 6. IGMP Snooping

This chapter describes IGMP Snooping in the E3208E ONU.

Chapter 7. STP and SLD

This chapter describes how to define Spanning Tree Protocol (STP) and Rapid Spanning Tree Protocol (RSTP) and to configure the Self-Loop Detection (SLD) features.

Chapter 8. CPU-Filter & SYSCTL

The E3208E ONU supports filtering of the incoming traffic to the switch and the traffic forwarded by the switch CPU. Using the following commands, you can set filtering by IP address, by protocol and by port.

Chapter 9. Static Monitoring & QoS

This chapter describes the administration and management function through RMON (Remote Monitoring) to monitor the current status of the E3208E ONU and to display the log information on the screen.

Chapter 10. Saving Configuration and Upgrading Software

This chapter describes flash file system management for the system. The flash file system stores the OS image and configuration files of the system, which will be loaded to the system upon system booting.

Chapter 11. Utility

This chapter describes other functions required for operation of the system.

Chapter 12. DAI

This chapter describes the function of dynamic Address Resolution Protocol (ARP) inspection (DAI) which is used for inspecting ARP packet.

Chapter 13. Auto-Reset

This chapter describes how to set reset function when equipment has specific situation or some problem.

Table of Content

List of Table

List of Figure

Chapter 1. Introduction

This chapter provides the information required for system operator to set up an operating environment and to get started with the E3208E ONU.

- Edit and help functions
- Command modes
- E3208E operation
- E3208E user interface
- Setting switch login and password
- SNMP environment setup
- Viewing and saving switch files and environment settings
- Access list
- Telnet client

Edit and Help Functions

This section describes the edit and help functions of the command editor.

Understanding Command Syntax

This chapter describes a procedure to enter commands for system operation. Details of using command interface will be described in the next chapter.

You can use command line interface as follows:

1. Before entering a command in the command prompt, ensure that you are authorized to the prompt level. Most commands related to environment setup require authentication in system operator level.
2. Enter a command to run. Go to Step 3 if you want to enter a sub-command or if no parameter values are required for the command entered.

   - If the command has a parameter, enter the parameter name and value.

   - Number, character string or address will be defined depending on the parameter of command.

3. When you completed the command input, press [Return] to run the command.

Notice The message "% Command incomplete." may be displayed when you run the entered command. This means that the parameters required for running the command have not been entered exactly, and the command entered would not be executed in such a case. Press the up arrow to view the command entered last.

The following shows an example where the command parameter is not entered exactly.

```
Switch# show ↵
% Command incomplete.
Switch#
```

Command Syntax Helper

Command Line Interface (CLI) of the E3208E is equipped with a command syntax helper. If you are not aware of the complete syntax of a command, you can display help by pressing '?'. The E3208E provides the two help functions:

Help All

- Provides help for the list of all parameters and values permitted. A space should be given after the entered command.

Help command

- Provides help for a short parameter entered by the operator. No space should be given after the entered command.

The following shows an example of help all using the command ‘show’. If you enter “?” along with a space following the show command, the list of all parameters and values permitted will be displayed. Then, the cursor will blink in the “Switch# show” prompt, waiting for user input. ‘?’ of the user input does not appear on the screen.

```
Switch# show ?
access-list             access list entry
arp                     Display ARP table entries
clock                   show current system's time
config                  Show config file information
cpu                     CPU information
debugging               Debugging functions
filter                  filter setting
flash                   display information about flash file system
flow-rule               flow-rule
interface               Interface status and configuration
ip                      IP information
logging                 Show all contents of logging buffers
mac-address-table       Display MAC address table entries
mac-count               MAC count configuration
memory                  Memory statistics
mirroring               Port mirroring configuration
ntp                     show current ntp status
port                    Port status and configuration
port-group              Port-group configuration
privilege               Display your current level of privilege
qos                     Qos configuration
rate-limit              Display rate-limit control parameters
rmon                    Remote Monitoring
running-config          Current operating configuration
service-policy          service-policy information
spanning-tree           Spanning tree topology
stack                   Show stacking information
startup-config          Show startup config file information
switchport              Switching port configuration
system                  Display the system information
uptime                  Display elapsed time since boot
users                   Display information about terminal lines
version                 Display the system version
vlans                   VLAN information

Switch# show_
```

The following shows an example of help command using the command ‘show’. If you enter ‘?’ after the show command without a space, the show command will be explained as seen below and the cursor will blink, waiting for user input.

```
Switch# show?
  show    Show running system information
Switch# show_
```

In the example, assume that you are not aware of the exact command to display port status. If you enter ‘p’ and press ‘?’ without a space, the subcommands beginning with ‘p’ will be listed as seen below. Then, the command you entered will be displayed and the cursor will blink, waiting for user input.

```
Switch# show p?
  port                Display port configuration
  port-group          Port group information
  privilege           Display your current level of privilege
Switch# show p_
```

Short Command Input

CLI of E3208E ONU supports execution of a short command without entering the complete command and parameter. You can execute a short command by entering the first two or three characters of a command.

Notice When using a short command, you should enter enough characters for the E3208E ONU to identify the entered command. A message “% Ambiguous command.” indicates that there is more than one command having the same prefix with the entered characters.

```
Switch# show i↵
% Ambiguous command.

Switch# show i ?
  ip                  IP information
  logging             Show all contents of logging buffers
Switch# show i_
```

Command Symbol

Various symbols are used for the system command syntax described in this guide.
Command symbol describes the syntax of parameter to be entered for command execution.
<Table 1> describes the symbols used for system command syntax.

<Table 1> Command Symbols

Symbol	Name	Description
<>:	Angle brackets	Indicates a variable or a value in command syntax. The parameter represented like this should be entered inevitably. In the example of a command given below, a value between 1-99 should be entered for standard IP access control list number: **access-list <1-99> (deny|permit) *address***
():	Braces	List of parameters or values used in command syntax System operator should enter one or more items of those included in the list. In the example of a command given below, qos-queue-map or qos-remarking should be specified for QoS method: **qos (*cos-queue-map*|*cos-remarking*)**
[]:	Square brackets	List of parameters or values used in command syntax The system operator should enter the items selected from those included in the list. Depending on cases, no items may be entered. For example, interface name may not be defined for a command given below: **show interfaces [*ifname*]**
|:	Vertical bar	Represents exclusive parameters in the parameter list
Italic		Input variables
Bold		Command to be entered by user
A.B.C.D		Indicates an IP address or a subnet mask
A.B.C.D/M		IP prefix (e.g. 192.168.0.0/24)

Command Line Edit Keys and Help

The E3208E ONU provides edit functions similar to Emacs. <Table 2> describes the command line edit and help functions provided by the operating terminal.

<Table 2> Command Line Edit and Help Functions

Command	Description
[Ctrl] + [A]	Moves the cursor to the start of the current line.
[Ctrl] + [E]	Moves the cursor to the end of the current line.
[Ctrl] + [B]	Moves the cursor backward a character.
[Ctrl] + [F]	Moves the cursor forward a character.
Backspace	Deletes the previous character of the cursor.
[Ctrl] + [K]	Deletes the characters from the cursor to the end of the current line.
[Ctrl] + [U]	Deletes the characters from the cursor to the start of the

	current line.
Tab	If [tab] is pressed after part of a command is entered, the list of commands will be displayed provided that there are several commands with the same prefix. If there is just one command, the complete command will be displayed.
[Ctrl] + [P] or ↑	Displays the latest 20 commands
[Ctrl] + [N] or ↓	Shows the next command.
?	Lists and describes the commands available in the prompt. If '?' is entered after a command, the parameters to be entered after the command will be listed. If '?' is entered just after a short command, the commands with the same prefix will be listed
Return, Spacebar or Q	Press the Return key on -- More – to display the next line. Press the Spacebar to display the next page and press Q to exit and restore the prompt.

Command Modes

The E3208E ONU supports various command modes as seen in <Table 3>. Users are authorized for each command mode.

<Table 3> Switch Command Modes

Mode	Prompt	Description
User mode	Switch>	Typically used to display statistics data
Privileged mode	Switch#	Used to display system configuration or to apply system management commands
Config mode	Switch(config)#	Used to globally change switch environment settings
Interface mode	Switch(config-if-fa1)# Switch(config-if-vlan1)#	Used to change interface environment settings
Interface mode	Switch(config-ifrange)#	The mode to set several interface at the same time.
Range Port mode	Switch(config-range-port)#	The mode to set several interface at the same time.

Notice Command prompt uses the E3208E ONU name as the host name in front of the character string indicating each mode. In this guide, the 'Switch' prompt is used as the common host name.

You will meet several prompts while configuring an environment for the E3208E ONU. Prompt indicates the position where you are in the environment setup mode. You should check the prompt to change switch environment setup. <Table 4> describes how to move between switch command modes.

<Table 4> Movement between Command Modes

Command	Description
enable	Moves from User mode to Privileged mode The password for Privileged mode should be entered.
disable	Moves from Privileged mode to User mode
configure terminal	Moves from Privileged mode to Config mode
interface *ifname*	Moves from Config mode to Interface mode
interface range (fastethernet |gigaethernet) *ifrange*	Enters to Interface range mode.
range port	Enters range port mode.
exit	Moves to the previous mode
End	Moves from a certain mode to Privileged mode No movement occurs in User mode.

E3208E Operation

When the E3208E runs first, it carries out the self-test, loads the OS image to the memory and starts the system. When system booting is completed, it loads the previous environment settings (startup-config) stored in the flash memory.

Notice The E3208E ONU manages more than two OS images to ensure system stability. The primary OS image is loaded in default. You can change it in the boot mode or privileged mode.

User Interface

System operator can access the switch to set up switch environment, to verify environment settings and to carry out system operation and maintenance including statistics data collection. Basically, system operator can directly access the switch through the separate console port provided by the E3208E ONU (*Out-of-band management*).

It is also possible to remotely access the switch using a telnet program. No separate port is supported but the service port is used for remote telnet connection (*In-band management*).

The operator can manage the E3208E ONU using one of the following methods:

- CLI access through a terminal connected to the console port.
- CLI access over Telnet in a TCP/IP based network.
- Management through the SNMP Network Manager.

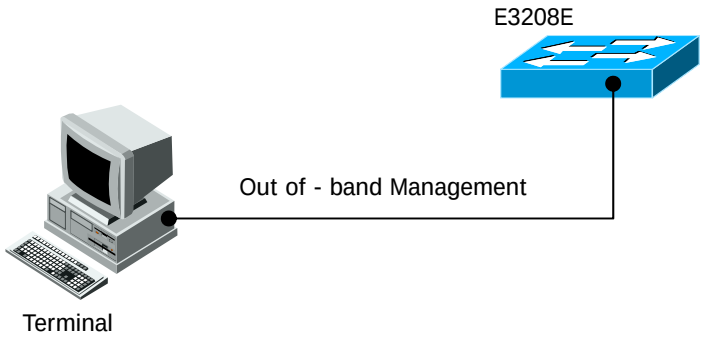
For operation and management, the E3208E ONU supports multiple links as follows:

- 1 console link
- Up to 4 telnet links

Console Connection

The CLI equipped in the system is accessible through the RJ-45 type Ethernet port. For this purpose, the operating terminal (or workstation equipped with terminal emulation software) should support 9-pin RS-232 DB9 port. The console port is mounted on the SGIM (Switching, Gigabit Ethernet I/O & Management Module) on the rear side of the E3208E ONU.

<Figure 1>, connect a terminal to the console port provided by the E3208E ONU. Then, the prompt will appear and the login process will run.



<Figure 1> Connection between a Terminal and the E3208E

Notice For details of terminal setup and console port pin settings, see the E3208E ONU hardware installation guide.

Telnet Connection

The system operator can access the E3208E through a workstation supporting TCP/IP and telnet connection. To use Telnet, the operator should define ID and password and the switch should carry more than one IP address.

telnet [<ipaddress> | <hostname>] {<port_number>}

If telnet is successfully connected, a prompt to enter password will appear. Enter your telnet password to enter User mode of the switch.

For the purpose of system security, it is possible to restrict users permitted to access Telnet using the access list. For details, see <

ACL (Access Control List)>

Connection through SNMP Network Manager

You can control the E3208E ONU through a network manager that supports the Simple Network Management Protocol (SNMP).

Notice For further information on SNMP, see <SNMP (Simple Network Management Protocol)>.

User Authentication

Adding and Deleting User

The system operator can login to the switch through the console port or over the Telnet. User registration is required for login. The E3208E can add or delete users and define password, authorization, session timeout and access list for user.

User privilege is represented in a privilege level. Privilege levels are classified into level 15 and the other levels. Privilege levels from 0 to 14 are not discriminated. Users of privilege level 15 are permitted to enter enable mode and those with privilege levels other than 15 are rejected to enter Privileged mode. A new user will be registered with privilege level 1.

Notice For further information on access list, see < ACL> section.

<Table 5> Commands for Adding and Deleting Switch Users

Command	Description	Mode
username *userID* nopassword	Creates userID No password	Config
username *userID* password *password* username *userID* password 0 *password*	Creates userID Gets non-coded password	Config
username *userID* password 7 *password*	Creates userID Gets coded password	Config
username *userID* privilege <0-15> nopassword	Creates userID No password Gets the highest privilege for privilege 15 (Permitted to enter the enable mode).	Config
username *userID* privilege <0-15> password *password* username *userID* privilege <0-15> password 0 *password*	Creates userID Gets the highest privilege for privilege 15 (Permitted to enter the enable mode). Gets non-coded password	Config
username *userID* privilege <0-15> password 7 *password*	Creates userID Gets the highest privilege for privilege 15 (Permitted to enter the enable mode). Gets coded password	Config
username *userID* timeout <0-600>	Sets session timeout (min) for each user (default 20 min)	Config
no username *userID* timeout	Deletes session timeout (min) for each user Resets session timeout to the default setting (20 min).	Config
username *userID* access-class *access-list-num*	Applies the access list to the specified user. *access-list-num* : <1-99>, indicating	Config

	standard ip access list	
no username *userID* access-class	Clears the access list applied to the user.	Config
no username *userID*	Deletes userID UserID root would not be deleted but the password will be set to the default password.	Config

Delete and Add User

```
Switch# configure terminal
Switch# configure terminal
Switch(config)# username lns nopassword
Switch(config)# username test password test
Switch(config)# username admin privilege 15 password admin
Switch(config)# username admin timeout 50
Switch(config)# end
Switch # show running-config
!
username lns nopassword
username test password 0 test
username admin privilege 15 password 0 admin
username admin timeout 50
!
Switch#
```

Setting Password

For the purpose of system security, the E3208E uses two passwords as follows.

- Enable password
  - Used for the purpose of security in Privileged mode
- User password
  - Used for access in user mode through the console or over Telnet

<Table 6> Commands for Setting Switch Enable Password

Command	Description	Mode
enable password *password*	Sets privileged mode password	Config
no enable password	Deletes privileged mode password	Config
service password-encryption	Enables password encryption mode	Config
no service password-encryption	Disables password encryption mode	Config

Notice For user password setting commands, see <Adding and Deleting User>

Setting Privileged Mode Password

```
Switch# configure terminal
Switch(config)# enable password lns
Switch(config)# end
Switch# show running-config
!
enable password 0 lns
!
Switch#
```

Setting Password Encryption

As seen in the example above, it is possible to display the defined password using the command show running-config. To prevent this, the E3208E supports setting password encryption mode.

```
Switch# configure terminal
Switch(config)# service password-encryption
Switch(config)# end
Switch# show running-config
!
enable password 7 xxEp88GxHJlgc
username lns nopassword
username test password 7 XX1LtbDbOY4/E
username admin privilege 15 password 7 xxiz1FI3TBLPs
!
Switch#
```

Setting Authentication Mode

Setting Authentication Mode upon Switch Login

The E3208E ONU supports various authentication modes for users who access the system. Typically, access privilege is given using the user ID and password registered in the switch. However, where user ID and password are defined using the user authentication protocol, RADIUS or TACACS+, access privilege is given using the user information stored in the database of each server.

<Table 7> Commands for Setting User Authentication

Command	Description	Mode
authentication login authen-type chap	When user authentication is carried out by the tacacs server, password encoded in chap mode is transferred.	Config
no authentication login authen-type	Password is not encoded when user authentication is carried out by the tacacs server.	Config
authentication login enable (local | radius | tacacs)	Selects authentication modes (local, radius, and tacacs) to be applied. Several authentication modes can be	Config

	selected.	
no authentication login enable (radius | tacacs)	Disables the selected authentication mode. Local mode is normally enabled.	Config
authentication login primary (local | radius | tacacs)	Sets primary authentication mode.	Config
no authentication login primary (local | radius | tacacs)	Clears primary authentication mode.	Config
authentication login template-user *userID*	Dummy user can be defined for authentication in radius or tacacs mode. Dummy user to be defined should be registered in the local database.	Config
no authentication login template-user	Clears dummy user.	Config
authorization exec tacacs	Gets privilege level from the tacacs server when authentication is carried out in tacacs mode.	Config
no authorization exec tacacs	No privilege level is obtained from the tacacs server.	Config
show authentication login	Shows authentication process.	Enable

Setting User Authentication

The E3208E ONU supports three methods of user authentication: using the user ID and password registered in the switch, using the RADIUS server or using the TACACS+ server. You can use the three methods selectively or apply all of the three methods.

When more than one method is used selectively, the authentication method with the highest priority will be applied first. In case authentication is carried out using the local database, the authentication method with the next priority will be applied for users not registered in the local database. At this time, ID and password will be requested again in the event of authentication fail. In case of authentication fail using RADIUS or TACACS+ server due to communication fail with the server, authentication will be carried out with the authentication method of the next priority. In the event of authentication fail, ID and password will be requested again.

```
Switch# configure terminal
Switch(config)# authentication login enable radius
Switch(config)# authentication login enable tacacs
Switch(config)# authentication login primary radius
Switch(config)# authentication login primary tacacs
Switch(config)# end
Switch # show authentication login
precedence      method     status
----------      ----------  ---------
first           tacacs     enable
second          radius     enable
third           local      enable
Switch#
```

Setting Authentication Mode upon Entering Privileged Mode

The E3208E supports various authentication methods when users enter privileged mode. Typically, access privilege is given using the enable password registered in the switch. However, if the user authentication protocol TACACS+ is enabled, access privilege will be given using the information registered in the database of each server.

<Table 8> Commands for Setting User Authentication

Command	Description	Mode
authentication enable enable (local | tacacs)	Selecta an authentication mode (local, tacacs) to be applied. Several authentication modes can be selected.	Config
no authentication enable enable (tacacs)	Disables the selected authentication mode. Local mode is normally enabled.	Config
authentication enable primary (local | tacacs)	Enables primary authentication mode.	Config
no authentication enable primary (local | tacacs)	Disables primary authentication mode.	Config
show authentication enable	Shows authentication process.	Enable

Setting User Authentication

The E3208E can authorize users entering privileged mode using the enable password registered in the switch or using the TACACS+ server. You can use the two methods selectively or apply both of the two methods.

When more then one method is used, the authentication method with the highest priority will be applied first. In case authentication is carried out using the local database, the authentication method with the next priority will be applied for users not registered in the local database. At this time, the enable password will be requested again in the event of authentication fail. In case of authentication fail using the TACACS+ server due to communication fail with the server, authentication will be carried out with the authentication method of the next priority. In event of authentication fail, the enable password will be requested again.

```
Switch# configure terminal
Switch(config)# authentication enable enable tacacs
Switch(config)# authentication enable primary tacacs
Switch(config)# end
Switch # show authentication enable
precedence      method     status
----------------    ----------    ---------
first               tacacs              enable
second              local      enable
Switch#
```

Setting Authentication Server

<Table 9> Commands for Setting RADIUS Server

Command	Description	Mode
radius-server host A.B.C.D	Sets radius-server.	Config
no radius-server host A.B.C.D	Deletes radius-server.	Config
radius-server host A.B.C.D key *encryption-key*	Sets radius-server. Sets an encryption key to be used for server access.	Config
radius-server host A.B.C.D auth-port <0-65536>	Sets radius-server. Sets auth-port to be used for server access.	Config
no radius-server host A.B.C.D auth-port	Deletes the auth-port used for server access (If deleted, the default auth-port will be used.).	Config
radius-server host A.B.C.D auth-port <0-65536> key *encryption-key*	Sets radius-server. Sets auth-port to be used to server access. Sets an encryption key to be used to access the server.	Config
radius-server key *encryption-key*	Sets a general key to be used for radius-server access. The general key is used when no keys	Config

	are defined in the server.	
no radius-server key	Deletes the general key.	Config
radius-server retransmit <1-5>	Sets a reattempt count for radius-server access.	Config
no radius-server retransmit	Clears the reattempt count (default 3 times)	Config
radius-server timeout <1-1000>	Sets timeout to receive response packet.	Config
no radius-server timeout	Clears timeout (default 5 sec)	Config

Setting RADIUS Server

You can set several RADIUS servers. In the event of authentication fail due to communication fail with the primary server, authentication will be carried out in the secondary server.

```
Switch# configure terminal
Switch(config)# radius-server host 192.168.0.1
Switch(config)# radus-server key test123
Switch(config)# radius-server host 192.168.0.2 key lns
Switch(config)# radius-server host 192.168.0.2 auth-port 3000
Switch(config)# end
Switch# show running-config
!
radius-server key test123
radius-server host 192.168.0.1
radius-server host 192.168.0.2 key lns
radius-server host 192.168.0.3 auth-port 3000
!
Switch#
```

<Table 10> Commands for Setting TACACS+ Server

Command	Description	Mode
tacacs-server host A.B.C.D key *encryption-key*	Sets tacacs -server. Sets an encryption key to be used for server access.	Config
no tacacs-server host A.B.C.D	Deletes tacacs –server.	Config
tacacs-server host A.B.C.D timeout <1-1000> key *encryption-key*	Sets tacacs -server. Sets timeout to receive response packet. Sets an encryption key to be used for server access	Config
tacacs-server host A.B.C.D timeout <1-1000>	Sets tacacs -server. Sets timeout to receive response packet.	Config

Setting TACACS+ Server

You can set several TACACS+ servers. In the event of authentication fail due to communication fail with the primary server, authentication will be carried out in the secondary server.

```
Switch# configure terminal
Switch(config)# tacacs-server host 192.168.0.1 key lns
Switch(config)# tacacs-server host 192.168.0.2 key test123
Switch(config)# end
Switch# show running-config
!
tacacs-server host 192.168.0.1 key lns
tacacs-server host 192.168.0.2 key test123
!
Switch#
```

Setting Hostname

Hostname is used to identify systems, and the prompt on the console/Telnet screen is composed of a combination of the hostname and the current command mode. The E3208E uses the default hostname “Switch”, which can be changed by user.

<Table 11> Commands for Setting Hostname

Command	Description	Mode
hostname *string*	Changes Hostname.	Config
no hostname	Sets hostname to the default value.	Config

You can set or change Hostname as follows.

```
Switch# configure terminal
Switch(config)# hostname ubiQuoss
Ubiquoss(config)# end
Ubiquoss#

Ubiquoss# configure terminal
Ubiquoss(config)# no hostname
Switch(config)# end
Switch#
```

SNMP (Simple Network Management Protocol)

The SNMP network manager can manage the switch that provides the Management Information Base (MIB). Each network manager provides a user interface for the convenience of management. Environment setup is required to manage the E3208E with the SNMP manager.

More than one IP address is required for the switch to access SNMP agent. For setting IP address, see the section concerning <IP>.

<Table 12> Commands for Setting SNMP Environment

Command	Description	Mode
snmp-server agent-address *agent-addr*	Sets an origination IP for the snmp packet transferred from the equipment	Config
no snmp-server agent-address *agent-addr*	Skips origination IP for the snmp packet transferred from the equipment	Config
snmp-server contact *string*	Changes system contact information	Config
no snmp-server contact *string*	Deletes system contact information	Config
snmp-server location *string*	Changes system location information	Config
no snmp-server location *string*	Deletes system location information	Config
snmp-server community *string* [ro|rw [access-class *number*]]	Sets an SNMP community ro : read only rw : read write number : Standard IP access-list <1-99>	Config
no snmp-server community *string*	Deletes SNMP community	Config
snmp-server enable traps [*notification-type*] [*notification-option*]	Sets SNMP Traps to be transferred to Trap-Host notification-type : Trap type (config, environ, perform, resource, security, snmp) notification-option : Trap option	Config
no snmp-server enable traps	Sets SNMP Traps not to be transferred to Trap-Host	Config
snmp-server trap-host *A.B.C.D* community *string*	Sets a community to be used to send SNMP Trap Host and traps	Config
no snmp-server trap-host *A.B.C.D*	Deletes SNMP Trap Host	Config
snmp-server trap-version 1	Sets to transmit SNMPv1 Trap	Config
no snmp-server trap-version	Sets to transmit SNMPv2 Trap	Config

Setting SNMP Community

Community string provides a simple authentication function between the system and the remote network manager. The E3208E ONU supports two types of community strings.

Read community strings

- Read-only access to the system
- Default read-only setting is public

Read-write community strings

- Read and write access to the system
- Default read and writing setting is private

```
Switch# configure terminal
Switch(config)# snmp-server community public ro
Switch(config)# snmp-server community private rw
Switch(config)# snmp-server community locuse ro access-class 1
Switch(config)# end
Switch# show running-config
!
snmp-server community public ro
snmp-server community private rw
snmp-server community locuse ro access-class 1
!
Switch#
```

Notice For setting access-class, see < ACL>

Setting SNMP Trap

More than one network management terminal can be authorized as trap receiver. The E3208E ONU transfers SNMP traps to all trap receivers.

```
Switch# configure terminal
Switch(config)# snmp-server enable traps
Switch(config)# snmp-server trap-host 192.168.0.3 community private
Switch(config)# end
Switch# show running-config
!
snmp-server enable traps config slotAdd slotDel GBICAdd GBICDel fanStatus
snmp-server enable traps environ tempUpRise tempUpFall tempLowRise tempLowFall
snmp-server enable traps perform rmonRise rmonFall bpsRise bpsFall ppsRise ppsFall
snmp-server enable traps resource cpuUsageRise cpuUsageFall
snmp-server enable traps security remoteConnect
snmp-server enable traps snmp coldStart warmStart linkDown linkUp authFail
snmp-server trap-host 192.168.0.3 community private
!
Switch#
```

Notice SNMP Trap supported from E3208E includes every switch's SNMP Trap.
When you set every SNMP Trap with 'snmp-server enable traps', SNMP Trap not supported from current switch can be included in the running-config.

Starting point IP Setting of SNMP Packet

When the switch sends SNMP Packet to more than one Network Manager, you can set the starting point IP of the sending SNMP packet with specific Local IP address.

```
Switch# configure terminal
Switch(config)# snmp-server agent-address 210.48.148.125
Switch(config)# end
Switch# show running-config
!
snmp-server agent-address 210.48.148.125
!
Switch#
```

Setting System Administrator

It is possible to register an administrator responsible for system management.

```
Switch# configure terminal
Switch(config)# snmp-server contact “gil-dong hong. hong@ubiquoss.com”
Switch(config)# end
Switch# show running-config
!
snmp-server contact “gil-dong hong. hong@ubiquoss.com”
!
Switch#
```

Setting System Configuration Location

```
Switch# configure terminal
Switch(config)# snmp-server location “Dogok-Dong, GangNam-gu, Seoul.”
Switch(config)# end
Switch# show running-config
!
snmp-server location “Dogok-Dong, GangNam-gu, Seoul.”
!
Switch#
```

ACL (Access Control List)

The network manager can control traffic transferred over the inter-network using the ACL (Access Control List). The network manager can acquire basic statistics data on the status of packet transmission and establish a security policy from the data. It is also possible to protect the system from unauthorized access. An access list can be used to permit or deny packets transferred through the router. It can also be used to access router over Telnet(vty) or SNMP.

The E3208E supports standard IP access list, to which numbers 1 – 99 can be assigned.

<Table 13> Commands for Setting Access List

Command	Description	Mode
access-list <**1-99**> {**deny**|**permit**} *address*	Sets standard IP access list *address* ::= {any | A.B.C.D/M}	Config
no access-list <1-199>	Deletes access list	Config

Rules to Create an Access List

- Declare a narrower range preferentially.
- Declare a condition which will be fulfilled more frequently.
- 'Deny any' is declared in default unless 'permit any' is not specified at the end of access list.
- It is not permitted to delete or modify a certain condition of several lines defined for an access list but new filters are added to the end of the list.

Setting Standard IP Access List

Permit Any

```
Switch# configure terminal
Switch(config)# access-list 1 permit any
Switch(config)# end
Switch# show access-list
Access-List 1
permit    any
```

Deny Any

```
Switch# configure terminal
Switch(config)# access-list 1 deny any
Switch(config)# end
Switch# show access-list
Access-List 1
          deny       any
```

Permit Access from a Specific Host

```
Switch# configure terminal
Switch(config)# access-list 1 permit 192.168.0.3/32
Switch(config)# end
Switch# show access-list
Access-List 1 permit    192.168.0.3/32
```

Permit Access from a Specific Network

```
Switch# configure terminal
Switch(config)# access-list 1 permit 192.168.0.0/24
Switch(config)# end
Switch# show access-list
Access-List 1
        permit   192.168.0.0/24
```

Deny Access from a Specific Network

```
Switch# configure terminal
Switch(config)# access-list 1 deny 192.168.0.0/24
Switch(config)# access-list 1 permit any
Switch(config)# end
Switch#   show access-list
Access-List 1
        deny      192.168.0.0/24
        permit   any
```

Setting Access List for SNMP Connection

Access list is applied by community to permit or deny access to switch over snmp.

The following shows an example of creating an access list to restrict snmp access by permitting access from the host 10.1.22.247 only.

```
Switch# configure terminal
Switch(config)# access-list 1 permit 10.1.22.247/32
Switch(config)# snmp-server community lns ro access-class 1
Switch# show running-config
!
snmp-server community lns ro access-class 1
!
access-list 1 permit 10.1.22.247/32
!
Switch#
```

Setting Access List for Telnet Connection

Access list is applied by user to permit or deny external access to the switch.

The following shows an example of creating an access list to restrict telnet access by permitting access from the network 192.168.0.0/24 only.

```
Switch# configure terminal
Switch(config)# access-list 1 permit 192.168.0.0/24
Switch(config)# username admin access-class 1
Switch# show running-config
!
username admin privilege 15 password 0 admin
username admin access-class 1
!
access-list 1 permit 192.168.0.0/24
!
Switch#
```

NTP Setup

Overview

NTP (Network Time Protocol) is used for time synchronization between systems over the network. NTP works over UDP (User Datagram Protocol) and applies Coordinated Universal Time (UTC) equal to the Greenwich Mean Time for time information of all NTP messages.

Setting NTP Client Mode

In global setup mode, the following command is used to set NTP client mode.

<Table 14> Setting NTP Client Mode

Command	Description
ntp server *address*	Sets NTP server (up to 5 servers)

Setting NTP Server Mode

In global setup mode, the following command is used to set NTP server mode.

<Table 15> Setting NTP Server Mode

Command	Description
ntp master *stratum*	Sets NTP master.

Setting NTP Time Zone

Time zone can be defined for an NTP server or client to represent an exact time currently used in the given zone.

<Table 16> Setting NTP Time Zone

Command	Description
ntp timezone plus *HH:MM*	Adds the given time period to the Coordinated Universal Time (UTC) to represent the current time.
ntp timezone minus *HH:MM*	Subtracts the given time period from the Coordinated Universal Time (UTC) to represent the current time.

Setting NTP summer time

For some geographic region use summer time (daylight savings time) the following command is to be used for this purpose.

<Table 17> Setting NTP summer time

Command	Description
ntp summer-time *week day month hh:mm week day month hh:mm*	Apply the start and finish date and time of Summer time period.
no ntp summer-time	Dismiss the set time for Summer time.

Other NTP Commands

<Table 18> Other NTP Commands

Command	Description
ntp poll-interval *number*	An interval to transmit NTP request message to the specified NTP server. A multiple of two ranged <4-17>.
show ntp	Shows NTP.

Example of NTP Settings

To get ntp time from ntp server 203.248.240.103, do the following configuration.

```
Switch#
Switch (config)# ntp server 203.248.240.103
Switch (config)# exit
Switch # show ntp
-------------------------------------------
Current time      : Thu Jan 12 20:40:25 2008
-------------------------------------------
NTP master                  : disable
NTP stratum                 : unspecified
Poll interval               : 6 (power of 2)
NTP timezone                : GMT
NTP summertime              : none
NTP summertime start    : none
NTP summertime end      : none
-------------------------------------------
The list of NTP Server is below.
-------------------------------------------
[1] 203.248.240.103
-------------------------------------------
Switch #
```

To set timezone, do the following configurtion.

```
Switch#
Switch# configure terminal
Switch(config)# ntp timezone plus 9:0
Switch(config)# end
Switch# show clock
Mon Jan 14 10:58:36 2008    GMT+9:0
Switch# show ntp
-----------------------------------------
Current time       : Mon Jan 14 10:58:39 2008
-----------------------------------------
NTP master                    : disable
NTP stratum                   : unspecified
Poll interval                 : 6 (power of 2)
NTP timezone                  : +9:0
NTP summertime                : none
NTP summertime start    : none
NTP summertime end        : none
-----------------------------------------
The list of NTP Server is below.
-----------------------------------------
Switch#
```

Chapter 2. Interface Environment Setup

This chapter describes interface environment configuration.

- Overview
- Port mirroring
- Setting Layer2 Interface Environment.
- Port group
- MAC Filtering
- Traffic-control

Overview

The E3208E supports the interfaces listed below.

<Table 19> Interfaces Supported by E3208E

Type	Description
Physical interfaces	Fast Ethernet 10/100Base-TX (Auto Negotiation) Giga Ethernet EPON
port-group interfaces	Port-group
VLAN Interfaces	VLAN

You can set up an interface environment as follows.

1. Enter the Config mode from the Privileged mode using the command “**configure terminal**”.
2. Enter the interface mode using the command “interface”.
3. Apply the configuration command depending on the given interface.

Common Command

The following shows a common command applied to interface environment setup.

<Table 20> Common Command

Command	Description
interface *ifname*	Enter the interface mode. *ifname*: Specifies an interface for environment setup.

Interface Name

The E3208E applies interface names for all environment setup. Interface names are identified with interface type and id as shown below.

<Table 21> Interface Name

Classification	Interface Type	Interface Name	Example
Physical interface	Fast ethernet	“fa” + port_number	fa1
Physical interface	Giga ethernet	“gi” + port_number	gi1
Port-group interface	Port group	“po” + port-group id	po1
VLAN interface	VLAN	“vlan” + vlan id	vlan10

Interface ID

An interface name consists of interface type and id. Interface id is dependent on E3208E ONU models. The following table lists interface id and supported range for each model.

<Table 22> Interface ID and Supported Range

Model	Interface Type	Interface ID	ID Range	Name(e.g.)
E32XX	Fast ethernet	port id	port id: 1-8	fa1, fa8
	Giga ethernet	port id	port id: 1	gi1
	Port group	port id	1 – 8	po1, po7
	VLAN	vlan id	1 – 4094	vlan1, vlan4094

Interface Mode Prompt

The following prompt appears on the screen when you enter the interface mode using the **interface** command. In the interface mode, you can set and modify an environment for interface.

```
Switch(config)# interface fa1
Switch(config-if-fa1)#
```

Interface-range Mode Prompt

You can enter the interface range mode using the **Interface range** command. This mode is applicable to port interface only and is not available for VLAN or other interfaces. In the interface range mode, the specified interface is repeated by looping.

```
Switch(config)# interface range fastethernet 1-8
Switch(config-ifrange)# speed 100
```

```
Switch(config-ifrange)# exit
```

The above configuration brings the same result when the following configuration is repeated.

```
Switch(config)# interface fa1
Switch(config-if-fa1)# speed 100
Switch(config-if-fa1)# exit
Switch(config)# interface fa2
Switch(config-if-fa2)# speed 100
Switch(config-if-fa2)# exit
!
Switch(config)# interface fa8
Switch(config-if-fa8)# speed 100
Switch(config-if-fa8)# exit
```

Range port mode prompt

The range port command allows using range port mode. This is available only for port interface, and not available for vlan or other interface. Use the interface command repeatedly in a different way from the Interface range mode.

```
Switch(config)# range-port
Switch(config-range-port)#
```

In Range-port mode, all the commands available in port interface can be used. In order to specify the port, a command system with [COMMAND] + [PORTRANGE] combination is used.

```
Switch(config)# range port
Switch(config-range-port)# speed 100 fa1
Switch(config-range-port)#

This command has the function same as below.

Switch(config)# interface fa1
Switch(config-if-fa1)# speed 100
Switch(config-if-fa1)#
```

Not only a single port, but also port range in combination can be used for [PORTRANGE]. Multiple ports can be specified in the combition of Port prefix plus (starting range) – (end range). For example, **fa1-4 refers to the ports from** fa1 to fa4. A comma is used to bind multiple ports placed not in sequence. For example, the format of **fa1 , fa3-4** is also possible.

```
Switch(config)# range
port
Switch(config rangeport)# speed 100 fa1 , fa3-4
Switch(config range port)#
```

This command is to set speed 100 to fa1, fa3 and fa4 port.

A port can be configured in three ways, interface, interface range, and range-port. ***show running-config*** command shows the result in two ways, range-port and interface.

1. Multiple ports are shown as port range.
2. A specific port are shown as interface.

```
Switch(config)# interface fa1
Switch(config-if-fa1)# speed 100
Switch(config-if-fa1)# exit
Switch(config)# interface fa2
Switch(config-if-fa2)# speed 100
Switch(config-if-fa2)# exit
Switch(config)# interface fa3
Switch(config-if-fa3)# speed 10
Switch(config-if-fa3)# exit
Switch(config)# exit
Switch#
Switch# show running-config
!
range port
   speed 100 fa1-2
!
interface fa3
  speed 10
!
Switch#
```

The result of the command ***speed 100*** set to both fa1 and fa2 are shown collectively using range port function, and the result of the command speed 10 set to fa3 only is shown as interface.

The range port function allows reducing the configuration for a port interface when checked by ***show run*** command, and helps to identify the current configuration easily compared to the normal L2 switch configuration in which repetitive configuration is usually required.

<Table 23> Range port mode prompt

When Range port is not used	When Range port is used

interface fa1
  shutdown
  switchport access vlan 100
!
interface fa2
  shutdown
  switchport access vlan 100
  description // fa2 is reserved //
!
interface fa3
  shutdown
  switchport access vlan 100
!
interface fa4
  shutdown
	!
	range port
	  shutdown fa1-4,fa8,gi1
	  switchport access vlan 100 fa1-4
	!
	interface fa2
	  description // fa2 is reserved //
	!

switchport access vlan 100 ! interface fa8 shutdown ! interface gi1 shutdown !	

Note The existing interface nodes are used also for PORT-GROUP and VLAN.

Viewing Interface Information and Status

Using the following commands, you can view the environment setup information, status information and statistics data for the interface.

<Table 24> Commands related to Interface Information and Status

Command	Description	Mode
show interfaces [*ifname*]	Shows the status and configuration information on the interface	Privileged
show port status	Shows the status information on all physical interfaces	Privileged
show switchport	Shows the switch port information on physical/port-group interface	Privileged

Show Interfaces

This command is used to view environment configuration, link status and statistics on interfaces. It shows the information on all interfaces defined.

```
Switch# show interfaces
fa1 is up
  type 100Base-TX
  auto-negotiation
  speed set auto, current 100M
  duplex set full, current full

  Last clearing of counters 1w0d
  1 minutes input    rate 13,119 bytes/sec, 198 packets/sec
  1 minutes output rate 1,586 bytes/sec, 24 packets/sec
     1,396,695 packets input, 148,951,819 bytes
     Received 796,623 broadcasts, 96,388 multicasts
     0 CRC, 0 oversize, 0 dropped
     4,747 packets output, 455,150 bytes
     Sent 1 broadcasts, 0 multicasts
```

Show Port Status

This command shows link status, shutdown status, Auto Negotiation mode, speed/duplex mode, flow control, Mdix settings and interface type for all physical ports.

```
Switch# show port status
shutdown : (A)admin, (S)sld
-------------------------------------------------------------------------------
 ifname type    shutdown block link    nego    set-speed cur-speed flow-ctl link-cnt eee
-------------------------------------------------------------------------------
 fa1    FE-TX      .        .    down auto    auto/auto      .         .        0    .
 fa2    FE-TX      .        .    down auto    auto/auto      .         .        0    .
 fa3    FE-TX      .        .    down auto    auto/auto      .         .        0    .
```

```
fa4    FE-TX     .     .    down auto    auto/auto      .     .     0    .
fa5    FE-TX     .     .    down auto    auto/auto      .     .     0    .
fa6    FE-TX     .     .    down auto    auto/auto      .     .     0    .
fa7    FE-TX     .     .    down auto    auto/auto      .     .     0    .
fa8    FE-TX     .     .      up  auto    auto/auto 100M/full    .     0    .
gi1    EPON      .     .    down manual 1G   /full      .     .     0    .
--------------------------------------------------------------------------
```

Notice The CLI capture screens for the examples given below are based on E3208E. See the interface ID <Table -13> for setting other models.

Show Switchport

Switchport refers to ports or port group working in the Layer 2 switching mode. The command **Show switchport** shows the switchport information on physical port and port-group. Switchport information includes mode, native and tagged VLAN list.

```
Switch# show switchport
IFNAME     SWMODE    N-VLAN TAGGED-VLAN-LIST
--------------------------------------------------------------------------
  fa1        access       1
  fa2        access       1
  fa3        access       1
  fa4        access       1
  fa5        access       1
  fa6        access       1
  fa7        access       1
  fa8        access    4094
  gi1        access       1
--------------------------------------------------------------------------
total 9 interfaces listed
```

Setting Physical Port Environment

The following the commands is used for setting up an environment for physical ports.

<Table 25> Commands for Setting up Physical Port Environment

Command	Description	Mode
Shutdown **no shutdown**	Disables/enables physical port	interface
Block **no block**	Blocks/unblocks physical port	interface
auto-negotiation **no auto-negotiation**	Enables/Disables speed auto-negotiation.	Interface
speed (10|100|1000) **speed auto**	Sets speed	interface
duplex (full-duplex|half-duplex) **duplex auto**	Sets duplex mode	interface
flow-control (on|off)	Enables/disables flow-control	interface

Shutdown

This command is used to disable a physical port.

Use the command '**show interface'** to check the shutdown status of physical port.

```
Switch# configure terminal
Switch(config)#
Switch(config)# interface fa1
Switch(config-if-fa1)# shutdown          <- disable port
Switch(config-if-fa1)# no shutdown       <- enable port
```

Block

This command blocks a specified port. At this time, the link with the remote side is alive but no traffic flows.

```
Switch# configure terminal
Switch(config)#
Switch(config)# interface fa1
Switch(config-if-fa1)# block             <- block port
Switch(config-if-fa1)# no block          <- unblock port
```

Speed and Duplex

The speeds supported by each interface of E3208E are listed below.

<Table 26> Speed and Duplex

type	auto-negotiation	speed	duplex
100Base-TX	on	10/100/auto	full/half/auto
	off	10/100	full/half
EPON-TEKNOVUS	off	1000	full

Note the following when setting speed and duplex.

If both ends support auto-negotiation, it is strongly recommended to apply auto-negotiation, wherever applicable.

If just one end of an interface supports auto-negotiation, it is not permitted for the both ends to apply auto-negotiation to “duplex” and “speed”.

Port Mirroring

Port mirroring mirrors incoming/outgoing traffic of a specific port (source port) to the target port specified by the operator. This function is used to monitor all packets of a desired port.

E3208E can mirror rx and tx traffic from several source ports to one target port.

<Table 27> Port Mirroring

Command	Description	Mode
mirroring target *ifname*	Sets a target port to mirror input/output packets	config
mirroring rx-traffic	Sets mirroring the input packets of a specified port	interface
mirroring tx-traffic	Sets mirroring the output packets of a specified port	interface

Setting Layer 2 Interface Environment

A Layer 2 interface works in the Layer 2 switching mode (IEEE 802.3 Bridged VLAN), and physical ports and port-group interfaces of the E3208E work in this mode.

This section describes the Layer 2 interface and shows the command and an example to set physical port and port-group to Layer 2 interface.

VLAN Trunking

Trunk is a point-to-point link between an Ethernet switch and other networking equipment (router, switch). It is permitted to transmit multiple VLAN traffics to a single link and to expand VLAN to the whole network through VLAN trunking.

The E3208E supports 802.1Q trunking encapsulation for all Ethernet interfaces. You can set trunk for a single Ethernet interface or port-trunk interface.

Layer 2 Interface Mode

The Layer 2 interface modes supported by the E3208E include trunk mode and access mode.

<Table 28> Layer 2 Interface Modes Supported by E3208E

Mode	Description
switchport mode access	non trunking mode Only native VLAN is permitted.
switchport mode trunk	trunking mode One native VLAN and several tagged VLANs can be defined.

Layer 2 Interface Default Settings

When a physical port or port-group is set to layer 2 interface, the E3208E provides the default settings as follows.

<Table 29> Layer 2 Interface Default Settings

Item	Setting
interface mode	switchport mode access
native vlan	VLAN 1

Enable/Disable Layer 2 Interface

The commands to enable/disable Layer 2 interface are given in the table below.

<Table 30> Layer 2 interface on/off command

Command	Description	Mode
switchport	Enable Layer2 interface	Interface
no switchport	Disable Layer2 interface	Interface

When an interface is initially set to Layer 2, it carries the default settings of Layer 2 interface, which will be cleared when the Layer 2 interface is disabled. Layer 2 interface needs to be cleared for port-grouping of physical ports.

Setting Trunk Port

The commands used to set physical port or port-group interface to Layer 2 trunk port are listed below.

<Table 31> Commands for Setting Trunk Ports

Command	Description	Mode
switchport mode trunk	Sets trunk mode	interface
switchport trunk native vlan *<1-4094>*	Sets trunk port native VLAN	interface
no switchport trunk native vlan	Sets trunk port native VLAN to default settings	interface
switchport trunk add *<2-4094>*	Adds trunk port tagged VLAN	interface
switchport trunk remove *<2-4094>* **switchport trunk remove all**	Removes trunk port tagged VLAN	interface

The following shows an example of setting physical port to Layer 2 trunk port.

```
Switch# configure terminal
Switch(config)# interface fa1
Switch(config-if-fa1)# switchport                    ! Set layer2 interface
Switch(config-if-fa1)# switchport mode trunk         ! Set trunk port
Switch(config-if-fa1)# switchport trunk native 2     ! Set native vlan
Switch(config-if-fa1)# switchport trunk add 3        ! Add tagged vlan
Switch(config-if-fa1)# switchport trunk add 4
Switch(config-if-fa1)# end
```

The following shows an example of setting a port-group interface to Layer 2 trunk port.

```
Switch# configure terminal
Switch(config)# interface po2
Switch(config-if-po2)# switchport                    ! Set layer2 interface
Switch(config-if-po2)# switchport mode trunk         ! Set trunk port
Switch(config-if-po2)# switchport trunk native 2     ! Set native VLAN
Switch(config-if-po2)# switchport trunk add 3        ! Add tagged vlan
Switch(config-if-po2)# switchport trunk add 4
Switch(config-if-po2)# end
```

Setting Access Port

The commands to set physical port or port-group interface to Layer 2 access port are given below.

<Table 32> Commands for Setting Access Ports

Command	Description	Mode
switchport mode access	Sets access mode	interface
switchport access vlan *<1-4094>*	Sets native VLAN	interface
no switchport access vlan	Sets native VLAN to default settings	interface

	(VLAN 1)	

The following shows an example of setting a physical port to Layer 2 access port.

```
Switch# configure terminal
Switch(config)# interface fa1
Switch(config-if-fa1)# switchport                    ! Set layer2 interface
Switch(config-if-fa1)# switchport mode access        ! Set access port
Switch(config-if-fa1)# switchport access vlan 5      ! Set native vlan
```

The following shows an example of setting port-group interface to Layer 2 access port.

```
Switch# configure terminal
Switch(config)# interface po2
Switch(config-if-po2)# switchport                    ! layer2 interface set
Switch(config-if-po2)# switchport mode access        ! access port set
Switch(config-if-po2)# switchport access vlan 5      ! native vlan set
```

Port Group

Overview

Port group is used to expand a bandwidth and to ensure duplication of links by grouping several physical ports into one logical group. In the E3208E, a port group interface can be used as a Layer 2 interface.

The number of port groups applicable to the E3208E is given below.

Model	Port Groups	Maximum ports per group
E3208E	8	8

Port Group Configuration

The commands to configure a port group are listed below.

<Table 33> Commands for Configuring Port Group

Command	Description	Mode
port-group create *ifname* **protocol none**	Creates static port group.	config
no port-group *ifname*	Deletes port-group	config
lb-mode layer2 (src|dst|mix)	Refers to mac for load-balance (source, destination, mixed).	interface
lb-mode layer3 (src|dst|mix)	Refers to IP for load-balance (source, destination, mixed)	interface
port-group *ifname* **no port-group** *ifname*	Adds port group member Deletes port group	interface *
show port-group	Shows port group settings	Privileged

```
Switch(config)# port-group create po1 protocol none   ! port-group create
Switch(config)# interface range fastethernet 7-8 ! interface range set
Switch(config-ifrange)# no switchport ! no switchport set
Switch(config-ifrange)# port-group po1
Switch(config-ifrange)# exit
```

MAC Filtering

Overview

MAC filtering is used to filter traffic to a specific MAC address for L2 Switching. You can set MAC filtering for each VLAN.

Setting MAC Filtering

The commands used for setting MAC filtering are given below.

<Table 34> Commands for Setting MAC-filter

Command	Description	Mode
mac-filter *vlan-id mac-addr*	Adds MAC filter	config
no mac-filter *vlan-id mac-addr*	Deletes MAC filter	config

Traffic-control

Overview

Traffic-control is a means of port flood guard to prevent excessive traffic being introduced from a specific port. The traffic will be blocked or an alarm will be issued when the traffic introduced from a specific port exceeds the specified limit, and normal status will be restored when the traffic is lowered below the specified limit.

Setting Traffic-control

You can set traffic-control by pps and by kbps based on inbound or outbound traffic. In case of traffic-control by pps, you can set traffic control by traffic types of unicast, multicast and broadcast or by total traffic volume. When traffic-control is defined with several items, traffic will be blocked even one item is enabled.

In block mode, the affected port will be blocked to control traffic and an alarm will be issued. In alarm-only mode, only an alarm will be issued without blocking the affected port.

Report-interval sets an interval in minutes to activate or deactivate alarm based on traffic volume of an affected port.

Observing-period sets a period to collect statistics data. For instance, if observing-period is set to 10, statistics data on traffic for the latest 10 minutes will be collected.

Alarm-mode supports three options of once / repeatable / disable for high threshold and two options of once / disable for low threshold. You can select a combination of the options for high and low thresholds. Set the alarm mode to ‘high once low once’ if you want to issue an alarm just once when traffic limit-over is activated and cleared respectively. Set the alarm mode to ‘high repeatable low disable’ if you want to repeatedly issue an alarm with the report-interval as long as the traffic exceeds the specified threshold and to issue no alarm when traffic limit-over is cleared. Set the alarm mode to ‘high disable low disable’ if you want to block traffic without activating an alarm when low limit-over is cleared.

<Table 35> Commands for Setting Traffic-control

Command	Description	Mode
traffic-control pps <inbound|outbound> <1-1500000> <1-1500000> block-mode	Sets traffic of a specific port in pps based on total inbound or outbound traffic volume and set traffic-control to block-mode.	interface
traffic-control pps <inbound|outbound> <1-1500000> <1-1500000> alarm-only	Sets traffic of a specific port in pps based on total inbound or outbound traffic volume and set traffic-control to alarm-only mode.	interface
traffic-control pps <unicast|multicast|broadcast> <inbound|outbound> <1-1500000> <1-1500000> block-mode	Sets traffic of a specific port in pps based on inbound or outbound traffic volume by traffic types and set traffic-control to block-mode.	interface
traffic-control pps <unicast|multicast|broadcast> <inbound|outbound> <1-1500000> <1-1500000> alarm-only	Sets traffic of a specific port in pps based on inbound or outbound traffic volume by traffic types and set traffic-control to alarm-only mode	interface

no traffic-control pps <inbound|outbound>	Clears the settings.	interface
no traffic-control pps <unicast|multicast|broadcast> <inbound|outbound>	Clears the settings.	Interface
traffic-control kbps <inbound|outbound> <1-1000000> <1-1000000> block-mode	Sets traffic of a specific port in kbps based on total inbound or outbound traffic volume and set traffic-control to block-mode.	interface
traffic-control kbps <inbound|outbound> <1-1000000> <1-1000000> alarm-only	Sets traffic of a specific port in kbps based on total inbound or outbound traffic volume and set traffic-control to alarm-only mode.	interface
no traffic-control kbps <inbound|outbound>	Clears the settings.	Interface
traffic-control report-interval <1-1440>	Sets an interval to activate alarm.	Config
traffic-control observing-period <1-1440>	Sets a period to collect statistics data	Config
Traffic-control alarm-mode high <once|repeatable|disable> low <once|disable>	Selects once/repeatable/disable to activate alarm at high threshold and low threshold	Config
show traffic-control	Shows the current settings and status.	Privileged

```
Switch(config)# traffic-control report-interval 2
Switch(config)# traffic-control oberserving-period 2
Switch(config)# interface fa1
Switch(config-if-fa1)# traffic-control pps unicast inbound 100000 50000 alarm-only
Switch(config-if-fa1)# traffic-control pps broadcast inbound 100000 50000 alarm-only
Switch(config-if-fa1)# end
Switch# show traffic-control
Traffic Contorl Status

 Report Interval    : 1 minutes
 Observing Period : 1 minutes
 Alarm Mode           : High - Once , Low - Once

 Interface : fa1
  Status     : Normal
                              High          Low      Average   1 Minute     Alarm
                         Threshold Threshold         Rate         Rate     Count Last Alarm Time
-------------------------------------------------------------------------------
 PPS
 All    In :                    -         -            -            -         -
 Unicast    In :         100000        50000          0            0         0
 Broadcast    In :       100000        50000          0            0         0
```

```
Multicast    In :          -          -          -          -          -
All Out :                  -          -          -          -          -
Unicast Out :              -          -          -          -          -
Broadcast Out :            -          -          -          -          -
Multicast Out :            -          -          -          -          -

KBPS
          All    In :      -          -          -          -          -
          All Out :        -          -          -          -          -
--------------------------------------------------------------------------------
total 1 entries found
```

Chapter 3. VLAN

Virtual LAN (VLAN) logically groups network users and resources connected to the switch ports. VLAN facilitates network management consuming much time and improves efficiency of network through broadcast traffic control.

This chapter covers the following subjects:

- Overview of VLAN
- VLAN types
- Configuring a VLAN
- Displaying VLAN settings

Overview of VLAN

A group of devices which seem to communicate over the same LAN is referred to as “Virtual LAN (VLAN)”. VLAN is a broadcast domain which is logically isolated by certain functions, structures or applications to enhance performance of network by preventing traffic flow into other VLANs and transmitting traffic only to the equipment over the same VLAN. In other words, VLAN segments are not physically identified by hardware connections but flexibly defined by logical groups created by the manager.

Definition of VLAN

VLAN is a switching network logically identified by structural criteria such as functions, project groups or applications rather than by physical connections or topological locations. For instance, all workstations and servers used by a specific task group can be connected over the same VLAN regardless of their physical networking. It is possible to reconfigure network through software setup without movement or reallocation of the equipment and cables.

VLAN can be regarded as a broadcast domain defined by a switch group. VLAN is configured with several terminal systems (network equipment such as host, bridge or router) connected to one bridge domain. VLAN is used to provide a segmentation service provided by a router in a conventional LAN configuration. VLAN provides expandability, security and network management. The router in a VLAN configuration provides broadcast filtering, security, address contraction and traffic flow control. The switches in a defined group do not transfer any frames as well as broadcast frames between two VLANs.

Advantages of VLAN

VLAN provides advantages as follows:

- **Traffic Control**

A conventional network might incur congestion due to the broadcast traffic transferred to all network devices irrespective of data to be received by each device. All devices in a VLAN are the components included in the same broadcast domain and receive all broadcast packets, while the broadcast traffic is not transferred to those ports of switches linked to other VLANs. Therefore, using a VLAN, it is possible to improve efficiency of network by preventing broadcast traffic flow into adjacent networks.

- **Enhanced Network Security**

In a conventional network, anyone who accesses a network can access its network resources. In addition, users who access the network analyzer through hub can view all network flow. However, devices included in a VLAN can communicate with the members of the same VLAN but are not permitted to access all network resources by just connecting their computers to switch ports. A device included in VLAN A can communicate with a device included in VLAN B only through a routing system.

- **Flexible Network Management**

Conventional network managers have consumed much time for moving and modifying their devices. Where those devices are moved to other sub-network, they need to manually change the IP address of each terminal. System operators can clear these problems by configuring a logical network over VLAN.

VLAN Types

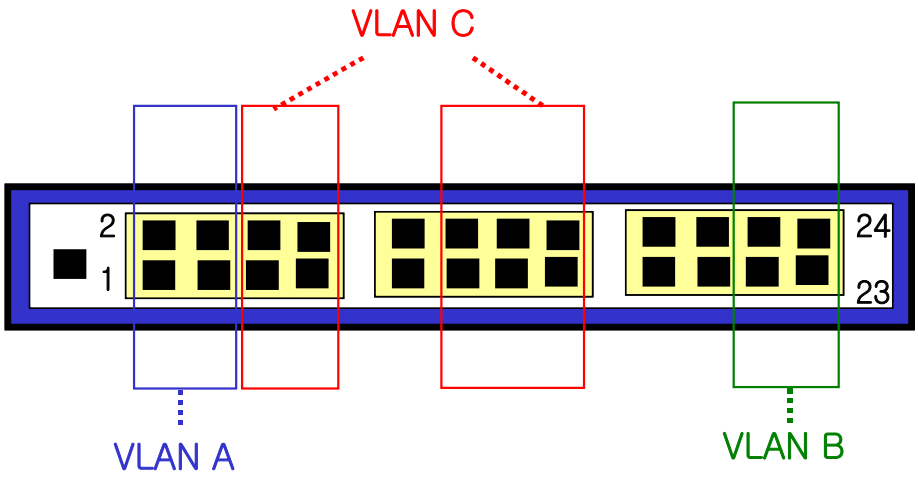
The E3208E ONU can support up to 256 VLANs. VLAN is created according to the following conditions:

- Physical ports
- 802.1Q tag
- Combination of the above conditions

Port-Based VLANs

In a port-based VLAN, the VLAN name is assigned to more than one switch port group. A switch port assigned to port-based VLAN is called access port. One access port is exclusively included in one port-based VLAN. Basically, every port is assigned as an access port of VLAN 1(default VLAN).

For example, in E3208E ONU shown *in* **오류! 참조 원본을 찾을 수 없습니다.**>, ports 1, 2, 3 and 4 are access ports of VLAN A and ports 21, 22, 23 and 24 are assigned as access ports of VLAN B. Ports 5, 6, 7, 8, 11, 12, 13, 14, 15 and 16 are defined as access ports of VLAN C.



<Figure 2> Example of Port-Based VLAN Configuration of E3208E ONU

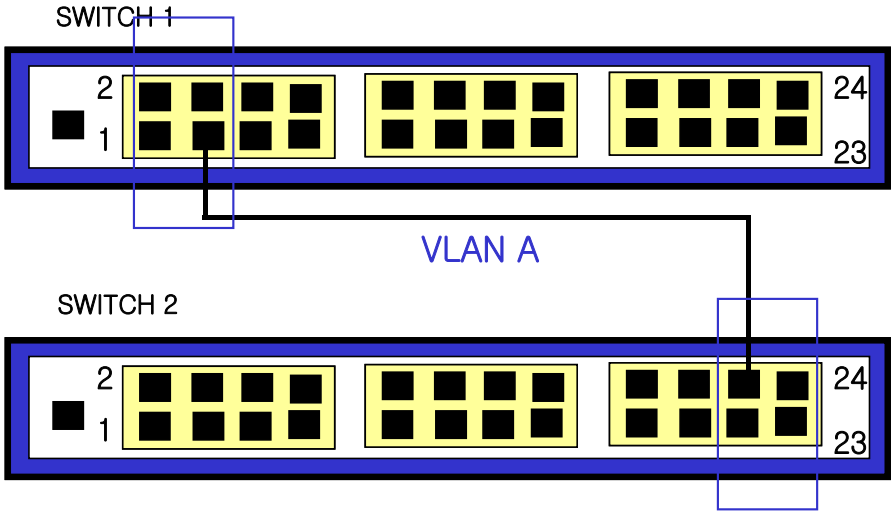
For communication between members of different VLANs, frames should be routed through the switch although they are physically a part of the same I/O module. This means that each VLAN should be defined as a router interface with a unique IP address.

Grouping Switches into Port-Based VLAN

You can group two switches into a port-based VLAN as follows:

- Assign an access port for VLAN in each switch.
- Connect the two switches with a cable using one of the access ports assigned to VLAN. You can connect several VLANs by connecting each VLAN with a cable.

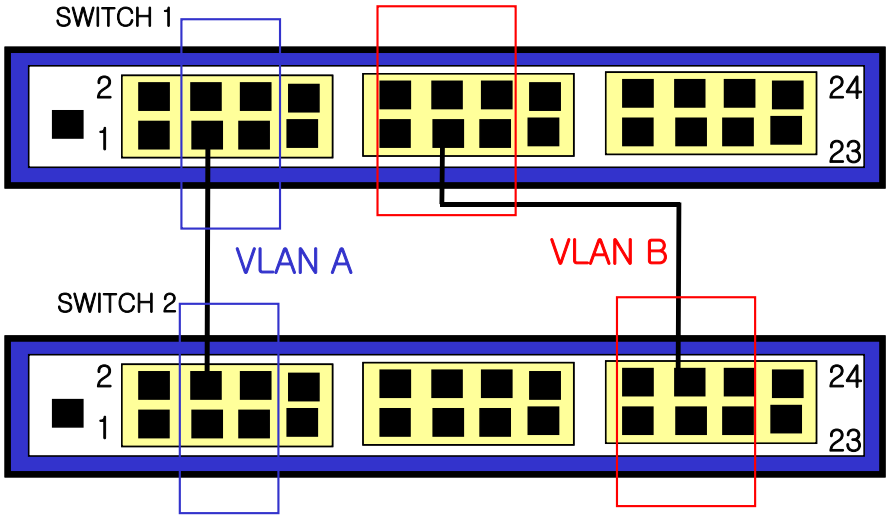
<Figure 3> shows an example of grouping two E3208E ONUes into one VLAN. Four ports of E3208E-1 are assigned to VLAN A, and four ports of E3208E 2 are assigned as access ports of VLAN A. As seen in <Figure 3>, the two switches are connected to form one broadcast domain.



<Figure 3> Single Port-Based VLAN Built with Two Switches

To create several port-based VLANs using two switches, ports of Switch 1 should be connected to those of Switch 2 with cable for each VLAN and at least one port of each switch should be defined as an access port for the corresponding VLAN.

오류! 참조 원본을 찾을 수 없습니다.4> shows two VLANs configured using two E3208E ONUes. Ports 3, 4, 5 and 6 of Switch 1 are assigned as access ports of VLAN A, and ports 9, 10, 11, 12, 13 and 14 are defined as access ports of VLAN B.



<Figure 4> Two Port-Based VLANs Configured with Two Switches

In VLAN A, E3208E- 1 is connected to E3208E- 2 through port 3 of E3208E- 1 and port 4 of E3208E- 2. In VLAN B, E3208E- 1 is connected to E3208E- 2 through port 11 of E3208E- 1 and port 20 of E3208E- 2.

In this way, you can create multiple VLANs by connecting several switches in a daisy chain. Each switch has dedicated access ports for VLAN connection, which are connected to the access ports of VLAN in the succeeding switch.

Tagged VLANs

Tagging refers to inserting a marker called tag into Ethernet frame. Tag contains VLANid to identify VLAN.

	Notice	Using 802.1Q tag frame, you can create a frame a little larger than the maximum frame size 1,518 bytes, of IEEE 802.3/Ethernet frame. This might affect frame error counter of other equipment that does not support 802.1Q and might result in network connection problems if there are bridges or routers over the path that do not support 802.1Q.

Uses of Tagged VLANs

Tagging is widely used to create a VLAN combining several switches. Using tags, several VLANs can send and receive frames through one or more trunks.

In a port-based VLAN as illustrated in **오류! 참조 원본을 찾을 수 없습니다.**4>, one port is assigned to each VLAN to connect two switches. However, it is possible to create several tagged VLANs connecting two switches using just one trunk.

Another advantage of tag

Tagged VLAN is that a port can be a member of several VLANs. Tagged VLAN is especially useful for using equipment like a server shared by several VLANs. In this case, the equipment should be equipped with a network interface card (NIC) supporting IEEE 802.1Q tag.

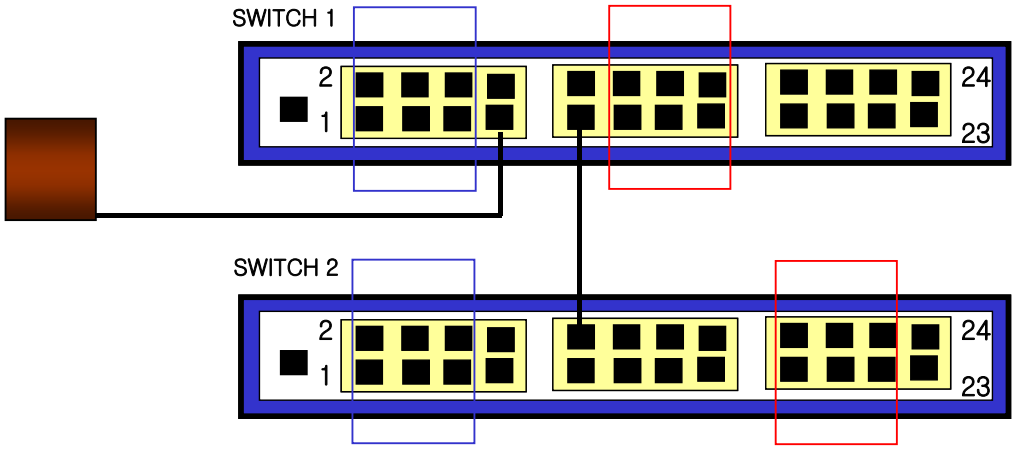
Assigning a VLAN Tag

When a VLAN is created, it is assigned with VLANid. A port defined as a trunk port of tagged VLAN uses frames with 802.1Q VLAN tag attached. In this case, VLANid of the tagged VLAN is used as a tag for those frames.

All ports of VLAN are not tagged. When a frame received through a port is transferred to an external switch, the switch determines whether the destination port of the frame uses tagged frame or untagged frame. The switch adds or deletes tag depending on port settings of VLAN.

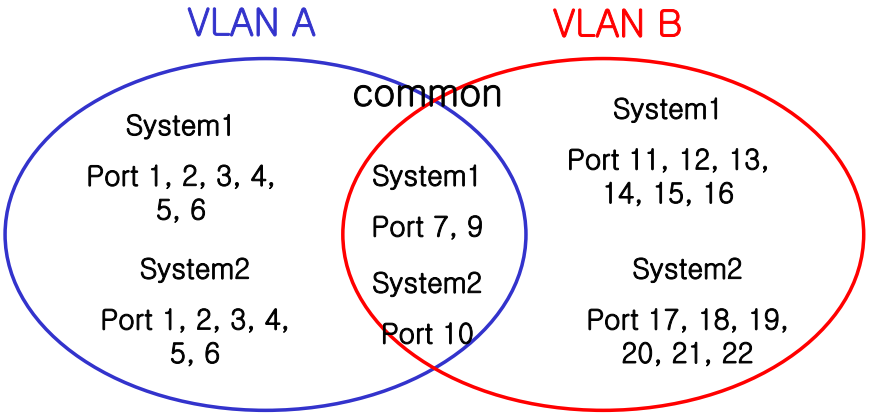
Notice Tagged frames received through a port for which no VLAN is configured would be ignored. For instance, a switch of members of VLANid 10 or 20 would ignore a frame of VLANid 30.

<5> illustrates a physical configuration of network that uses both tagged frame and untagged frame.



<Figure 5> Physical Diagram of Tagged Frames and Untagged Frames

<6> shows a logical diagram for the network above.



<Figure 6> Logical Diagram of Tagged Frame and Untagged Frame

In

<5> and <6>:

- Trunk port (Tagged port) of each switch transfers traffic of VLAN A and VLAN B.
- Trunk port of each switch transfers tagged frames.
- The server connected to port 17 in system 1 is equipped with a network interface card that supports 802.1Q tag and is a member of both VLAN A and VLAN B.
- Other terminals send and receive untagged frames.

When a frame is received, the switch determines using a tagged frame or an untagged frame for the destination port. All frames sent/received to / from a server or a trunk port would be tagged but those transmitted to other devices in the network would not be tagged.

Combining Port-Based VLAN and Tagged VLAN

It is possible to build port-based VLAN and tagged VLAN in a switch. A port exclusively included in a port-based VLAN can be a member of several VLANs. In other words, a port can be a member of one port-based VLAN and several tagged VLAN at the same time.

VLAN Configuration

VLAN ID

Numbers from 1 through 4,094 are used for VLAN IDs to identify VLANs. VLAN id 1 is reserved for one *default VLAN* created when the switch is initialized. Therefore, new VLANs added can not use VLAN id 1.

VLAN id is used as a tag attached to each frame when the affected port, which is a member of the tagged VLAN, works in trunk mode. Where VLAN id is defined incorrectly, frames may be transferred to an undesired VLAN. Therefore, VLAN id should be determined considering the whole network configuration.

Default VLAN

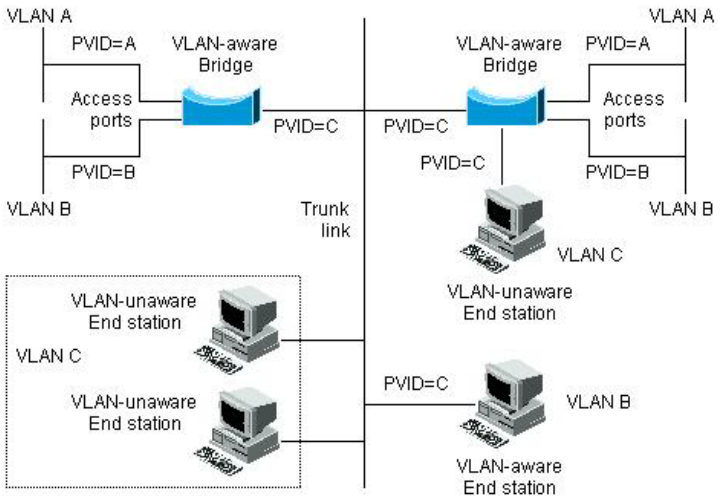
Default VLAN defined in a switch is featured as follows.

- The default VLAN uses VLANid 1.
- The default VLAN is untagged.
- In initial state, the default VLAN for each port is set to native VLAN.

Native VLAN

Each physical port carries a PVID (Port VLAN ID). The native VLAN ID is assigned as PVID of 802.1Q port. All untagged frames are transferred to the VLAN specified by PVID. When an untagged frame is received through a port, the PVID included in the frame is regarded as a tag.

As seen in <, untagged frames are permitted to coexist with frames with PVID defined, bridges or end stations supporting VLAN can be connected to those not supporting VLAN with cable.



<Figure 7> Native VLAN

In <7>, the two end stations shown at the bottom are connected to the central trunk link. They are unaware of VLAN but PVID of the bridge which is aware of VLAN will allow them to be included in VLAN C. As an end station which is not aware of VLAN sends only untagged frames, the equipment which is aware of VLAN will transfer the untagged frames to VLAN C.

VLAN Setup

This section describes the commands used for setting up VLAN in E3208E ONU. You can set up VLAN as follows.

1. Set the values associated with the created VLAN.
2. Set a port mode depending on the VLAN type to which ports will be assigned.
3. Assign more than one port to VLAN. Determine use of 802.1Q tag when adding a port to VLAN.

VLAN Setup Commands

The following table summarizes the commands used for setting up a VLAN.

<Table 36> VLAN Setup Commands

Command	Description	Mode
vlan *vlanid*	Creates deletes and modifies VLAN parameters. 1 is reserved for the default VLAN. *vlanid* : A value between 2 and 4094.	config
switchport mode {access|trunk}	Sets a VLAN type of a port. **access** – Sets a port to access mode (port-based VLAN). The port will act as an interface of a single VLAN which transfers untagged frames. **trunk** – Sets a port to trunk mode (tagged VLAN). The port will send or receive tagged frames.	Interface
switchport access vlan *vlanid*	Sets an access port of VLAN. The port set to access mode will act as a member of VLAN. vlanid : A value between 1 and 4094	Interface
switchport trunk add *vlanid*	Sets a port as a trunk port of VLAN. To set the port as a trunk port of several VLANs, repeat this command for each VLAN. *vlanid* : A value between 2 and 4094. The default VLAN(VLANid=1) is port-based VLAN.	Interface
switchport trunk native *vlanid*	Sets a native VLAN to transfer untagged frames to a trunk port of tagged VLAN in 802.1Q trunk mode. The default VLAN (VLANid = 1) will be set to native VLAN provided that a native VLAN is not defined separately. *vlanid* : A value between 1 and 4094.	Interface
switchport trunk remove {*vlanid*|all}	Removes a member of VLAN for the specified port. *vlanid* : A value between 2 and 4094. all : Deletes the member from all VLANs.	Interface

Example of VLAN Setup

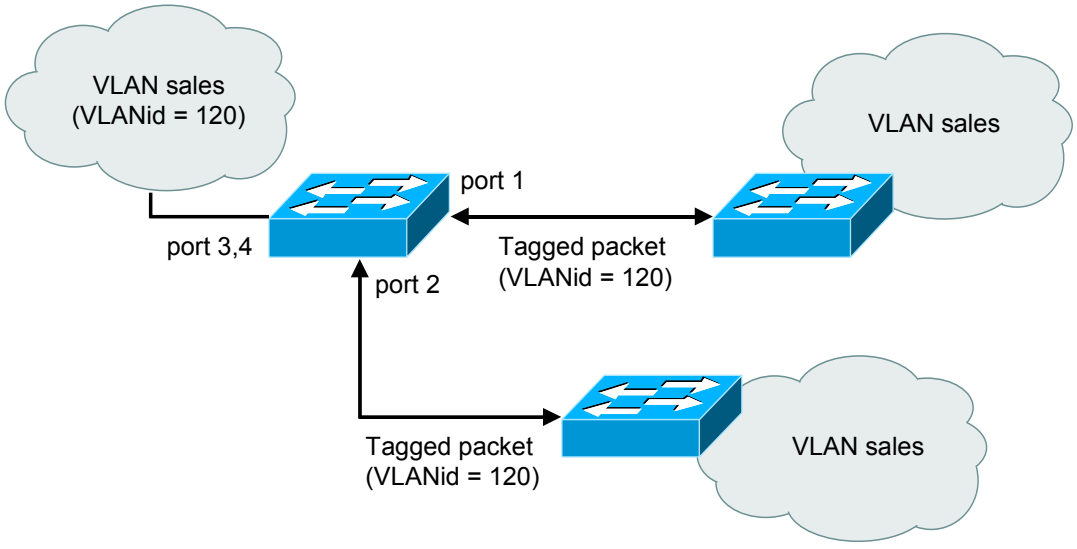
The following shows an example of setting VLANid to 1000 and IP address 132.15.121.1 to VLAN and assigning port 2 and port 4 to VLAN.

```
Switch(config)# vlan 1000
Switch(config)# interface vlan1000
Switch(config-int-vlan)# ip address 132.15.121.1/24
Switch(config-int-vlan)# interface fa2
Switch(config-int-fa2)# switchport mode access
Switch(config-int-fa2)# switchport access vlan 1000
Switch(config-int-fa2)# interface fa4
Switch(config-int-fa4)# switchport mode access
Switch(config-int-fa4)# switchport access vlan 1000
```

In the following example, tag-based VLANid is set to 2000 and port 1 and port 2 are added to VLAN as trunk port.

```
Switch(config)# vlan 2000
Switch(config)# interface fa1
Switch(config-int-fa1)# switchport mode trunk
Switch(config-int-fa1)# switchport trunk add 2000
Switch(config-int-fa1)# interface fa2
Switch(config-int-fa2)# switchport mode trunk
Switch(config-int-fa2)# switchport trunk add 2000
```

The following shows an example of creating VLAN *sales* of VLANid 120 supporting both tagged ports (trunk ports) and untagged ports (access ports). Port 1 and port 2 are tagged and port 3 and port 4 are untagged. Ports will be untagged unless otherwise specified.



<Figure 8> Example of VLAN Settings– Tagged and Untagged VLAN

```
Switch(config)# vlan 120
Switch(config)# interface fa1
```

```
Switch(config-int-fa1)# switchport mode trunk
Switch(config-int-fa1)# switchport trunk add 120
Switch(config-int-fa1)# interface fa2
Switch(config-int-fa2)# switchport mode trunk
Switch(config-int-fa2)# switchport trunk add 120
Switch(config-int-fa2)# interface fa3
Switch(config-int-fa3)# switchport access vlan 120
Switch(config-int-fa3)# interface fa4
Switch(config-int-fa4)# switchport access vlan 120
```

The following shows an example of defining Port 1 as a member of both port-based VLAN *Marketing* and tagged VLAN *Engineering*. VLANid of VLAN *Marketing* is 200 and VLANid of VLAN *Engineering* is 400.

```
Switch(config)# vlan 200
Switch(config)# vlan 400
Switch(config-vlan)# exit
Switch(config)# interface fa1
Switch(config-int-fa1)# switchport mode trunk
Switch(config-int-fa1)# switchport trunk native 200
Switch(config-int-fa1)# switchport trunk add 400
```

The switch will transfer untagged frames received through the port fa1/1 to member port of VLAN *marketing*.

Viewing VLAN Configuration

Use the following command to view the VLAN setup information.

<Table 37> Viewing VLAN Configuration

Command	Description	Mode
show vlans	Shows the following information on VLAN. VLANid Member port	Privileged

```
Switch# show vlans
VLAN MEMBER-LIST
--------------------------------------------------------------------------------
   1 fa1    fa2   fa3   fa4   fa5 gi1
  11 fa6   fa7   fa8
 --------------------------------------------------------------------------------
Switch#
```

Chapter 4. IP Environment

This chapter describes how to set IP addresses.

Overview

This chapter describes how to set IP addresses.

To set an IP address, it is needed to assign the IP address to a network interface. Then, the interface is activated as a layer 3 interface.

The E3208E ONU can assign IP addresses to the following interfaces.

- VLAN interfaces

Assigning an IP Address to Network Interface

IP address identifies a destination to which the received IP datagram will be transferred. Some IP addresses reserved for special purposes cannot be used as host, subnet or network addresses. The following table lists IP address ranges, reserved addresses and available addresses.

<Table 38> Available IP addresses

Class	Address Range	Status
A	0.0.0.0	Reserved
	1.0.0.0 ~ 126.0.0.0	Available
	127.0.0.0	Reserved
B	128.0.0.0 ~ 191.254.0.0	Available
	191.255.0.0	Reserved
C	192.0.0.0	Reserved
	192.0.1.0 ~ 223.255.255.254	Available
	224.255.255.0	Reserved
D	224.0.0.0 ~ 239.255.255.255	Multicast group address
E	240.0.0.0 ~ 255.255.255.254	Reserved
	255.255.255.255	Broadcast

Notice For the official description of IP addresses, refer to RFC1166, Internet Number.

Notice To be assigned a network number, inquire of your ISP (Internet Service Provider).

The E3208E ONU supports assigning several IP addresses to one interface. The E3208E ONU permits up to two IP addresses assigned to one interface. Multiple IP addresses are useful in various circumstances. Typical applications of multiple IP addresses are described below:

- Host addresses are not sufficient for specific network segments. For example, assume that you want to build a subnet which allows 254 hosts per logical subnet over one physical subnet that requires 300 host addresses. If multiple IP addresses are used for a router or an access server, you can build two logical subnets with one physical subnet.
- Many conventional networks are not composed of subnets but built using layer 2 bridges. Using multiple addresses facilitates conversion into subnets and into router-based network. A router included in a conventional bridge segment can easily be aware of many subnets included in the segment.
- Two subnets of a network can be separated by other network. Using multiple addresses, you can build a network with subnets physically separated by other network. In this example, the first network will be extended or located above the second network. A subnet cannot simultaneously appear at more than one activated interface of router.

You can assign an IP address to network interface, using the following command in interface setup mode.

<Table 39> Command for Assigning an IP Address

Command	Description
ip address *ipaddress/prefixlen*	Sets an IP address to interface.

Notice Prefixlen indicates the bit length of ip address to identify the network.

ARP (Address Resolution Protocol)

You can view the information on ARP table in privilege mode, using the command given in the following table.

<Table 40> Command for ARP Environment Setup

Command	Description
show arp	Shows the entry of ARP table.

Setting a Default Gateway

The default gateway is very useful where it is impossible to establish a path to a specific destination for IP packets. Using the following command in Config mode, you can set a default gateway to send packets that cannot be routed.

<Table 41> Command for Setting a Default Gateway

Command	Description
ip default-gateway *gateway-ipaddress*	Registers a default gateway. *gateway-ipaddress*: IP address of gateway.

To Show the default gateway information, use the following command in privileged mode.

<Table 42> Showing Default Gateway Information

Command	Description
show ip default-gateway	Shows default gateway information.

Example of IP Settings

This section provides an example of IP address settings:

- Assign IP address to network interface
- ARP
- Default gateway

The following shows an example of setting Class C IP address 192.10.25.1 to vlan5 interface of the switch.

```
Switch(config)# interface   vlan5
Switch(config-int-vlan5)# ip address   192.10.25.1/24
```

The following shows an example of showing the ARP table entry.

```
Switch# show arp
------------------------------------------------------------------
 IP Address          MAC Address        IPF          PORT     Flags
------------------------------------------------------------------
192.10.25.190     0000.f083.f6d4   vlan5     fa2       S
------------------------------------------------------------------
 total 1 entries found
```

The following shows an example of setting the default gateway of switch to 192.10.25.254.

```
Switch(config)# ip default-gateway 192.10.25.254
Switch(config)# end
Switch# show ip default-gateway

default gateway information
   gateway: 192.10.25.254, vlan5, active
```

Chapter 5. DHCP Relay and Client

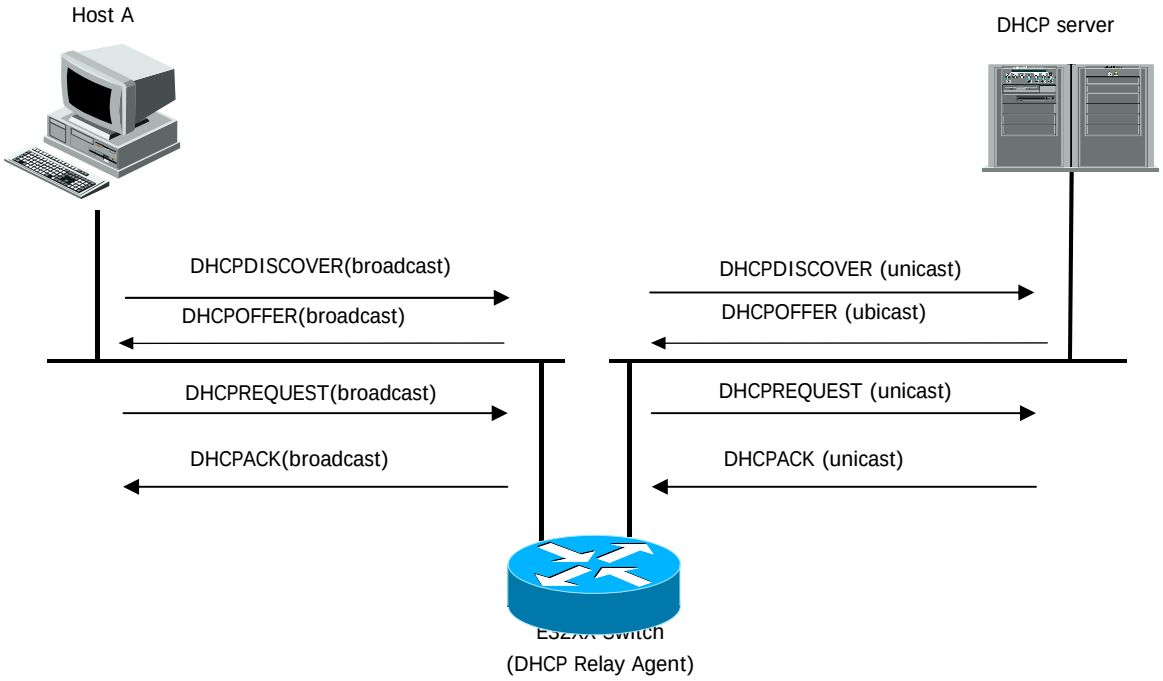
This chapter describes how to set DHCP Relay and DHCP Client.

Configuration of DHCP Relay Function

Overview of DHCP Relay

DHCP (Dynamic Host Configuration Protocol) provides a mean to dynamically assign reusable IP addresses and parameters to other IP hosts(DHCP clients) of an IP network. And DHCP Relay is a protocol that receives and transfers DHCP or BOOTP packet from a client to a DHCP Server(s) which resides in other network.

<Figure 9> illustrates a process for the DHCP server acting as a DHCP relay agent to transfer messages of DHCP client to a DHCP server of other network.



<Figure 9> Message Forwarding by DHCP Server as a DHCP Relay Agent

1. A DHCP client sends the broadcast message *DHCPDISCOVER* to get an IP address.
2. Where the DHCP server cannot meet the request of the client, it transfers the request to the DHCP server specified by the operator using the unicast message *DHCPDISCOVER*.
3. Receiving the message from the DHCP relay agent, the DHCP server transfers IP address of the client and router information to the DHCP relay agent using the unicast message *DHCPOFFER*.
4. The DHCP relay agent sends the received *DHCPOFFER* message to the client.
5. The *DHCPREQUEST* and *DHCPACK* messages between the DHCP server and the client are also transferred to the DHCP relay agent in the similar way.

Setting a DHCP Relay Agent

Using the E3208E as a DHCP relay agent, you can relay the DHCP request from a DHCP client to the specified DHCP server.

Activation of DHCP relay function

As a default, DHCP relay function is not activated. In order to activate, you need to get in global configuration mode and use the following commands.

<Table 43> Activation of DHCP relay function

Command	Description
service dhcp relay	To activate switch's DHCP relay function 'no' prefix shall be used in front of activation command to inactive it.

The box below shows the example how DHCP Relay function is activated.

```
Switch# configure terminal
Switch(config)# service dhcp relay
Switch(config)# exit
Switch# show ip dhcp relay

DHCP relay                      : Enabled
DHCP Smart Relay feature        : Disabled
DHCP Smart Relay retry count    : 3
DHCP server-id based relay      : Disabled
Verification of MAC address     : Enabled
Insertion of option 82          : Disabled
DHCP Option82 Management-IP     : 0.0.0.0
DHCP maximum hop count          : 10

DHCP helper-address is configured on following servers:
  None
```

Setting DHCP server at DHCP relay agent

To configure DHCP Server at DHCP relay agent, the following command is to be used in Global configuration mode.

<Table 44> Setting DHCP server at DHCP relay agent

Command	Description
Ip dhcp-server *address*	To register the IP address of DHCP Server when the DHCP relay agent relays DHCP request packet. 'no' prefix shall be used to remove the IP address of DHCP Server.

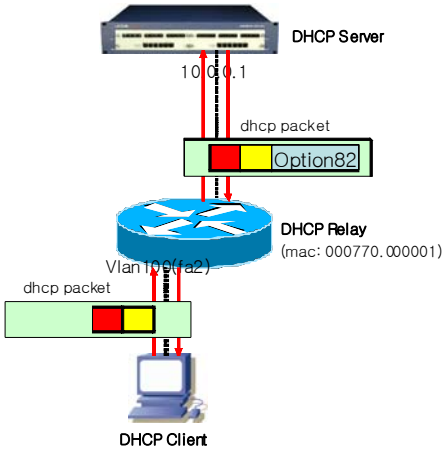
Notice E3208E can have up to 20 helper-addresses as a DHCP relay Agent.

The box below shows the example how to set DHCP Server address at a DHCP Relay Agent.

```
Switch# configure terminal
Switch(config)# ip dhcp helper-address 192.168.0.254
Switch(config)# exit
Switch#
Switch#
Switch# show ip dhcp relay

DHCP relay                          : Enabled
DHCP Smart Relay feature            : Disabled
DHCP Smart Relay retry count        : 3
DHCP server-id based relay          : Disabled
Verification of MAC address         : Enabled
Insertion of option 82              : Disabled
DHCP Option82 Management-IP         : 0.0.0.0
DHCP maximum hop count              : 10

DHCP helper-address is configured on following servers:
   192.168.0.254
```

Configuring DHCP relay information option (OPTION82)

DHCP relay agent, when it transfer DHCP request from a DHCP client to DHCP server, can provide DHCP relay information option by which the information of DHCP relay agent itself and client interface. Then DHCP Server will assign IP address and determine host configuration policy by seeing the Option82 information. For example, if a certain specified port of a specified switch is correlated with a MAC address ‘a’, later when a request with the same port of the same switch combined with different MAC address, let’s say ‘b’ would arrive in DHCP server, then DHCP server can reject or ignore it.



<Figure 10> DHCP Relay Option82

As shown in figure 10, DHCP Option82 is only used between DHCP Relay and DHCP Server. DHCP Relay shall add DHCP Option82 into the packet when it forwards the packet sent from a DHCP Client which is heading for DHCP Server, and remove it from the packet which is sent from DHCP Server to DHCP Client.

Activation of DHCP relay information option

In order to activate the function of relay information option at DHCP relay agent, the following command is to be used.

<Table 45> Activation of DHCP relay information option

Command	Description
ip dhcp relay information option	To activate DHCP relay information(option-82 field) Default setting is inactive.

The box below shows the example how to activate Option82 function of DHCP Relay.

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

DHCP relay                    : Enabled
```

```
DHCP Smart Relay feature          : Disabled
DHCP Smart Relay retry count      : 3
DHCP server-id based relay        : Disabled
Verification of MAC address       : Enabled
Insertion of option 82            : Enabled
DHCP relay information policy     : replace
DHCP Option82 Management-IP       : 0.0.0.0
DHCP maximum hop count            : 10

DHCP helper-address is configured on following servers:
   192.168.0.254
```

Setting Relay Information Policy

The default policy of the E3208E is to replace the relay information of the packet received from DHCP client with the relay information of the switch. You can change the default policy of the switch using the following command in Global mode.

<Table 46> Setting Relay Information Policy

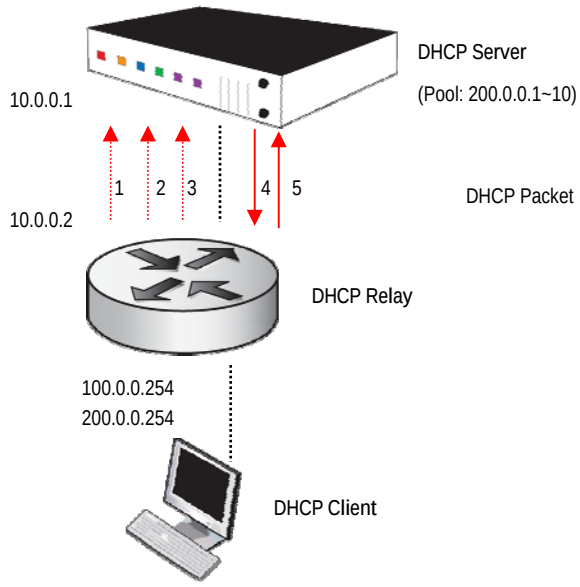
Command	Description
ip dhcp relay information policy {drop|keep|replace}	The default setting is 'replace'. drop: Drops the packet with relay information inserted. keep: Keeps the current relay information. replace: Replaces the current relay information with the relay information of the switch.

The following example shows how DHCP Relay Information Option is set. In this case it is set to Drop.

```
Switch# configure terminal
Switch(config)# ip dhcp relay information policy drop
Switch(config)# exit
Switch# show ip dhcp relay

DHCP relay                        : Enabled
DHCP Smart Relay feature          : Disabled
DHCP Smart Relay retry count      : 3
DHCP server-id based relay        : Disabled
Verification of MAC address       : Enabled
Insertion of option 82            : Enabled
DHCP relay information policy : drop
DHCP Option82 Management-IP       : 0.0.0.0
DHCP maximum hop count            : 10

DHCP helper-address is configured on following servers:
   192.168.0.254
```

Setting DHCP Smart Relay

Where the smart-relay feature is enabled, the DHCP Relay Agent changes the gateway address (giaddr) to the next ip address in case it fails to receive the BOOTPREPLY message from the DHCP Server by the specified count(default : 3).



<Figure 11> DHCP Smart-Relay procedure

1. When the DHCP Relay receives a request packet from a DHCP Client, it assigns an address '100.0.0.254' to giaddr and forwards it to a DHCP Server. Then the DHCP Server shall look at the giaddr of the packet and learn that it's not its packet, and subsequently drop it.
2. The DHCP Client asks for IP address again as it has not received Reply packet. Receiving this packet, the Relay Agent shall increase the Retry Count for the IP request from the DHCP Client.
3. If the Retry Count is 3 ('4' th packet), DHCP Relay shall set 'giaddr' to '200.0.0.254'. DHCP Server then, by seeing the giaddr and knowing that it's in its pool range, send out Reply packet to the Relay Agent.

<Table 47> Setting DHCP Smart Relay

Command	Description
ip dhcp smart-relay	To activate DHCP smart-relay function. Default is inactive.

The following example shows how DHCP Smart-Relay is enabled.

```
Switch# configure terminal
Switch(config)#
Switch(config)# ip dhcp smart-relay
Switch(config)# exit
Switch#
Switch#
Switch# show ip dhcp relay
DHCP relay                          : Enabled
DHCP Smart Relay feature            : Enabled
DHCP Smart Relay retry count        : 3
DHCP server-id based relay          : Disabled
```

```
Verification of MAC address      : Enabled
Insertion of option 82           : Enabled
DHCP relay information policy : drop
DHCP Option82 Management-IP      : 0.0.0.0
DHCP maximum hop count           : 10

DHCP helper-address is configured on following servers:
   192.168.0.254
```

Configuring DHCP Relay Verify MAC-Address

When a DHCP Client Identifier or a Client HW Address is forged, in order to drop the packet, the following command is used.

<Table 48> Configuring DHCP Relay Verify MAC-Address

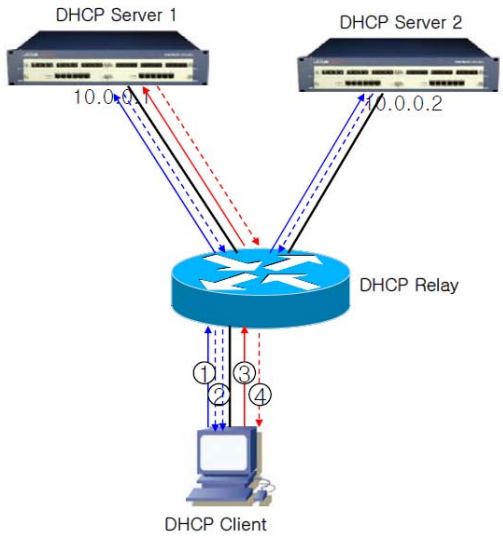
Command	Description
ip dhcp snooping verify mac-address	To Drop packets when its DHCP Client Identifier or Client HW Address is forged. Default value is 'Enabled'.

The box below shows how DHCP Relay Verify Mac-Address fuction is used.

```
Switch# configure terminal
Switch(config)# no ip dhcp relay verify mac-address
Switch(config)# exit
Switch# show ip dhcp relay

DHCP relay                       : Enabled
DHCP Smart Relay feature         : Enabled
DHCP Smart Relay retry count     : 3
DHCP server-id based relay       : Disabled
Verification of MAC address      : Disabled
Insertion of option 82           : Enabled
DHCP relay information policy : drop
DHCP Option82 Management-IP      : 0.0.0.0
DHCP maximum hop count           : 10

DHCP helper-address is configured on following servers:
   192.168.0.254
```

Configuring DHCP relay server-id-relay

When multiple DHCP Servers are configured at DHCP relay agent, the DHCP relay agent provides the function of DHCP relay server-id-relay to relay only to the DHCP Server which DHCP Client designated in advance.



<Figure 12> DHCP Relay Server-Id-Relay procedure

1. DHCP Relay Agent forwards DHCPDISCOVER packet to its pre-registered servers, for example, DHCP Server 1, DHCP Server 2 when it receives them from a DHCP Client.
2. DHCP Server 1 and DHCP Server 2 respectively receive the DHCPDISCOVER and then reply by sending back DHCPOFFER packet. In the DHCP Server Identifier Option Filed of DHCPOFFER packet is the Server IP address.
3. When the DHCP Client receives DHCPOFFER packets from DHCP Server 1 and DHCP Server 2, it chooses either one of them (ex. DHCP Server 1) and transmit DHCPREQUEST packet. In DHCPREQUEST packet is the DHCP Server Identifier Option.
4. The DHCP Relay Agent, when it receives DHCPREQUEST packet, will look into the Server Idnetifier Option of the packet and forward the DHCPREQUEST packet only to DHCP Server 1. However if the DHCP Server Selection function is not enabled, then DHCP Relay Agent will transmit to all its registered DHCP Servers.

<Table 49> Configuring DHCP relay server-id-relay

Command	Description
ip dhcp relay server-id-relay	To activate DHCP relay server-id-relay function. Default is 'Disable'.

The box below shows how DHCP Relay Server-Id-Relay function works.

```
Switch# configure terminal
Switch(config)# ip dhcp relay server-id-relay
  <cr>
Switch(config)# ip dhcp relay server-id-relay
Switch(config)# exit
Switch#
Switch# show ip dhcp relay
```

```
DHCP relay                          : Enabled
DHCP Smart Relay feature            : Enabled
DHCP Smart Relay retry count    : 3
DHCP server-id based relay        : Enabled
Verification of MAC address      : Enabled
Insertion of option 82              : Enabled
DHCP relay information policy : drop
DHCP Option82 Management-IP      : 0.0.0.0
DHCP maximum hop count              : 10

DHCP helper-address is configured on following servers:
   192.168.0.254
```

Monitoring and managing DHCP relay

<Table 50> Commands for DHCP relay monitor and management

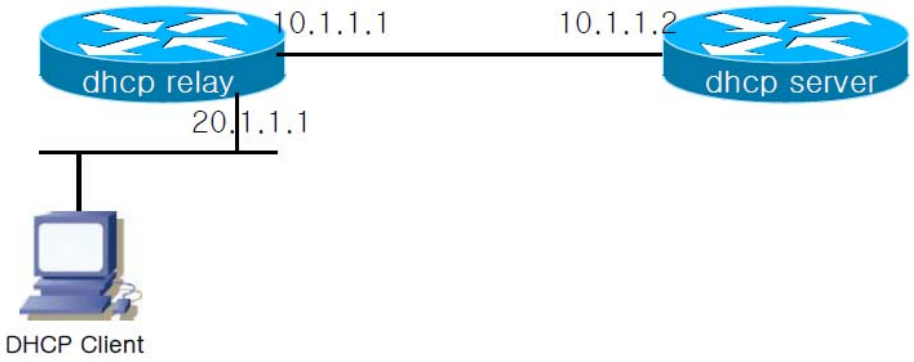
Command	Description
show ip dhcp relay	Display the DHCP Relay Confiuration
show ip dhcp relay information option	Display the values of DHCP relay information option
show ip dhcp relay statistics	Display the values of relay statistics and message counter
debug ip dhcp relay {events|packets}	Enable the debugging function of DHCP relay

DHCP Relay configuration example

In this clause the following examples are shown.

- Configuring DHCP Relay Agent
- Monitoring and managing DHCP Relay Agent

The following example shows how a DHCP Relay Agent is configured to transfer client's DHCP request packet to DHCP Server.



<Figure 13> Configuring the environment of DHCP Relay agent

```
Switch(config)# configure terminal
Switch(config)# ip dhcp-server 10.1.1.2
Switch(config)# service dhcp relay
Switch(config)# end
Switch#
Switch# show ip dhcp relay

DHCP relay                      : Enabled
DHCP Smart Relay feature        : Disabled
DHCP Smart Relay retry count    : 3
DHCP server-id based relay      : Disabled
Verification of MAC address     : Enabled
Insertion of option 82          : Disabled
```

DHCP maximum hop count : 10

DHCP helper-address is configured on following servers:
10.1.1.2

Switch # show ip dhcp relay statistics

Destination(Server)	Value
Client-packets relayed	8
Client-packets errored	0

Destination(Client)	value
Server-packets relayed	6
Server-packets errored	0
Giaddr errored	0
Corrupt agent options	0
Missing agent options	0
Bad circuit id	0
Missing circuit id	0

<Table 51> Field Description

Field title	Description
Client-packets relayed	Succeed to forward the packet from client to server.
Client-packets errored	Failed to forward the packet from client to server.
Server-packets relayed	Succeed to forward the packet from server to client
Server-packets errored	Failed to forward the packet from server to client.
Giaddr errored	There is no giaddr in the DHCP packet received from a server.
Corrupt agent options	When Option82 is Enabled as to Relay Agent, the DHCP packet that came from a server has an Option82 error (The actual Option82 Length and the value of the Option82 Length field in the packet is different)
Missing agent options	When Option82 is Enabled as to Relay Agent, the DHCP packet doesn't have Option82 information.
Bad circuit id	When Option82 is Enabled as to Relay Agent, the value of circuit id in the Option82 information has errors
Missing circuit id	When Option82 is Enabled as to Relay Agent, the DHCP packet doesn't have circuit id in the Option82 information.

DHCP snooping function

DHCP snooping function

DHCP Snooping verifies the validity of DHCP Discover Message, conducts the Rate-limit as to the DHCP Message, adds/removes Option82 information, creates and manages the DHCP Snooping binding database. DHCP Snooping works with respect to the unit of Vlan and is basically in 'Inactive'.

Trust and Untrust Source

DHCP Snooping discerns the traffic sources whether it is 'trusted' or 'untrusted'. In case of untrusted sources, it can conduct any sort of traffic attack or other forms of harmful behavior. To prevent system from this danger, DHCP Snooping can perform message filtering from untrusted source.

DHCP Snooping Binding Database

DHCP Snooping dynamically creat a database and maintain it by using of the information of the DHCP Message which it intercepts. The database includes the entry for the untrusted hosts of a VLAN which is enabled for DHCP Snooping. As a Database Entry, any DHCP message that comes from DHCP Server or Client is to be added after validation check. And in case of the serial sequence of normal messages from an same DHCP Client, only the last one message is to be registered into the database. When IP Address lease time is expired or DHCPRELEASE message is received, the state field is set to time expired or released respectively.

In the DHCP Snooping binding database, host MAC Address, Client Hardware Address, Client Identifier, leased IP address, lease time, received time, State, Vlan ID, and interface port information are included.

Packet Validation

The switch verifies the validity of DHCP packet which comes from the untrusted interface of VLAN where DHCP Snooping is enabled. The switch will update the state field in the DHCP Snooping binding Table when the following event occurs.

The switch receives DHCPDISCOVER packet from the untrusted interface while source MAC address and DHCP Client Identifier or DHCP Client Hardware Address are not congruent. Packet Rate-limit

DHCP Snooping conducts Rate-limit function with respect to the DHCP Packet that comes from same DHCP Client. DHCP Snooping allows two DHCP Packets per second as far as they are from same DHCP Client.

Packet Rate-limit

DHCP Snooping conducts Rate-limit function with respect to the DHCP Packet that comes from the same DHCP Client. DHCP Snooping allows two DHCP Packets per second as far as they are from same DHCP Client.

Configuring DHCP Snooping

When E3208E is enabled for DHCP Snooping, the switch will conduct Snooping with every DHCP packets that pass through it to creat the DHCP Snooping Binding Entry in which DHCP Client information, IP Lease information, and Client interface information are kept.

Activation of DHCP snooping function

As default value, DHCP Snooping function is 'inactive.' In global setting mode, the following commands are used to activate the DHCP Snooping function.

<Table 52> Activation of DHCP snooping function

Command	Description
ip dhcp snooping	To enable DHCP Snooping to be 'no' prefix shall be used in front of activation command to inactive DHCP Snooping.

The box below shows how DHCP Snooping function is enabled.

```
Switch# configure terminal
Switch(config)# ip dhcp snooping
Switch(config)# exit
Switch# show ip dhcp snooping
Switch DHCP Snooping is enabled
Invalid entry keep time: 14400 mins
DHCP Packet rate-limit per client: 2 pps
Verification of hwaddr field is enabled
Insertion of option 82 is disabled
DHCP snooping is configured on following VLANs:
                none
```

Configuring DHCP Snooping Vlan

The target VLAN which is related with Snooping function is to be set. Other DHCP packet that pass through different VLAN from the target VLAN are not processed for Snooping.

<Table 53> Configuring DHCP Snooping Vlan

Command	Description
ip dhcp snooping vlan *vlan_ID*	To set the target Vlan for Snooping DHCP packet 'no' prefix shall be used in front of configuring command to remove DHCP Snooping Vlan

Notice In case DHCP Snooping is in use with DHCP Relay, the DHCP Relay will forward the packet.

Notice In case DHCP Snooping is in use with DHCP Relay, the both Vlans of DHCP Server and DHCP Client need to be set for Snooping Vlan.

The box below shows how DHCP Snooping in ‘vlan1’ is enabled.

```
Switch# configure terminal
Switch(config)#
Switch(config)#
Switch(config)# ip dhcp snooping vlan 1
Switch(config)# exit
Switch# show ip dhcp snooping
Switch DHCP Snooping is enabled
Invalid entry keep time: 14400 mins
DHCP Packet rate-limit per client: 2 pps
Verification of hwaddr field is enabled
Insertion of option 82 is disabled
DHCP snooping is configured on following VLANs:
                vlan1
```

Configuring DHCP Snooping information option (OPTION82)

DHCP Snooping shall provide the DHCP Snooping information option function by which the information about DHCP client interface and connect equipment can be supplied.

Activation of DHCP Snooping information option function:

In order to activate the information option function in DHCP Snooping, the following command is used.

<Table 54> Configuring DHCP Snooping information option (OPTION82)

Command	Description
ip dhcp snooping information option	To activate DHCP Snooping information(option-82 field) Default value is ‘inactive’.

The box below shows how DHCP Snooping Information Option function is enabled.

```
Switch# configure terminal
Switch(config)# ip dhcp snooping information option
Switch(config)# exit
Switch# show ip dhcp snooping
Switch DHCP Snooping is enabled
Invalid entry keep time: 14400 mins
DHCP Packet rate-limit per client: 2 pps
Verification of hwaddr field is enabled
Insertion of option 82 is enabled [drop]
DHCP snooping is configured on following VLANs:
  vlan1
```

Setting the policy of retransmission of DHCP Snooping Information option

Basically the policy of E3208E's DHCP Snooping information shall drop the packets which have information Option. In order to change the policy, the following command is used in Global mode.

<Table 55> DHCP Snooping Information option

Command	Description
ip dhcp snooping information policy {drop|keep|replace}	Default is 'drop' drop : to discard the packet which has DHCP Snooping information. keep : to maintain existing DHCP Snooping information. replace : To replace existing DHCP Snooping information with switch's DHCP Snooping information.

The box below shows how DHCP Snooping Information Option is set to 'Keep'

```
Switch# configure terminal
Switch(config)# ip dhcp snooping information policy keep
Switch(config)# exit
Switch#
Switch# show ip dhcp snooping
Switch DHCP Snooping is enabled
Invalid entry keep time: 14400 mins
DHCP Packet rate-limit per client: 2 pps
Verification of hwaddr field is enabled
Insertion of option 82 is enabled [keep]
DHCP snooping is configured on following VLANs:
  vlan1
```

Configuring DHCP Snooping Trust Port

The reliable ports (ex, port toward DHCP Server direction) can be configured as Trust Port. Once Trust Port is setup, then all Request packets from Host shall be forwarded to the Trust Port.

<Table 56> Configuring DHCP Snooping Trust Port

Command	Description
ip dhcp snooping trust	To designate the specified port as Trust Port. The DHCP packets that arrive to Trust Port are not due for Validation check. All Request packets from Host shall be forwarded only to Trust Port. As a default, all ports are 'untrust' port.

The box below shows how port 'fa1' is set to be Trust Port.

```
Switch(config)# interface fa1
Switch(config-if-fa1)# ip dhcp snooping trust
Switch(config-if-fa1)# end
```

```
Switch# show ip dhcp snooping interface
Interface              Trust State       Max Entry
---------------        -----------       ------------
fa1                    Trusted                 2000
fa2                    Untrusted               2000
fa3                    Untrusted               2000
fa4                    Untrusted               2000
fa5                    Untrusted               2000
fa6                    Untrusted               2000
fa7                    Untrusted               2000
fa8                    Untrusted               2000
gi1                    Untrusted               2000
```

Configuring DHCP snooping max-entry

To set the number of DHCP Snooping max-entry per port, the following command is used.

<Table 57> Configuring DHCP snooping max-entry

Command	Description
ip dhcp snooping max-entry	To set the number of DHCP Snooping max-entry per port. The number of Max-entry per port is 2000.

The box below shows how the DHCP Snooping Max-Entry of ‘fa1’ is set to be ‘100’.

```
Switch# configure terminal
Switch(config)# interface fa1
Switch(config-if-fa1)# ip dhcp snooping max-entry 100
Switch(config-if-fa1)# end
Switch# show ip dhcp snooping interface
Interface              Trust State       Max Entry
---------------        -----------       ------------
fa1                    Trusted                  100
fa2                    Untrusted               2000
fa3                    Untrusted               2000
fa4                    Untrusted               2000
fa5                    Untrusted               2000
fa6                    Untrusted               2000
fa7                    Untrusted               2000
fa8                    Untrusted               2000
gi1                    Untrusted               2000
                Switch#
```

Configuring DHCP Snooping Entry Time

In order to set the time which specifies for the period the Invalid DHCP Snooping Binding Entry shall be stored and maintained, the following command is used.

<Table 58> Configuring DHCP Snooping Entry Time

Command	Description
ip dhcp snooping entry-time	To set the time period for storage of the invalid entry. The unit is minute. The default value is 14400 minutes (10days).

The box below shows how the Entry Time of DHCP Snooping is set to be '10 minutes'.

```
Switch# configure terminal
Switch(config)# ip dhcp snooping entry-time
  <5-65535>  Minutes
Switch(config)# ip dhcp snooping entry-time 10
Switch(config)# ex
Switch# sh ip dhcp snooping
Switch DHCP Snooping is enabled
Invalid entry keep time: 10 mins
DHCP Packet rate-limit per client: 100 pps
Verification of hwaddr field is enabled
Insertion of option 82 is enabled [keep]
DHCP snooping is configured on following VLANs:
 vlan1
```

Configuring DHCP Snooping Rate-Limit

In order to set the Rate-limit of the DHCP Packets that come from same DHCP Client, the following command is used.

<Table 59> Configuring DHCP Snooping Rate-Limit

Command	Description
ip dhcp snooping rate-limit	To set the acceptable number of packets per second while the packets come from same DHCP Client and have same Packet type. Default is 2 packets per second.

The box below shows how DHCP Snooping Rate-Limit is set to be '100'.

```
Switch# configure terminal
Switch(config)# ip dhcp snooping rate-limit
<1-100>  DHCP Packet rate-limit in pps
Switch(config)# ip dhcp snooping rate-limit 100
Switch(config)# end
Switch#
Switch# show ip dhcp snooping
Switch DHCP Snooping is enabled
Invalid entry keep time: 14400 mins
DHCP Packet rate-limit per client: 100 pps
Verification of hwaddr field is enabled
Insertion of option 82 is enabled [keep]
DHCP snooping is configured on following VLANs:
 vlan1
```

Configuring DHCP Snooping Verify MAC-Address

In case DHCP Client Identifier or Client HW Address are counterfeited, to discard the forged packet the following command is used.

<Table 60> Configuring DHCP Snooping Verify MAC-Address

Command	Description
ip dhcp snooping verify mac-address	To discard the forged packet. Default status for this feature is 'inactive'.

The box below shows how DHCP Snooping Verify Mac-Address function is disabled.

```
Switch# configure terminal
Switch(config)# no ip dhcp snooping verify mac-address
Switch(config)# exit
Switch# show ip dhcp snooping
Switch DHCP Snooping is enabled
Invalid entry keep time: 10 mins
DHCP Packet rate-limit per client: 100 pps
Verification of hwaddr field is disabled
Insertion of option 82 is enabled [keep]
DHCP snooping is configured on following VLANs:
  vlan1
```

DHCP Snooping Manual Binding configuration

The following commands are used to configure the DHCP Snooping Binding Entry.

<Table 61> DHCP Snooping Manual Binding configuration

Command	Description
ip dhcp snooping binding *H.H.H* **vlan** *<1-4094> A.B.C.D* **interface** *IFNAME*	Configure a DHCP Client whose MAC-Address is *H.H.H in the specified* Interface to use IP *A.B.C.D as* its IP address. And the lease time is Infinite.

In the following example, a user whose MAC address is 1111.2222.333 is to use IP 100.0.0.10 being assigned to the port fa2 of Vlan 1 is shown.

```
Switch# configure terminal
Switch(config)# ip dhcp snooping binding 1111.2222.3333 vlan 1 z100.0.0.10 interface fa2
Switch(config)# exit
Switch#
Switch#
Switch# show ip dhcp snooping binding
State Codes: (C) - Invalid Client Identifier, (E) - Lease Time Expired
             (H) - Invalid Client HW Address, (R) - Rate Limit Dropped
             (M) - Mac Validation Check Dropped

Mac Address     IP Address      State                Lease(sec) Vlan Interface
```

```
-------------- --------------- ------------------- ---------- ---- ---------
1111.2222.3333 100.0.0.10      Manual              Infinite   1    fa2
total 4 bindings found
```

DHCP Snooping monitor and management

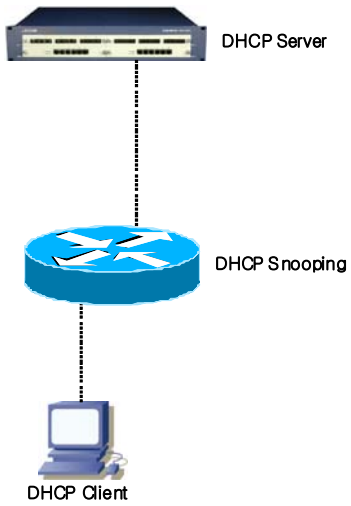
Commands for monitoring and managing DHCP Snooping.

<Table 62> DHCP Snooping monitor and management

Command	Description
show ip dhcp snooping	Display Global DHCP Snooping Configuration
show ip dhcp snooping binding {IFNAME|valid|invalid|manual}	Display DHCP Snooping Binding Entry
show ip dhcp snooping interface	Display the DHCP Snooping Configuration set in the Interface
show ip dhcp snooping statistics	Display the statistics of DHCP Snooping
show debugging ip dhcp snooping	Display the configured status of DHCP Snooping debugging
debug ip dhcp snooping	Activate the function of DHCP Snooping debugging

DHCP snooping configuration example

The following figure shows how the DHCP Snooping Switch which resides in between DHCP Server and DHCP Client, conducts the packet Snooping and creates DHCP Snooping Binding Entry.



<Figure 14> DHCP snooping Configuration

Switch# configure terminal
Switch(config)# **ip dhcp snooping vlan 200**
Switch(config)# **ip dhcp snooping**
Switch (config-if-vlan200)# **end**
Switch# **show ip dhcp snooping binding**
State Codes: (C) - Invalid Client Identifier, (E) - Lease Time Expired
(H) - Invalid Client HW Address, (D) – Rate Limit Dropped

MacAddress	IpAddress	State	Lease(sec)	VlanId	Port
0000.864a.c185	100.0.0.100	Ack	87	200	fa1/8

DHCP Client

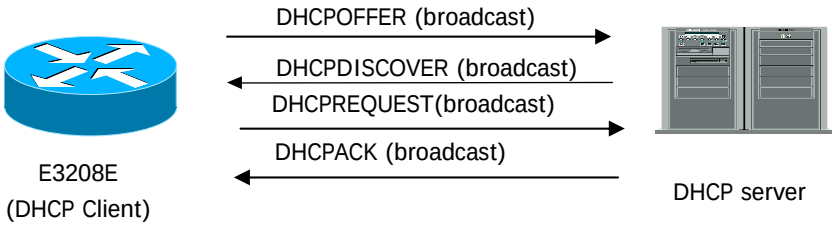
DHCP Client Function and Configuration

DHCP Client Overview

DHCP Client is the protocol that defines Internet host getting configuration parameters like IP address via DHCP or BOOTP packet from DHCP Server.

Because IP address is assigned dynamically and user does not need to configure TCP/IP, it is easy to manage.

The following the procedure shows that E3208E as DHCP Client requests IP Address from DHCP Client.



<Figure 15> IP Address Requst from DHCP Client

The following procedure shows how DHCP client to request IP Address from DHCP server..

1. A DHCP client sends the broadcast message DHCPDISCOVER to get an IP address.
2. DHCP Server broadcasts DHCPOFFER having IP address and basic router information for Client.
3. DHCP Client broadcasts DHCPREQUEST message to use offered IP address.
4. DHCP make sure that IP address is assigned by broadcasting DHCPACK message.

DHCP Client Configuration

If you use E3208E by DHCP Client, E208E can use IP address talking from DHCP Server dynamically.

E3208 DHCP ClinetFunction Activation

By default, DHCP Client Function is disabled. You can enable DHCP Client Function with the following command on VLAN interface Configuration mode.

<Table 63> DHCP Client Function Enabling Command

Command	Description
ip address dhcp	Enables DHCP Client Function on E3208E If you want to disable DHCP Client Function, use ‘no’ in front of the command.

The following example shows how to enable DHCP Client Function.

```
Switch# configure terminal
Switch(config)# interface vlan100
```

```
Switch(config-if-vlan100)# ip address dhcp
Switch(config-if-vlan100)# end
Switch# show ip dhcp client
DHCP Client Service     : Enable

DHCP Client is configured on:
        vlan100
Switch#
```

Caution You can not configure static IP addres on VLAN interface assigned IP address and ip default-gateway on configure node at the same time.

DHCP Client Monitoring and Management

<Table 64> DHCP Client Monitoring and Management

Command	Description
show ip dhcp client	Shows DHCP Client Configuration.
show ip dhcp client binding-address	Shows DHCP Client binding information.

```
Switch# show ip dhcp client
DHCP Client Service     : Enable

DHCP Client is configured on:
        vlan100
Switch#
Switch# show ip dhcp client binding-address
  Interface       IP Address      Lease expiration        Gateway
  ----------      ----------      ----------------        -------
  vlan100         10.1.21.4       86394 (sec)             10.1.21.254
Switch#
```

Notice If you enable DHCP Client Function and assign new IP address, it can check ‘show ip interfaces’ or ‘show ip interface brief’ commands.

```
Switch# show ip interfaces
vlan1 is link down.
ip address: 100.1.1.1/24 broadcast address: 100.1.1.255

vlan100 is link up.
ip address: 10.1.21.4/24 broadcast address: 10.1.21.255 (dhcp)

Switch#
Switch# show ip interfaces brief
```

```
 IFNAME     LPROTO   1st IP-ADDRESS        2nd IP-ADDRESS
-------------------------------------------------------------
 vlan1      down      100.1.1.1/24
 vlan100    up        10.1.21.4/24 (dhcp)
-------------------------------------------------------------
Switch#
```

Notice You can check gateway information with ‘show ip default-gateway’ by enabling DHCP Client Function.

```
Switch# show ip default-gateway

default gateway information
   gateway: 10.1.21.254, vlan100, active(dhcp)

   gateway static mac : not set ( auto )
Switch#
```

Notice If link of VLAN interface being enabled dhcp client function is down, IP address is released and it disappears. If link is up again, it sends DHCPDISCOVER and does Rebinding. Then you can check with ‘show command’

Chapter 6. IGMP Snooping

This chapter describes IGMP Snooping in the E3208E ONU.

Overview of IGMP Snooping

Typically, multicast traffic in a switch is processed with unknown MAC addresses or into broadcast frames and flooded to all ports included in the VLAN.

IGMP snooping does not forward multicast traffic to all member ports of VLAN but dynamically adds/deletes the ports to which multicast traffic will be forwarded in order to improve efficiency of network bandwidth. When IGMP snooping is enabled, the switch snoops the IGMP traffic between the host and the router to get the information on the multicast group and member ports.

If an IGMP join message for a specific multicast group is received from the host, the ports connected to the host will be added to the affected multicast forwarding table entry. On the contrary, if an IGMP leave message is received from the host, the ports connected to the host will be deleted from the table entry. The IGMP query from the multicast router is forwarded to the ports of VALN, and the ports that failed to receive the IGMP join message will be deleted.

Setting IGMP Snooping

You can globally enable/disable IGMP snooping for all VLANs.

Enable Global IGMP Snooping

You can globally enable IGMP snooping using the following command in global configuration mode.

<Table 65> Enable Global IGMP Snooping

Command	Description
ip igmp snooping	Enables IGMP snooping.
no ip igmp snooping	Disables IGMP snooping.

```
Switch # configure terminal
Switch (config)# ip igmp snooping
Switch (config)#
Switch # show ip igmp snooping
Global IGMP Snooping configuration:
  - Aging Interval                : 300 sec
  - Last Member Join Interval     : 300 sec
  - TCN Query Solicit             : DISABLED
IGMP snooping is DISABLED on ALL interface
IGMP snooping fast-leave is DISABLED on ALL interfaces
```

Enable IGMP-TRAP on an interface

While the Switch is in operation of IGMP Snooping, in order to receive IGMP packets, IGMP-TRAP should be enabled at each port interface.

To configure IGMP-TRAP the following commands are to be used in Interface configuration mode.

<Table 66> Enable IGMP-TRAP on an interface

Command	Description
igmp-trap	To enable igmp-trap at the interface.
no igmp-trap	To disable igmp-trap.

```
Switch # configure terminal
Switch (config)# interface fa1
Switch (config-if-fa1)# igmp-trap
Switch (config-if-fa1)# end
Switch # show running-configure
…
!
interface fa1
  igmp-trap
```

Enable IGMP Snooping on a VLAN

You should enable/disable IGMP snooping for an individual VLAN in the E3208E ONU.

You can set IGMP snooping for a VLAN using the following command in global configuration mode.

<Table 67> Enable IGMP Snooping on a VLAN

Command	Description
ip igmp snooping vlan *<1-4096>*	Enables IGMP snooping for a specified VLAN.
no ip igmp snooping vlan *<1-4096>*	Disables IGMP snooping for a specified VLAN.

```
Switch # configure terminal
Switch (config)# ip igmp snooping
Switch (config)# ip igmp snooping vlan 1
Switch (config)# exit
Switch # show ip igmp snooping vlan 1
Global IGMP Snooping configuration:
  - Aging Interval                : 300 sec
  - Last Member Join Interval     : 300 sec
  - TCN Query Solicit             : DISABLED
vlan1
            IGMP snooping is ENABLED on this interface
            IGMP snooping fast-leave is DISABLED on this interface
```

```
IGMP snooping mr-learn is DISABLED on this interface
Vlan Members : fa1 fa2 fa3 fa4
```

Configure IGMP Snooping Functionality

The following settings are required to configure IGMP snooping functionality.

Setting Report-Suppression

IGMP report-suppression of IGMP snooping is disabled by default and all received IGMP reports are forwarded to the multicast router. In the case IGMP report-suppression is enabled, just one IGMP report for each multicast membership group is forwarded to the multicast router by IGMP snooping.

This feature is applicable to IGMPv1 and IGMPv2 report messages only.

<Table 68> Setting Report-Suppression

Command	Description
ip igmp snooping report-suppression	Enables IGMP report-suppression.
no ip igmp snooping report-suppression	Disables IGMP report-suppression.

```
Switch # configure terminal
Switch (config)# ip igmp snooping report-suppression
Switch (config)# exit
Switch # show ip igmp snooping
Global IGMP Snooping configuration:
  - Aging Interval                : 300 sec
  - Last Member Join Interval : 10 sec
  - TCN Query Solicit             : DISABLED
  - IGMP Report Suppression     : ENABLED
Global IGMP Proxy-Reporting configuration:
  - IGMP Querier & Host           : DISABLED
  - Query Interval                : 60s
  - Query Based Port              : ENABLED

 vlan1
            IGMP snooping is ENABLED on this interface
            IGMP Proxy-Reporting is DISABLED on this interface
            IGMP snooping fast-leave is ENABLED on this interface
            IGMP snooping mr-learn is DISABLED on this interface
            Vlan Members :
                  fa1    fa2    fa3    fa4

 ------------------------------------------------------------------------
total : 1
```

Setting Fast-Leave

When the fast-leave feature of IGMP snooping is enabled, the switch immediately deletes the affected port from the forwarding table provided that an IGMPv2 leave message is received from the host.

This feature should be applied to the case where just one host is defined for each port of VLAN. If this feature is enabled where a port is included in several hosts, the hosts that have not sent an IGMPv2 leave message might fail to receive traffic of the affected multicast group during the given time. In addition, this feature is effective only if all hosts use IGMPv2 that supports the leave message.

As described below, fast-leave is applicable to each VLAN and to each port. Fast-leave defined for a VLAN is prior to that defined for a port, which is a member of VLAN.

<Table 69> Setting Fast-Leave

Command	Description
ip igmp snooping vlan *<1-4096>* **fast-leave**	Enables fast-leave for a specific VLAN.
no ip igmp snooping vlan *<1-4096>* **fast-leave**	Disables fast-leave for a specific VLAN.
ip igmp snooping vlan *<1-4096>* **fast-leave** *IFNAME*	Enables fast-leave for a specific port of VLAN.
no ip igmp snooping vlan *<1-4096>* **fast-leave** *IFNAME*	Disables fast-leave for a specific port of VLAN.

```
Switch # configure terminal
Switch (config)# ip igmp snooping vlan 1 fast-leave fa1
Switch (config)# ip igmp snooping vlan 1 fast-leave fa2
Switch(config)# exit
Switch# show ip igmp snooping vlan 1
Global IGMP Snooping configuration:
 - Aging Interval                : 300 sec
 - Last Member Join Interval : 10 sec
 - TCN Query Solicit             : DISABLED
 - IGMP Report Suppression     : ENABLED
Global IGMP Proxy-Reporting configuration:
 - IGMP Querier & Host           : DISABLED
 - Query Interval                : 60s
 - Query Based Port              : ENABLED

vlan1
        IGMP snooping is ENABLED on this interface
        IGMP Proxy-Reporting is DISABLED on this interface
        IGMP snooping fast-leave is ENABLED on this interface
        IGMP snooping mr-learn is DISABLED on this interface
        Vlan Members :
            fa1   fa2   fa3   fa4
```

total : 1

Setting Mrouter

A switch transfers all multicast traffic to the multicast router to forward all multicast traffic of a VLAN to other networks. Therefore, the ports connected to the multicast router are added to all multicast forwarding table entries as outgoing ports.

Basically, IGMP snooping is carried out on IGMP traffic only to detect the ports connected to the multicast router, but it is possible to detect the mrouter ports by manually enabling the PIM/DVMRP protocol.

The mrouter ports detected like this are registered as outgoing ports whenever a new multicast forwarding table entry is created, and the IGMP join message transferred from the host as well as the multicast traffic is forwarded to the mrouter.

You can manually set a multicast router port using the following command in global configuration mode.

<Table 70> Setting Mrouter

Command	Description
ip igmp snooping vlan *<1-4096>* **mrouter interface** *IFNAME*	Manually sets an mrouter port. IFNAME should be a member port of the VLAN.
no ip igmp snooping vlan *<1-4096>* **mrouter interface** *IFNAME*	Deletes the mrouter port. IFNAME should be a member port of the VLAN.

```
Switch # configure terminal
Switch (config)# ip igmp snooping vlan 1 mrouter interface fa1
Switch(config)# exit
Switch# show ip igmp snooping mrouter
   VLAN          MULTICAST-ROUTER-PORT
   0001          fa1

_____________________________________________________________________
total : 1
```

You can set multicast router port detection over PIM/DVMRP protocol using the following command in global configuration mode.

<Table 71> Multicast router port detection over PIM/DVMRP

Command	Description
ip igmp snooping vlan *<1-4096>* **mrouter learn pim-dvmrp**	Sets mrouter port detection by snooping the PIM/DVMRP protocol.
no ip igmp snooping vlan *<1-4096>* **mrouter learn pim-dvmrp**	Deletes mrouter port detection.

```
Switch # configure terminal
Switch (config)# ip igmp snooping vlan 1 mrouter learn pim-dvmrp
Switch(config)# exit
Switch# show ip igmp snooping vlan 1
Global IGMP Snooping configuration:
 - Aging Interval                : 300 sec
 - Last Member Join Interval : 10 sec
 - TCN Query Solicit             : DISABLED
 - IGMP Report Suppression     : ENABLED
Global IGMP Proxy-Reporting configuration:
 - IGMP Querier & Host          : DISABLED
 - Query Interval                : 60s
 - Query Based Port              : ENABLED

vlan1
        IGMP snooping is ENABLED on this interface
        IGMP Proxy-Reporting is DISABLED on this interface
        IGMP snooping fast-leave is ENABLED on this interface
        IGMP snooping mr-learn is ENABLED on this interface
        Vlan Members :
            fa1   fa2   fa3   fa4

_____________________________________________________________

total : 1
```

Setting an Aging Time

In the IGMP protocol, membership of multicast group is managed in such a way that the multicast router acting as an IGMP Querier transmits an IGMP Query message and the hosts send an IGMP join message in response to the received message. IGMP snooping adds/deletes outgoing port of the multicast forwarding table entry using these IGMP protocol messages.

In case the multicast forwarding table entry fails to be updated because no IGMP join message is received within the specified aging time, the port will be deleted from the multicast forwarding table entry of outgoing ports.

The default setting of aging time is 300 sec. You can set an aging time using the following command in global configuration mode.

<Table 72> Setting an Aging Time

Command	Description
ip igmp snooping aging *<30-3600>*	Sets an aging time (default : 300 sec)
no ip igmp snooping aging	Changes the specified aging time to the default aging time.

Switch **# configure terminal**
Switch (config)**# ip igmp snooping aging 250**
Switch(config)**# exit**
Switch**# show ip igmp snooping**
Global IGMP Snooping configuration:
- Aging Interval : 250 sec
- Last Member Join Interval : 10 sec
- TCN Query Solicit : DISABLED
- IGMP Report Suppression : ENABLED
Global IGMP Proxy-Reporting configuration:
- IGMP Querier & Host : DISABLED
- Query Interval : 60s
- Query Based Port : ENABLED

vlan1
IGMP snooping is ENABLED on this interface
IGMP Proxy-Reporting is DISABLED on this interface
IGMP snooping fast-leave is ENABLED on this interface
IGMP snooping mr-learn is ENABLED on this interface
Vlan Members :
fa1 fa2 fa3 fa4

---

total : 1

Setting Last-Member-Join-Interval

If an IGMP leave message is received where the fast-leave feature of IGMP snooping is not enabled for a VLAN, the affected port would be deleted from the multicast forwarding table entry not immediately, but after the specified aging time.

You can set a last-member-join-interval in order to complete multicast membership management within the specified aging time.

Unless otherwise specified, last-member-join-interval will be automatically set equal to the aging time and the affected port will be deleted according to the aging time of IGMP snooping. This feature is effective only where the fast-leave feature is not enabled in VLAN.

You can set a last-member-join-interval using the following command in global configuration mode.

<Table 73> Setting Last-Member-Join-Interval

Command	Description
ip igmp snooping last-member-join-interval *<5-300>*	Sets last-member-join-interval (default : 300 sec)
no ip igmp snooping last-member-join-interval	Deletes last-member-join-interval.

```
Switch # configure terminal
Switch (config)# ip igmp snooping last-member-join-interval 5
Switch(config)# exit
Switch# show ip igmp snooping
Global IGMP Snooping configuration:
 - Aging Interval                : 250 sec
 - Last Member Join Interval : 5 sec
 - TCN Query Solicit             : DISABLED
 - IGMP Report Suppression     : ENABLED
Global IGMP Proxy-Reporting configuration:
 - IGMP Querier & Host          : DISABLED
 - Query Interval                : 60s
 - Query Based Port              : ENABLED

vlan1
        IGMP snooping is ENABLED on this interface
        IGMP Proxy-Reporting is DISABLED on this interface
        IGMP snooping fast-leave is ENABLED on this interface
        IGMP snooping mr-learn is ENABLED on this interface
        Vlan Members :
            fa1   fa2   fa3   fa4

_____________________________________________________________

total : 1
```

Setting TCN (Topology Change Notification)

When receiving a spanning-tree Topology Change Notification (TCN), IGMP snooping clears the multicast forwarding table entry by default. Then, a new multicast forwarding table entry is created by the IGMP Query of multicast router.

Where tcn provided by the switch is enabled, the IGMP Leave message for Group “0.0.0.0” is transmitted to the multicast router when spanning-tree Topology Change Notification (TCN) is received. Receiving the IGMP Leave message for Group “0.0.0.0”, the multicast router sends an IGMP Query message and then a new multicast forwarding table entry is created for the changed network topology.

You can set tcn for all equipment configured in a spanning-tree, using the following command in global configuration mode.

<Table 74> Setting TCN (Topology Change Notification)

Command	Description
ip igmp snooping tcn query-solicit	Sets TCN Query Solicit.
no ip igmp snooping tcn query-solicit	Deletes TCN Query Solicit.

```
Switch # configure terminal
Switch (config)# ip igmp snooping tcn query-solicit
Switch(config)# exit
Switch# show ip igmp snooping
Global IGMP Snooping configuration:
  - Aging Interval                : 250 sec
  - Last Member Join Interval : 5 sec
  - TCN Query Solicit             : ENABLED
  - IGMP Report Suppression     : ENABLED
Global IGMP Proxy-Reporting configuration:
  - IGMP Querier & Host           : DISABLED
  - Query Interval                : 60s
  - Query Based Port              : ENABLED

vlan1
        IGMP snooping is ENABLED on this interface
        IGMP Proxy-Reporting is DISABLED on this interface
        IGMP snooping fast-leave is ENABLED on this interface
        IGMP snooping mr-learn is ENABLED on this interface
        Vlan Members :
            fa1   fa2   fa3   fa4

_____________________________________________________________________
total : 1
```

Setting IGMP Filtering

IGMP filtering filters user's IGMP packets of a switch port. This function enables the network manager to manage distribution of multicast service by providing service according to the service plan or request under a specific network environment.

Each switch port carries an IGMP profile for filtering, which contains more than one multicast group and filtering information.

For setting IGMP filtering, you should first create an IGMP profile using the following commands in global configuration mode.

<Table 75> Setting IGMP Filtering

Command	Description
ip igmp snooping profile *<1-99>* permit *<multicast address>* range *<multicast address>*	Sets an IGMP profile that allows IGMP filtering.
ip igmp snooping profile *<1-99>* deny *{<multicast address>* | *<all>}* range *<multicast address>*	Sets an IGMP profile that denies IGMP filtering.
no ip igmp snooping profile *<1-99>*	Deletes the created IGMP profile.

```
Switch # configure terminal
Switch (config)# ip igmp snooping profile 1 deny 224.1.0.0/16
Switch (config)# ip igmp snooping profile 2 deny 224.1.0.0/16 range 224.2.0.0/16
Switch (config)# ip igmp snooping profile 3 permit 224.0.0.0/8
Switch(config)# exit
Switch# show ip igmp snooping profile
IGMP Profile 1
            deny     range : 224.1.0.0/16 224.1.0.0/16
IGMP Profile 2
            deny     range : 224.1.0.0/16 224.2.0.0/16
IGMP Profile 3
          permit     range : 224.0.0.0/8 224.0.0.0/8
```

After creating an IGMP profile, you can apply IGMP filtering using the following command in global configuration mode.

<Table 76> IGMP filtering

Command	Description
ip igmp snoop-filter *<1-99>*	Applies IGMP filtering to the switch port.
no ip igmp snoop-filter *<1-99>*	Deletes IGMP filtering.

```
Switch # configure terminal
Switch (config)# interface fa1
Switch (config-if-fa1)# ip igmp snoop-filter 1
Switch (config-if-fa1)# end
Switch # show running-configure
…
!
interface fa1
    ip igmp snoop-filter 1
```

Setting IGMP Max-Group-Count

You can restrict the number of multicast groups to provide multicast service by subscribers.

To set a number of multicast groups, run the following command in global configuration mode.

<Table 77> Setting IGMP Max-Group-Count

Command	Description
ip igmp snooping max-group-count *IFANME* <*count*>	Applies a max-group-count for a switch port.
no ip igmp snooping max-group-count *IFANME*	Clears max-group-count.

```
Switch # configure terminal
Switch (config)# ip igmp snooping max-group-count fa1 10
Switch # show running-configure
…
ip igmp snooping
ip igmp snooping max-group-count fa1 10
…
Switch #
```

Setting IGMP Max-Reporter-Count

You can set the number of hosts to provide multicast service by subscribers for each VLAN interface.

To set a number of hosts, run the following command in global configuration mode.

<Table 78> Setting IGMP Max-Reporter-Count

Command	Description
ip igmp snooping max-reporter-count vlan *<vlan-id> <count>*	Applies max-reporter-count for a VLAN interface.
no ip igmp snooping max-reporter-count vlan *<vlan-id>*	Clears max- reporter -count.

```
Switch # configure terminal
Switch (config)# ip igmp snooping max-reporter-count vlan 1 10
Switch #
Switch # show running-configure
…
ip igmp snooping
ip igmp snooping max-reporter-count vlan 1 10
…
Switch #
```

<Table 79> Setting IGMP Max-Reporter-Count by Port

Command	Description
ip igmp snooping max-reporter-count port *IFNAME <count>*	Apply max-reporter-count to a Port.
no ip igmp snooping max-reporter-count port *IFNAME*	Remote the max- reporter –count from a PORT.

```
Switch # configure terminal
Switch (config)# ip igmp snooping max-reporter-count port fa1 10
Switch (config)# exit
Switch # show running-configure
…
ip igmp snooping
ip igmp snooping max-reporter-count port fa1 10
```

Configuring drop-igmp-ttl-over

In order to provide multicast service, you can limit the TTL suppressing abnormal packet. To put the limitation on the number of packets which exceed the allowed TTL, the following command is to be used in global configuration mode.

<Table 80> Configuring drop-igmp-ttl-over

Command	Description
ip igmp snooping drop-igmp-ttl-over *<1-255>*	Apply drop-igmp-ttl-over.
no ip igmp snooping drop-igmp-ttl-over	Remove the drop-igmp-ttl-over

```
Switch # configure terminal
Switch(config)# ip igmp snooping drop-igmp-ttl-over 1
Switch(config)# exit
Switch # show running-configure
…
ip igmp snooping
ip igmp snooping drop-igmp-ttl-over 1
```

Configuring snooping ignore-mpkt-upstream-forward

When multicast traffic is generated in a port which is not mrouter port, the multicast traffic shall be transferred to mrouter port. The transfer of multicast traffic toward mrouter port can be limited for some reasons of network management.

In order to limit the transfer of the multicast traffic, the following command is to be used in global configuration mode.

<Table 81> Configuring snooping ignore-mpkt-upstream-forward

Command	Description
ip igmp snooping snooping ignore-mpkt-upstream-forward	Apply snooping ignore-mpkt-upstream-forward.
no ip igmp snooping snooping ignore-mpkt-upstream-forward	Remove snooping ignore-mpkt-upstream-forward.

```
Switch # configure terminal
Switch(config)# ip igmp snooping snooping ignore-mpkt-upstream-forward
Switch(config)# exit
Switch # show running-configure
…
ip igmp snooping
ip igmp snooping snooping ignore-mpkt-upstream-forward
```

Overview of IGMP Proxy-Reporting

While the throughput of network equipment is confined, membership requests of IGMP to be processed simultaneously are increasing due to increase in various multicast services and multi-accessed network environment. IGMP membership requests of these IGMP hosts might cause overload on the equipment located in a higher network and incur multicast service delay or service down.

For this reason, the DSL Forum provides a document defining the IGMP proxy-reporting, and the switch supports the IGMP proxy-reporting defined by the DSL Forum.

IGMP proxy-reporting provides all features defined in IGMP. IGMP host sends an IGMP report when IGMP query is received from the multicast router. IGMP general query is periodically transmitted for subscriber's IGMP membership management and IGMP Specific Query is issued when IGMP Leave is received.

For IGMP proxy-reporting, the IP source address of the IGMP Report and IGMP Query messages is used as the IP address of a specified VLAN, provided that the VLAN interface with IGMP proxy-reporting enabled carries an IP Address. The latest IGMP Host Address used for IGMP membership management is used in the case where IP Address of VLAN is not defined.

Setting IGMP Proxy-Reporting

You can globally enable/disable IGMP proxy-reporting and apply IGMP proxy-reporting by VLAN Interface.

Enable IGMP Proxy-Reporting

You can globally enable IGMP proxy-reporting using the following command in global configuration mode.

<Table 82> Enable IGMP Proxy-Reporting

Command	Description
ip igmp snooping proxy-reporting	Enables IGMP proxy-reporting.
no ip igmp snooping proxy-reporting	Disables IGMP proxy-reporting.

```
Switch # configure terminal
Switch (config)# ip igmp snooping proxy-reporting
Switch (config)# exit
Switch # show ip igmp snooping
Global IGMP Snooping configuration:
  - Aging Interval                : 250 sec
  - Last Member Join Interval : 5 sec
  - TCN Query Solicit              : ENABLED
  - IGMP Report Suppression     : ENABLED
Global IGMP Proxy-Reporting configuration:
  - IGMP Querier & Host          : ENABLED
  - Query Interval                : 60s
  - Query Based Port              : ENABLED

vlan1
```

```
        IGMP snooping is ENABLED on this interface
        IGMP Proxy-Reporting is DISABLED on this interface
        IGMP snooping fast-leave is ENABLED on this interface
        IGMP snooping mr-learn is ENABLED on this interface
        Vlan Members :
              fa1   fa2   fa3   fa4   gi1   gi2
_____________________________________________________________
total : 1
```

Enable IGMP Proxy-Reporting on a VLAN

The switch allows you to enable/disable IGMP proxy-reporting for an individual VLAN.

You can enable/disable IGMP proxy-reporting for a VLAN using the following command in global configuration mode.

A VLAN with IGMP proxy-reporting enabled does not support IGMP packet forwarding through IGMP snooping.

<Table 83> Enable IGMP Proxy-Reporting on a VLAN

Command	Description
ip igmp snooping proxy-reporting vlan *<1-4096>*	Enables IGMP proxy-reporting for a specific VLAN.
no ip igmp snooping proxy-reporting vlan *<1-4096>*	Disables IGMP proxy-reporting for a specific VLAN.

```
Switch # configure terminal
Switch (config)# ip igmp snooping proxy-reporting vlan 1
Switch (config)#
Switch # show ip igmp snooping vlan 1
Global IGMP Snooping configuration:
  - Aging Interval                : 250 sec
  - Last Member Join Interval : 5 sec
  - TCN Query Solicit              : ENABLED
  - IGMP Report Suppression     : ENABLED
Global IGMP Proxy-Reporting configuration:
  - IGMP Querier & Host          : ENABLED
  - Query Interval                 : 60s
  - Query Based Port               : ENABLED

vlan1
        IGMP snooping is ENABLED on this interface
        IGMP Proxy-Reporting is ENABLED on this interface
        IGMP snooping fast-leave is ENABLED on this interface
        IGMP snooping mr-learn is ENABLED on this interface
        Vlan Members :
              fa1   fa2   fa3   fa4
_____________________________________________________________
```

total : 1

Configure IGMP Proxy-Reporting Functionality

The following settings are required to configure the IGMP proxy-reporting functionality.

Setting IGMP Static-Group

IGMP proxy-reporting supports a static-group feature to minimize the join delay time required to receive traffic of a specific multicast group.

Static-group is provided to continually receive multicast traffic by periodically transmitting an IGMP report to multicast-router ports.

It is essential to apply this feature along with IGMP snooping, using the following command in global configuration mode.

<Table 84> Setting IGMP Static-Group

Command	Description
ip igmp snooping proxy-reporting vlan *<1-4096>* **static-group** *A.B.C.D*	Sets an IGMP Static-Group through IGMP proxy-reporting for a specific VLAN.
no ip igmp snooping proxy-reporting vlan *<1-4096>* **static-group** *A.B.C.D*	Clears the defined IGMP Static-Group.

```
Switch # configure terminal
Switch (config)# ip igmp snooping proxy-reporting vlan 1 static-group
224.1.1.1
Switch (config)# exit
Switch # show running-configure
!
ip igmp snooping proxy-reporting
ip igmp snooping proxy-reporting vlan 1
ip igmp snooping proxy-reporting vlan 1 static-group 224.1.1.1
!
```

Display System and Network Statistics

<Table 85> Commands for Monitoring IGMP Snooping

Command	Description
show ip igmp snooping	Shows the IGMP snooping status of all VLANs.
show ip igmp snooping vlan *<1-4096>*	Shows the IGMP snooping status of a specific VLAN
show ip igmp snooping mrouter	Shows the information on all mrouters.
show ip igmp snooping mac-entry	Shows the information on a specific multicast forwarding table entry.
show ip igmp snooping mac-entry vlan *<1-4096>*	Shows the information on the specified multicast forwarding table entry for a specific VLAN.

show ip igmp snooping querier	Shows the information on all IFMP Queriers of multicast router.
show ip igmp snooping querier vlan *<1-4096>*	Shows the information on all IFMP Queriers of the multicast routers for a specific VLAN.
show ip igmp snooping reporter	Shows the information on all IGMP reporters.
show ip igmp snooping reporter vlan *<1-4096>*	Shows the information on all IGMP reporters for a specific VLAN.
show ip igmp snooping profile	Shows the information on the specified IGMP profile.
show ip igmp snooping statistics	Shows statistics information about Igmp packet.

The following example shows how to set igmp snooping.

```
interface fa1
igmp-trap
ip igmp snoop-filter 1
!
flow-rule mcast_deny classify ip any 224.0.0.0/4
flow-rule mcast_deny match drop
!
policy-map iptv_filter flow-rule mcast_deny
!
service-policy downonly iptv_filter
!
ip igmp snooping proxy-reporting
ip igmp snooping proxy-reporting vlan 1
!
ip igmp snooping
ip igmp snooping vlan 1
ip igmp snooping profile 1 deny igmp_query
ip igmp snooping profile 1 permit 224.1.1.1/24 range 224.3.1.1/24
ip igmp snooping profile 1 permit 224.5.1.1/24 range 224.6.1.1/24
ip igmp snooping profile 1 deny all
```

Chapter 7. STP and SLD

This chapter describes how to define Spanning Tree Protocol (STP) and Rapid Spanning Tree Protocol (RSTP) and to configure the Self-Loop Detection (SLD) features.

This chapter is organized into the following sections:

- Understanding Spanning-Tree Features
- Understanding RSTP
- Configuring Spanning-Tree Features
- Displaying the Spanning-Tree Status
- Self-loop Detection

Understanding Spanning-Tree Features

This section describes the following STP features:

- STP Overview
- Bridge Protocol Data Units
- Election of the Root Switch
- Bridge ID, Switch Priority, and Extended System ID
- Spanning-Tree Timers
- Creating the Spanning-Tree Topology
- Spanning-Tree Interface States

STP Overview

STP is a Layer 2 link management protocol which prevents self-loops and provides duplicated paths in a network. To let a Layer 2 Ethernet network operate normally, only one active path should be established between two random terminals. As spanning-tree operation is transparent to end stations, it is impossible to determine whether end stations are connected to a single LAN or to a switched LAN composed of several segments.

To configure a fault-free network, there should be no self-loops between nodes of the network. The spanning-tree algorithm calculates an optimized loop-free path over the switched Layer 2 network. The switch periodically sends and receives spanning-tree frames called bridge protocol data units (BPDUs). It does not forward these frames but processes them to create a loop-free path.

A loop is formed where there are several active paths between two end stations. If a loop exists in a network, the affected end stations will receive replicated frames. In such a case, MAC address of a certain end station will be registered for several Layer 2 interfaces in the switch. This situation makes the network unstable.

Spanning tree defines loop-free path from root switch to every switch in a Layer 2 network. Spanning tree makes replicated data paths enter standby (blocked) status. If faults are detected in a network containing replicated path, the spanning-tree algorithm recalculates the spanning-tree topology to enable the standby path.

Where two interfaces of a switch compose a part of loop, the spanning-tree port priority and path cost settings determine forwarding state and blocking state of these interfaces. ‘port priority’ shows the location of an interface in the network, and ‘path cost’ indicates the link speed.

Bridge Protocol Data Units

An active spanning-tree topology is determined by the following elements:

- Unique BridgeID associated with each VLAN(switch priority and MAC address)
- Spanning-tree path cost to the root switch
- Port identifier assigned to each Layer 2 interface(port priority and port number)

When powered on, the switch acts as a root switch. Each switch sends the configuration BPDUs to all of its own ports. Switches exchange BPDUs each other to calculate a spanning-tree topology. Each configuration BPDU contains the following information:

- BridgeID of root switch
- Spanning-tree path cost to the root
- BridgeID of the source switch
- Message age
- Interface identifier of the source switch

- Hello, forward-delay and max-age protocol timer values

  When the switch receives a BPDU carrying information superior to that of the current port (lower BridgeID, lower path cost, etc.), it stores the information in the port that has received the BPDU. If the port is a root port, the switch updates the message and forwards it to the designated LAN.

  The switch drops a BPDU containing information inferior to that of the current port. When the switch receives an inferior message from the designated LAN, it transfers the BPDU updated with the information stored in the port to LAN. In this way, inferior information is dropped and superior information is forwarded to the network.

  The following describes the results of BPDU exchange:

- A certain switch in the network is selected as a root switch.
- A root port is selected in each switch except for the root switch. This port provides an optimal path (the lowest path cost) for the switch to transmit packets to the root switch.
- Each switch calculates the shortest distant to the root switch based on the path cost.
- A designated switch is determined for each LAN. The designated switch provides the lowest path cost to transfer packets from LAN to the root switch. The port of the designated switch connected to LAN is called designated port.
- The interfaces to be included in the spanning-tree are determined. The root port and the designated port are forwarding state.
- All interfaces not included in the spanning-tree are blocked.

Election of Root Switch

Every switch participating in the spanning tree of Layer 2 network collects information on other switches by exchanging BPDUs. The following events occur through message exchange:

- Electing a unique root switch for each spanning-tree instance
- Electing a designated switch for every switched LAN segment
- Removing self-loops of switched network by blocking Layer 2 interfaces connected through replicated links

A switch with the highest priority (with the smallest value) in each VLAN is determined as the root switch. In case all switches are set to the default priority (32768), the switch with the smallest MAC address in the VLAN will be a root switch. Switch priority is carried by the most significant bit of BridgeID.

You can change the possibility of a switch to be a root switch by changing its switch priority. A larger switch priority has a lower probability to be a root switch.

Root switch is at the logical center of a spanning-tree topology in a switched network. Those paths unnecessary for reaching the root switch in a switched network go into blocking state in the spanning-tree.

A BPDU contains the information such as source switch and port, MAC address, switch priority, port priority and path cost. Spanning tree determines root switch, root port and designated port from the information.

Bridge ID, Switch Priority, and Extended System ID

In accordance with the IEEE 802.1D standard, each switch is assigned a unique bridge identifier (BridgeID) to select a root switch. Since each VLAN is logically regarded as an individual bridge, a unique BridgeID is assigned for each VLAN. A switch carries BridgeID of 8 bytes; the most significant 2 bytes are used for switch priority and the rest 6 bytes indicate MAC address of the switch.

The E3208E ONU supports 802.1T spanning-tree extensions. As seen in the table, the two bytes used for switch priority are reallocated to 4-bit priority and 12-bit extended system ID identical to the VLAN ID.

<Table 86> Switch Priority Value and Extended System ID

Switch Priority Value				Extended System ID (Set Equal to the VLAN ID)											
Bit16	**Bit15**	**Bit14**	**Bit13**	**Bit12**	**Bit11**	**Bit10**	**Bit9**	**Bit8**	**Bit7**	**Bit6**	**Bit5**	**Bit 4**	**Bit3**	**Bit2**	**Bit1**
32768	16384	8192	4096	2048	1024	512	256	128	64	32	16	8	4	2	1

Spanning tree creates BridgeID with extended system ID, switch priority and MAC address.

Spanning-Tree Timers

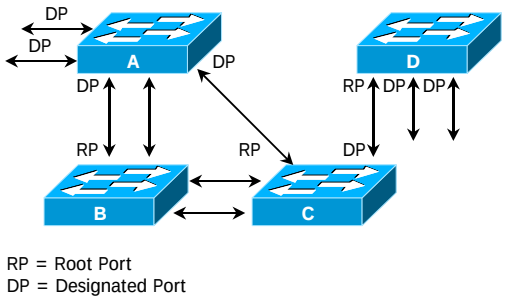
The table below describes the timers affecting performance of a spanning-tree.

<Table 87> Spanning-Tree Timers

Variable	Description
Hello timer	Determines an interval for a switch to send the hello message to other switches.
Forward-delay timer	Determines a period that an interface will hold listening and learning states respectively prior to entering forwarding state.
Maximum-age timer	Determines a period to keep the protocol information received from an interface

Creating the Spanning-Tree Topology

Assuming that switch priority of all switches in the figure is default (32768) and Switch A carries the lowest MAC address, Switch A becomes a root switch. However, Switch A is not an ideal root switch on account of the number of forwarding interfaces or link-type. It is possible to recalculate the spanning-tree topology to let an ideal switch elected as a root switch by increasing its switch priority (using a smaller value).



<Figure 16> Spanning-Tree Topology

When a spanning-tree topology is calculated based on the default settings, the path between a source terminal and a destination terminal would not be an ideal one. For instance, a high-speed link connected to an interface with a port number higher than that of the root port may result in changing the root port of the switch. The goal is to elect the fastest link as a root port.

For example, assume that a port of Switch B is a gigabit Ethernet link and another port (10/100 link) of Switch B is currently a root port. It is more efficient to transfer network traffic

through the gigabit Ethernet link. It is possible to elect the gigabit Ethernet interface as a new root port by changing the port priority of the gigabit Ethernet interface to a priority (lower value) higher than the root port.

Spanning-Tree Interface States

Propagation delay occurs when protocol information is transferred through a switched LAN, resulting in changes in switched LAN configuration in a different place at a different time. A transient data loop may be formed if a Layer 2 interface not participating in the spanning-tree immediately goes into forwarding state. Therefore, prior to forwarding the frames, the switch should wait for new configuration information transferred through the switched LAN.

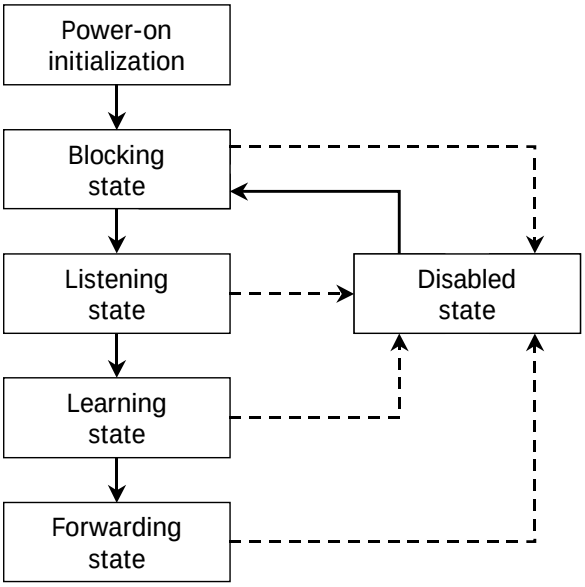
A Layer 2 interface of the switch with spanning tree enabled is one of the following states:

- Blocking – The interface does not forward any frames.
- Listening – The state succeeding the blocking state when the interface decides to forward frames.
- Learning – The interface is ready to forward frames. MAC learning is carried out in this state.
- Forwarding – The interface forwards frames.
- Disabled – The interface does not participate in the spanning tree because the port is shutdown state, or no link is available for the port, or there is no spanning-tree instance under execution.

An interface can change its state as follows:

- From initial state to blocking state
- From blocking state to listening or disabled state
- From listening state to learning or disabled state
- From learning state to forwarding or disabled state
- From forwarding state to disabled state

The figure below illustrates state transition of an interface.



<Figure 17> Spanning-Tree Interface States

When STP is enabled, all interfaces of the switch are in blocking state and then go into listening and learning state for a while. In a stabilized spanning tree, each interface is in forwarding state or blocking state.

If the spanning-tree algorithm decides to set a Layer 2 interface to forwarding state, the following process occurs:

1. Receiving the protocol information to set the interface to forwarding state, the interface goes into listening state.
2. Upon forward-delay time out, the spanning tree lets the interface go into learning state and sets the forward-delay timer again.
3. In learning state, the interface blocks forwarding while learning MAC address of the end station.
4. When the forward-delay timer expires, the spanning tree lets the interface enter forwarding state in which both learning and forwarding are permitted.

Blocking State	A Layer 2 interface in blocking state does not forward frames. The switch transfers BPDUs to each interface after initialization. The switch acts as a root switch until it exchanges BPDUs with other switches. One switch of the network is elected as root switch through BPDU exchange. If only one switch is included in the network, BPDU exchange between switches does not occur and the interface goes into listening state after forward-delay timer out. The interface is always set to blocking state after switch initialization. An interface acts as following in blocking state: • Drops the frames received through the port • Drops the frames switched from other interfaces • Does not perform address learning • Receives BPDUs
Listening State	Listening state comes after the blocking state. If an interface decides to forward the frames, it goes into listening state. An interface acts as following in listening state: • Drops the frames received through the port • Drops the frames switched from other interfaces • Does not perform address learning • Receives BPDUs
Learning State	In learning state, a Layer 2 interface is ready to forward frames. The interface goes from listening state to learning state. In learning state, an interface acts as follows: • Drops the frames received through the port • Drops the frames switched from other interfaces • Performs address learning • Receives BPDUs
Forwarding State	In forwarding state, a Layer 2 interface forwards frames. The interface goes from learning state to forwarding state. In forwarding state, an interface acts as follows: • Forwards the frames received through the port • Forwards the frames switched from other interfaces • Performs address learning • Receives BPDUs
Disable State	In disabled state, a Layer 2 interface does not participate in frame

	forwarding or spanning tree. A disabled interface acts as follows: • Drops the frames received through the port • Drops the frames switched from other interfaces • Does not perform address learning • Does not receive BPDUs

Understanding RSTP

RSTP provides fast recovery of spanning tree for point-to-point links. Spanning tree reconfiguration is accomplished within 1 sec (in contrast to maximum 50 sec required for default setting of 802.1D spanning tree). This feature is efficient for a network which transmits traffic sensitive to delay such as voice and image.

This chapter gives an understanding of RSTP:

- RSTP Overview
- Port Roles and the Active Topology
- Rapid Convergence
- Bridge Protocol Data Unit Format and Processing

RSTP Overview

RSTP provides fast link recovery (within 1 sec) from switch, switch port or LAN failure. The port elected as a new root port can immediately transit to forwarding state. The designated port determined by explicit acknowledgement between switches can also transit to forwarding state.

Port Roles and the Active Topology

RSTP provides fast recovery of spanning tree by assigning port roles to determine an active topology. Like STP, RSTP selects a switch with the highest switch priority (the smallest priority value) as the root switch. RSTP assigns port role to each port as follows:

- Root port – Provides an optimal path(the lowest cost) for a switch to forward packets to the root switch.
- Designated port – Connected to the designated switch to provide the lowest cost to forward packets from LAN to the root switch. The port of the designated switch connected to LAN is called designated port.
- Alternate port – Provides an alternative path to the root switch provided by the current root port.
- Backup port – Acts as a backup port of the path provided by the designated port toward the leaves of the spanning tree. Backup port is available when two ports are connected by loop-back through point-to-point link or when the switch provides more than two links for shared LAN segments.
- Disabled port – Plays no actions on operation of the spanning tree.

A root port or a designated port is included in the active topology. An alternate or a backup port is excluded from the active topology.

In a stable topology where the entire network carries out consistent port roles, RSTP ensures immediate transition of the root port and the designated port to forwarding state. On the contrary, all alternate ports and backup ports are in discarding state(equal to the blocking state of 802.1D). Port state controls the forwarding and learning processes. The table below provides a comparison between 802.1D and RSTP port states.

<Table 88> Port State Comparison

Operational Status	STP Port State	RSTP Port State	Is Port Included in the Active Topology?
Enabled	Blocking	Discarding	No
Enabled	Listening	Discarding	No
Enabled	Learning	Learning	Yes
Enabled	Forwarding	Forwarding	Yes
Disabled	Disabled	Discarding	No

For consistency with STP implementation, this document uses *blocking* state instead of *discarding* state. The designated port is initiated in listening state.

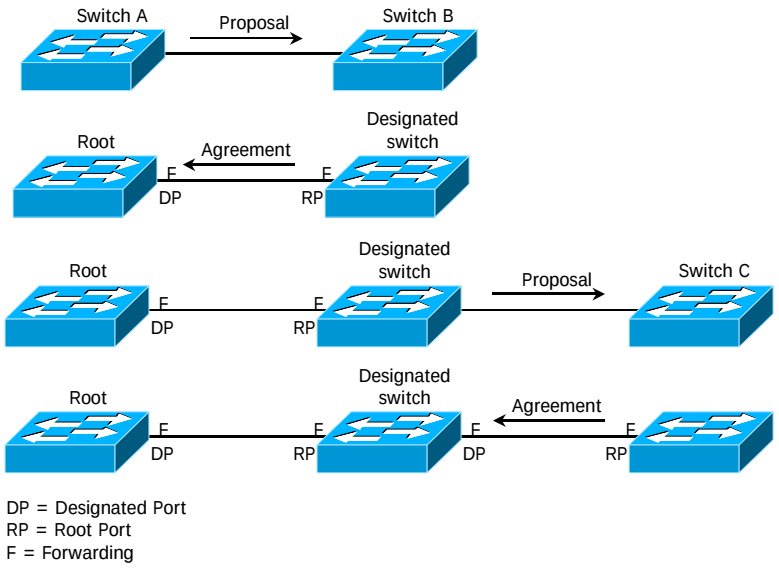
Rapid Convergence

RSTP provides fast link recovery from switch, port or LAN failure as described below. It also provides fast recovery of edge ports, root ports and point-to-point links:

- Edge ports –Edge ports defined by the RSTP switch immediately transit to the forwarding state. Edge port corresponds to a port for which PortFast is defined in STP and should be defined only for a port connected to a single end station.
- Root ports – When RSTP selects a new root port, the old root port goes into block state and the new root port immediately transits to forwarding state.
- Point-to-point links – When a port is connected to another port through point-to-point link, the local port becomes a designated port and negotiates fast transition to remove loops by exchanging proposal-agreement with other ports.
- In the figure below, Switch A is connected to Switch B through point-to-point link and all ports are in blocking state. Assume that the priority value of Switch A is smaller than that of Switch

B. Switch A transmits a proposal message (BPDU with proposal flag enabled) to Switch B and proposes itself as a designated switch.

- Receiving the proposal message, Switch B selects the port that has received the proposal message as a new root port, sets all non-edge ports to blocking state, and sends an agreement message (BPDU with agreement flag enabled) through the new root port.
- Receiving the agreement message of Switch B, Switch A changes the designated port to forwarding state. No loop is formed in the network because Switch B has blocked all non-edge ports and Switch A is connected to Switch B through point-to-point link.
- A similar negotiation message is exchanged when Switch C is connected to Switch B. Switch C selects a port connected to Switch B as a root port, and the two ports of the two switches transit to forwarding state. In the process of negotiation, more than one switch participates in the active topology. In the network recovery, such a proposal-agreement negotiation proceeds toward leaves of the spanning tree.
- A switch determines link-type with the duplex port mode: a full-duplex port is regarded as a point-to-point link and a half-duplex port is regarded as a shared link. You can change the default settings determined by duplex mode using the interface configuration command and the spanning-tree link-type command.



<Figure 18> Proposal and Agreement Handshaking for Rapid Convergence

Bridge Protocol Data Unit Format and Processing

Except that the value of protocol version field is set to 2, the format of RSTP BPDU is the same as that of IEEE 802.1D BPDU. The length field of the new 1 byte version 1 is set to 0, indicating that the information on the version 1 protocol is not included. The table below describes the RSTP flag fields.

<Table 89> RSTP BPDU Flags

Bit	Function
0	Topology change (TC)
1	Proposal
2-3:	Port role:
00	Unknown
01	Alternate port
10	Root port
11	Designated port

4	Learning
5	Forwarding
6	Agreement
7	Topology change acknowledgement (TCA)

A switch that wants to propose itself as a designated switch of LAN sends RSTP BPDU with the proposal flag enabled. The port role of a proposal message is always set to designated port.

A switch that agrees to the proposal of other switches sends RSTP BPDU with the agreement flag enabled. The port role of an agreement message is always set to root port.

RSTP does not use a separate topology change notification (TCN) BPDU. To notify topology change, it uses the topology change (TC) flag of RSTP BPDU flag. However, it creates and processes TCN BPDUs for interface with 802.1D switch.

The learning and forwarding flags are set depending on the status the transmitting port.

Configuring Spanning-Tree Features

This section describes how to configure spanning-tree features.

Default STP Configuration:

The table below shows the default settings for STP.

<Table 90> Default STP Configuration

Feature	Default Setting
Enable state	Disabled.
Spanning-tree mode	STP
System priority	32768.
Spanning-tree VLAN port priority (configurable on a per-VLAN basis)	128.
Spanning-tree VLAN port cost (configurable on a per-VLAN basis)	1000 Mbps: 4. 100 Mbps: 19. 10 Mbps: 100.
Hello time	2 sec.
Forward-delay time	15 sec.
Maximum-aging time	20 sec.

STP Configuration Guidelines

The E3208E ONU supports IEEE 802.1w RSTP. As 802.1D STP is internally included in 802.1w, the E3208E ONU provides compatibility with 802.1D.

Enabling STP

STP is disabled in default. If there is any possibility that a loop will be included in the network, it is essential to enable STP.

To enable STP for each VLAN, go through the following steps starting in privileged EXEC mode:

<Table 91> Enabling STP

		Command	Purpose
Step1		**configure terminal**	Enters global configuration mode.
Step2		**spanning-tree vlan** *vlan-id*	Enables STP by VLAN. VLAN ranges from 1 to 4094.
Step3		**End**	Changes to privileged EXEC mode.
Step4		**show spanning-tree vlan** *vlan-id*	Views the settings.
Step5		**copy running-config startup-config**	Stores the (option) settings in the configuration file.

To disable STP, use the global configuration command **no spanning-tree vlan** *vlan-id*.

The following example shows how to enable/disable STP on VLAN 1.

```
Switch#
Switch# configure terminal
Switch(config)# spanning-tree vlan 1
Switch(config)#
Switch(config)# end
Switch#
Switch# show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID      Priority    32768
               Address     0007.7012.2932
               This bridge is the root
               Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID    Priority    32768  (priority 32768 sys-id-ext 0)
               Address     0007.7012.2932
               Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
Interface          Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
fa5                Desg FWD 19        128.5    P2p
fa6                Desg FWD 19        128.6    P2p
Switch#
Switch# configure terminal
Switch(config)# no spanning-tree vlan 1
Switch(config)# end
Switch# show spanning-tree vlan 1
Spanning tree instance(s) for vlan 1 does not exist
Switch#
```

Disable per VLAN STP

The E3208E ONU can run a spanning-tree for an individual VLAN. That is, you can set STP state for each VLAN of VLAN trunk ports. If there are more the 32 VLANs in a switch, disable 'per VLAN STP' and use one spanning-tree instance to control all VLANs.

Note If STP is enabled for several VLANs while the 'Per VLAN STP' feature is disabled, the STP state of VLAN trunk ports might be unstable.

To disable 'per VLAN STP' for a switch, go through the following steps starting in privileged EXEC mode:

<Table 92> Disable per VLAN STP

		Command	Purpose
Step1		**configure terminal**	Enters global configuration mode.
Step2		**spanning-tree one-for-all-vlans**	Disables Per VLAN STP.
Step3		**End**	Changes to privileged EXEC mode.
Step4		**copy running-config startup-config**	Stores the (option) settings in the configuration file.

To enable 'per VLAN STP' of a switch, use the global configuration command **no spanning-tree one-for-all-vlans**.

```
Switch#
Switch# show spanning-tree
Spanning tree instance(s) does not exist
Switch# configure terminal
Switch(config)# spanning-tree one-for-all-vlans
%Warning: you may enable only one spanning-tree instance per port.
Switch(config)# spanning-tree vlan 1
Switch(config)# end
Switch# show running-config
!
spanning-tree one-for-all-vlans
spanning-tree vlan 1
!
Switch#
Switch#
```

```
Switch# configure terminal
Switch(config)# no spanning-tree vlan 1
Switch(config)# no spanning-tree one-for-all-vlans
Switch(config)# end
Switch# show running-config
!
!
Switch#
```

Configuring the Port Priority

If a loop is formed, the spanning tree determines the interfaces in forwarding state with port priority. You can assign a high priority (a small number) to an interface to be selected preferentially and a low priority(a large number) to an interface to be selected later. Where all interfaces carry the same priority, the spanning tree lets an interface with a smaller interface number go into forwarding state and blocks other interfaces.

To set an interface priority, go through the following steps starting in privileged EXEC mode:

<Table 93> Configuring the Port Priority

		Command	Purpose
Step1		**configure terminal**	Enters the global configuration mode.
Stpe2		**interface** *interface-id*	Specifies an interface and enters interface configuration mode. Effective interfaces include physical interfaces and port groups.
Step3		**spanning-tree vlan** *vlan-id* **port-priority** *priority*	Sets a VLAN port priority of the interface. • *vlan-id* ranges from 1 to 4094. • *priority* is a multiple of 16 between 0 and 240. The default setting is 128. A smaller number indicates a higher priority. Effective numbers include 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224 and 240. Other values are rejected.
Step4		**End**	Changes to privileged EXEC mode.
Step5		**show spanning-tree interface** *interface-id* or **show spanning-tree vlan** *vlan-id*	Views the settings.
Step6		**copy running-config startup-config**	Stores the (option) settings in the configuration file.

To restore the default setting of an interface, use the interface configuration command **no spanning-tree vlan** *vlan-id* **port-priority**.

```
Switch# show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32768
              Address     0007.7012.2932
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID   Priority    32768  (priority 32768 sys-id-ext 0)
              Address     0007.7012.2932
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
fa5              Desg FWD 19        128.5    P2p
fa6              Desg FWD 19        128.6    P2p
Switch# configure terminal
Switch(config)# interface fa5
Switch(config-if-fa5)# spanning-tree vlan 1 port-priority 240
Switch(config-if-fa5)# end
Switch# show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32768
              Address     0007.7012.2932
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID   Priority    32768  (priority 32768 sys-id-ext 0)
              Address     0007.7012.2932
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
fa5              Desg FWD 19        240.5    P2p
fa6              Desg FWD 19        128.6    P2p
Switch#
Switch# configure terminal
Switch(config-if-fa5)# no spanning-tree vlan 1 port-priority
Switch(config-if-fa5)# end
Switch# show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32768
              Address     0007.7012.2932
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID   Priority    32768  (priority 32768 sys-id-ext 0)
```

```
                Address         0007.7012.2932
                Hello Time      2 sec   Max Age 20 sec   Forward Delay 15 sec
Interface           Role Sts Cost         Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
fa5                 Desg FWD 19           128.5    P2p
fa6                 Desg FWD 19           128.6    P2p
Switch#
```

Configuring the Path Cost

The default value of path cost in a spanning-tree is determined from the interface speed. If a loop is formed, the spanning tree determines interfaces in forwarding state with path costs of the ports. You can assign a small cost value to an interface to be selected preferentially and a large cost value to an interface to be selected later. Where all interfaces carry the same cost values, the spanning tree lets an interface with a smaller interface number go into forwarding state and blocks other interfaces.

Note For a port group, you cannot determine path cost from the interface speed: member ports may have different speeds each other. Therefore, you should manually set path cost for a port group.

To set a path cost for an interface, go through the following steps starting in privileged EXEC mode:

<Table 94> Configuring the Path Cost

		Command	Purpose
Step1		**configure terminal**	Enters global configuration mode.
Stpe2		**interface** *interface-id*	Specifies an interface and enters interface configuration mode. Effective interfaces include physical interfaces and port groups.
Step3		**spanning-tree vlan** *vlan-id* **cost** *cost*	Sets a cost value of VLAN. If a loop is formed, the spanning tree determines ports in forwarding state with path cost. A lower path cost indicates forwarding at a higher rate. • *vlan-id* ranges from 1 to 4094. • *cost* ranges from 1 to 200000000. The default value is determined from the transfer rate of interface.
Step4		**End**	Changes to privileged EXEC mode.
Step5		**show spanning-tree interface** *interface-id* or **show spanning-tree vlan** *vlan-id*	Views the settings.
Step6		**copy running-config startup-config**	Stores the (option) settings in the configuration file.

To restore the default setting of the interface, use the interface configuration command **no spanning-tree vlan** *vlan-id* **cost**.

```
Switch# show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID      Priority    0
               Address     0007.70bc.cdde
               Cost        19
               Port        5 (fa5)
               Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID    Priority    32768  (priority 32768 sys-id-ext 0)
               Address     0007.7012.2932
               Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
fa5              Root FWD 19        128.5    P2p
fa6              Altn BLK 19        128.6    P2p
Switch# configure terminal
Switch(config)# interface fa5
Switch(config-if-fa5)# spanning-tree vlan 1 cost 100
Switch(config-if-fa5)# end
Switch# show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID      Priority    0
               Address     0007.70bc.cdde
               Cost        19
               Port        6 (fa6)
               Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID    Priority    32768  (priority 32768 sys-id-ext 0)
               Address     0007.7012.2932
               Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
fa5              Altn BLK 100       128.5    P2p
fa6              Root FWD 19        128.6    P2p
Switch# configure terminal
Switch(config)# interface fa5
Switch(config-if-fa5)# no spanning-tree vlan 1 cost
Switch(config-if-fa5)# end
Switch# show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID      Priority    0
               Address     0007.70bc.cdde
               Cost        19
```

```
                Port            5 (fa5)
                Hello Time      2 sec   Max Age 20 sec   Forward Delay 15 sec
  Bridge ID     Priority        32768   (priority 32768 sys-id-ext 0)
                Address         0007.7012.2932
                Hello Time      2 sec   Max Age 20 sec   Forward Delay 15 sec
Interface           Role Sts Cost          Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
fa5                 Root FWD 19              128.5    P2p
fa6                 Altn BLK 19              128.6    P2p
Switch#
```

Configuring the Switch Priority of a VLAN

You can change the switch priority to increase a possibility to be a root switch.

To set a switch priority for VLAN, go through the following steps starting in privileged EXEC mode:

<Table 95> Configuring the Switch Priority of a VLAN

		Command	Purpose
Step1		**configure terminal**	Enters global configuration mode.
Step2		**spanning-tree vlan** *vlan-id* **priority** *priority*	Sets a switch priority for VLAN. • *vlan-id* ranges from 1 to 4094. • *priority* is a multiple of 4096 between 0 and 61440. The default setting is 32768. A smaller number is more probable to be a root switch. Effective priority values include 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344 and 61440. Other values are not permitted.
Step3		**End**	Changes to privileged EXEC mode.
Step4		**show spanning-tree vlan** *vlan-id*	Views the settings.
Step5		**copy running-config startup-config**	Stores the (option) settings in the configuration file.

To restore the default setting of the switch, use the global configuration command **no spanning-tree vlan** *vlan-id* **priority**.

```
Switch# show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    0
              Address     0007.70bc.cdde
              Cost        19
              Port        5 (fa5)
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID   Priority    32768  (priority 32768 sys-id-ext 0)
              Address     0007.7012.2932
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
fa5              Root FWD 19        128.5    P2p
fa6              Altn BLK 19        128.6    P2p
Switch# configure terminal
Switch(config)# spanning-tree vlan 1 priority 0
Switch(config)# end
Switch#
Switch# show spanning-tree
VLAN0001
```

```
   Spanning tree enabled protocol ieee
   Root ID      Priority    0
                Address     0007.7012.2932
                This bridge is the root
                Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
   Bridge ID    Priority    0      (priority 0 sys-id-ext 0)
                Address     0007.7012.2932
                Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
fa5              Desg FWD 19        128.5    P2p
fa6              Desg FWD 19        128.6    P2p
Switch#
Switch# configure terminal
Switch(config)# no spanning-tree vlan 1 priority
Switch(config)# end
Switch# show spanning-tree
VLAN0001
   Spanning tree enabled protocol ieee
   Root ID      Priority    0
                Address     0007.70bc.cdde
                Cost        19
                Port        5 (fa5)
                Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
   Bridge ID    Priority    32768  (priority 32768 sys-id-ext 0)
                Address     0007.7012.2932
                Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
fa5              Root FWD 19        128.5    P2p
fa6              Altn BLK 19        128.6    P2p
Switch#
```

Configuring the Hello Time

You can set a period to send the configuration BPDU from the root switch by changing the hello time.

To set a hello time for VLAN, go through the following steps starting in privileged EXEC mode:

<Table 96> Configuring the Hello Time

		Command	Purpose
Step1		**configure terminal**	Enters global configuration mode.
Step2		**spanning-tree vlan** *vlan-id* **hello-time** *seconds*	Sets a hello time of VLAN. Hello time is a period for the root switch to send a configuration message, indicating that the switch is alive. • *vlan-id* ranges from 1 to 4094. • *seconds* ranges from 1 to 10. The default setting is 2.
Step3		**End**	Changes to privileged EXEC mode.
Step4		**show spanning-tree vlan** *vlan-id*	Views the settings.
Step5		**copy running-config startup-config**	Stores the (option) settings in the configuration file.

To restore the default setting of the switch, use the global configuration command **no spanning-tree vlan** *vlan-id* **hello-time**.

```
Switch# show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32768
              Address     0007.7012.2932
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID   Priority    32768  (priority 32768 sys-id-ext 0)
              Address     0007.7012.2932
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
fa5              Desg FWD 19        128.5    P2p
fa6              Desg FWD 19        128.6    P2p
Switch# configure terminal
Switch(config)# spanning-tree vlan 1 hello-time 5
Switch(config)# end
Switch# show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32768
              Address     0007.7012.2932
```

```
                This bridge is the root
                Hello Time   5 sec   Max Age 20 sec   Forward Delay 15 sec
  Bridge ID   Priority      32768   (priority 32768 sys-id-ext 0)
                Address        0007.7012.2932
                Hello Time   5 sec   Max Age 20 sec   Forward Delay 15 sec
Interface          Role Sts Cost          Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
fa5                Desg FWD 19            128.5    P2p
fa6                Desg FWD 19            128.6    P2p
Switch# configure terminal
Switch(config)# no spanning-tree vlan 1 hello-time
Switch(config)# end
Switch# show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID      Priority      32768
                Address        0007.7012.2932
                This bridge is the root
                Hello Time    2 sec   Max Age 20 sec   Forward Delay 15 sec
  Bridge ID   Priority      32768   (priority 32768 sys-id-ext 0)
                Address        0007.7012.2932
                Hello Time    2 sec   Max Age 20 sec   Forward Delay 15 sec
Interface          Role Sts Cost          Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
fa5                Desg FWD 19            128.5    P2p
fa6                Desg FWD 19            128.6    P2p
Switch#
```

Configuring the Forwarding-Delay Time for a VLAN

To set a forwarding-delay time for VLAN, go through the following steps starting in privileged EXEC mode:

<Table 97> Configuring the Forwarding-Delay Time for a VLAN

		Command	Purpose
Step1		**configure terminal**	Enters global configuration mode.
Step2		**spanning-tree vlan** *vlan-id* **forward-time** *seconds*	Sets a forward time of VLAN. Forward delay is a waiting time for a port to transit from listening or learning state of spanning-tree to forwarding state. • *vlan-id* ranges from 1 to 4094. • *seconds* ranges from 4 to 30. The default setting is 15.
Step3		**End**	Changes to privileged EXEC mode.
Step4		**show spanning-tree vlan** *vlan-id*	Views the settings.
Step5		**copy running-config startup-config**	Stores the (option) settings in the configuration file.

To restore the default setting of the switch, use the global configuration command **no spanning-tree vlan** *vlan-id* **forward-time**.

```
Switch# show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32768
              Address     0007.7012.2932
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID   Priority    32768  (priority 32768 sys-id-ext 0)
              Address     0007.7012.2932
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
fa5              Desg FWD 19        128.5    P2p
fa6              Desg FWD 19        128.6    P2p
Switch# configure terminal
Switch(config)# spanning-tree vlan 1 forward-time 20
Switch(config)# end
Switch# show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32768
              Address     0007.7012.2932
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 20 sec
  Bridge ID   Priority    32768  (priority 32768 sys-id-ext 0)
```

```
                Address         0007.7012.2932
                Hello Time      2 sec   Max Age 20 sec   Forward Delay 20 sec
Interface           Role Sts Cost         Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
fa5                 Desg FWD 19           128.5    P2p
fa6                 Desg FWD 19           128.6    P2p
Switch# configure terminal
Switch(config)# no spanning-tree vlan 1 forward-time
Switch(config)# end
Switch# show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID       Priority    32768
                Address         0007.7012.2932
                This bridge is the root
                Hello Time      2 sec   Max Age 20 sec   Forward Delay 15 sec
  Bridge ID     Priority    32768   (priority 32768 sys-id-ext 0)
                Address         0007.7012.2932
                Hello Time      2 sec   Max Age 20 sec   Forward Delay 15 sec
Interface           Role Sts Cost         Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
fa5                 Desg FWD 19           128.5    P2p
fa6                 Desg FWD 19           128.6    P2p
Switch#
```

Configuring the Maximum-Aging Time for a VLAN

To set a maximum-aging time for VLAN, go through the following steps starting in privileged EXEC mode:

<Table 98> Configuring the Maximum-Aging Time for a VLAN

		Command	Purpose
Step1		**configure terminal**	Enters global configuration mode.
Step2		**spanning-tree vlan** *vlan-id* **max-age** *seconds*	Sets a maximum-aging time of VLAN. Maximum-aging time is a waiting time to receive the spanning-tree information before the switch carries out reconfiguration. • *vlan-id* ranges from 1 to 4094. • *seconds* ranges from 6 to 40. The default setting is 20.
Step3		**End**	Changes to privileged EXEC mode.
Step4		**show spanning-tree vlan** *vlan-id*	Views the settings.
Step5		**copy running-config startup-config**	Stores the (option) settings in the configuration file.

To restore the default setting of the switch, use the global configuration command **no spanning-tree vlan** *vlan-id* **max-age**.

```
Switch# show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32768
              Address     0007.7012.2932
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID   Priority    32768  (priority 32768 sys-id-ext 0)
              Address     0007.7012.2932
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
fa5              Desg FWD 19        128.5    P2p
fa6              Desg FWD 19        128.6    P2p
Switch# configure terminal
Switch(config)# spanning-tree vlan 1 max-age 10
Switch(config)# end
Switch# show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32768
              Address     0007.7012.2932
              This bridge is the root
              Hello Time  2 sec  Max Age 10 sec  Forward Delay 15 sec
  Bridge ID   Priority    32768  (priority 32768 sys-id-ext 0)
              Address     0007.7012.2932
              Hello Time  2 sec  Max Age 10 sec  Forward Delay 15 sec
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
fa5              Desg FWD 19        128.5    P2p
fa6              Desg FWD 19        128.6    P2p
Switch# configure terminal
Switch(config)# no spanning-tree vlan 1 max-age
Switch(config)# end
Switch# show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32768
              Address     0007.7012.2932
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID   Priority    32768  (priority 32768 sys-id-ext 0)
              Address     0007.7012.2932
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
fa5              Desg FWD 19        128.5    P2p
```

fa6	Desg FWD 19	128.6	P2p

Switch#

Configuring the Port as Edge Port

To enable STP in the E3208E, a port connected to a single host should be defined as an edge port. If a port is not defined as an edge port, 2 x Forward Time will be taken for the port to transit to the forwarding state.

Note You should set a port connected to your terminal as an edge port. Otherwise, STP state of the port connected to the terminal will be affected by changes in the STP configuration of the network.

To define a port as an edge port, go through the following steps starting in privileged EXEC mode:

<Table 99> Configuring the Port as Edge Port

		Command	Purpose
Step1		**configure terminal**	Enters global configuration mode.
Step2		**Interface** *interface-id*	Sets an interface and enters interface configuration mode. Effective interfaces include physical interfaces and port groups.
Step2		**spanning-tree admin-edge-port**	Sets a port as an edge port.
Step3		**End**	Changes to privileged EXEC mode.
Step4		**show running-config**	Views the settings.
Step5		**copy running-config startup-config**	Stores the (option) settings in the configuration file.

To restore the default setting of the switch, use the interface configuration command **no spanning-tree admin-edge-port**.

```
Switch# show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32768
              Address     0007.7012.2932
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID   Priority    32768  (priority 32768 sys-id-ext 0)
              Address     0007.7012.2932
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
fa5              Desg FWD 19        128.5    P2p
fa6              Desg FWD 19        128.6    P2p
fa7              down DIS 0         128.7    P2p
Switch# configure terminal
Switch(config)# interface fa7
Switch(config-if-fa7)# spanning-tree admin-edge-port
Switch(config-if-fa7)# end
Switch# show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32768
              Address     0007.7012.2932
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID   Priority    32768  (priority 32768 sys-id-ext 0)
              Address     0007.7012.2932
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
fa5              Desg FWD 19        128.5    P2p
fa6              Desg FWD 19        128.6    P2p
fa7              down DIS 0         128.7    P2p Edge
Switch#
```

Configuring the RSTP Mode

You can set protocol mode for each spanning-tree instance of VLAN. In RSTP, a spanning-tree is configured using RSTP BPDUs only, and 802.1D BPDUs are used for compatibility only if 802.1D BPDUs are received. However, in STP compatible mode, RSTP BPDUs are not used but only 802.1D BPDUs are used. In addition, the fast recovery provided by RSTP is not applicable.

To change the protocol mode of STP, go through the following steps starting in privileged EXEC mode:

<Table 100> Configuring the RSTP Mode

		Command	Purpose

Step1		**configure terminal**	Enters global configuration mode.
Stpe2		**spanning-tree vlan** *vlan-id* **force-version rstp**	Sets protocol mode to RSTP mode for an RSTP instance of a specific VLAN. *vlan-id* ranges from 1 to 4094. Default is STP mode.
Step3		**End**	Changes to privileged EXEC mode.
Step4		**show running-config**	Views the settings.
Step5		**copy running-config startup-config**	Stores the (option) settings in the configuration file.

To restore the default setting, use the global configuration command **no spanning-tree vlan** *vlan-id* **force-version**.

```
Switch# show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID      Priority    32768
               Address     0007.7012.2932
               This bridge is the root
               Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID    Priority    32768  (priority 32768 sys-id-ext 0)
               Address     0007.7012.2932
               Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
fa5              Desg FWD 19        128.5    P2p
fa6              Desg FWD 19        128.6    P2p
Switch# configure terminal
Switch(config)# spanning-tree vlan 1 force-version rstp
Switch(config)# end
Switch# show spanning-tree
VLAN0001
  Spanning tree enabled protocol rstp
  Root ID      Priority    32768
               Address     0007.7012.2932
               This bridge is the root
               Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID    Priority    32768  (priority 32768 sys-id-ext 0)
               Address     0007.7012.2932
               Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
fa5              Desg FWD 19        128.5    P2p
fa6              Desg FWD 19        128.6    P2p
Switch# configure terminal
Switch(config)# no spanning-tree vlan 1 force-version
Switch(config)# end
Switch# show spanning-tree
```

```
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32768
              Address     0007.7012.2932
              This bridge is the root
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID   Priority    32768  (priority 32768 sys-id-ext 0)
              Address     0007.7012.2932
              Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
fa5              Desg FWD 19        128.5    P2p
fa6              Desg FWD 19        128.6    P2p
Switch#
```

Specifying the Link Type to Ensure Rapid Transitions

When a port is connected to another port over a point-to-point link, the port becomes a designated port.

Basically, Link-type is determined by duplex mode of interface: a full-duplex port is regarded as a point-to-point link; and half-duplex mode is regarded as a shared link. If there is a half-duplex link connected to a port of the remote switch by point-to-point connection, you can enable fast transition to forwarding state by changing the default setting of link-type.

Note In case of a port group, it is not feasible to determine the link type from duplex mode: the ports may have different duplex modes each other. Therefore, you should manually set link type for a port group.

To change the default link-type, go through the following steps starting in privileged EXEC mode:

<Table 101> Specifying the Link Type to Ensure Rapid Transitions

		Command	Purpose
Step1		**configure terminal**	Enters global configuration mode.
Stpe2		**interface** *interface-id*	Sets an interface and enters interface configuration mode.
Stpe3		**spanning-tree link-type point-to-point**	Sets the link type of port to point-to-point.
Step4		**End**	Changes to privileged EXEC mode.
Step5		**show running-config**	Views the settings.
Step6		**copy running-config startup-config**	Stores the (option) settings in the configuration file.

To restore the default setting, use the interface configuration commands **no spanning-tree link-type**.

Restarting the Protocol Migration Process

A switch that supports RSTP also supports a protocol migration mechanism that enables interworking with a switch running over 802.1D STP. If a switch receives a configuration BPDU (BPDU with protocol version set to 0), it transmits only 802.1D BPDUs to the port.

Although the switch does not receive further 802.1D BPDUs, it does not automatically switch to RSTP mode because it cannot be determined whether the STP switch has been removed from the switch or the 802.1D switch is not a designated switch any longer. Therefore, the switch continues to use 802.1D BPDUs only.

To initiate a protocol migration procedure (negotiation with adjacent switches) from a specific switch port, use the interface configuration command **spanning-tree mcheck**.

```
Switch# configure terminal
Switch(config)# interface fa5
Switch(config-if-fa5)# spanning-tree vlan 1 mcheck
Switch(config-if-fa5)#
```

Displaying the Spanning-Tree Status

To view the spanning-tree state, use one of the privileged EXEC commands listed in the following table:

<Table 102> Displaying the Spanning-Tree Status

Command	Purpose
show spanning-tree active	Shows the spanning-tree information on active interfaces only.
show spanning-tree interface *interface-id*	Shows the spanning-tree information on a specific interface.
show spanning-tree summary	Shows the spanning-tree summary.

For further information on other keywords of the privileged EXEC command **show spanning-tree**, see the command reference.

```
Switch# show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32768
              Address     0007.7012.2932
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID   Priority    32768  (priority 32768 sys-id-ext 0)
              Address     0007.7012.2932
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
fa5                 Desg FWD 19          128.5    P2p
fa6                 Desg FWD 19          128.6    P2p
Switch# show spanning-tree active
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    32768
              Address     0007.7012.2932
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID   Priority    32768  (priority 32768 sys-id-ext 0)
              Address     0007.7012.2932
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
fa5                 Desg FWD 19          128.5    P2p
fa6                 Desg FWD 19          128.6    P2p
Switch# show spanning-tree interface fa5
 Port 5 (fa5) of VLAN0001 is designated forwarding
    Port path cost 19, Port priority 128, Port Identifier 128.5.
    Designated root has priority 32768, address 0007.7012.2932
```

```
Designated bridge has priority 32768, address 0007.7012.2932
Designated port id is 128.5, designated path cost 0
Timers: message age 0, forward delay 0, hold 0
Number of transmition to forwarding state: 1
BPDU: sent 627, received 7
```

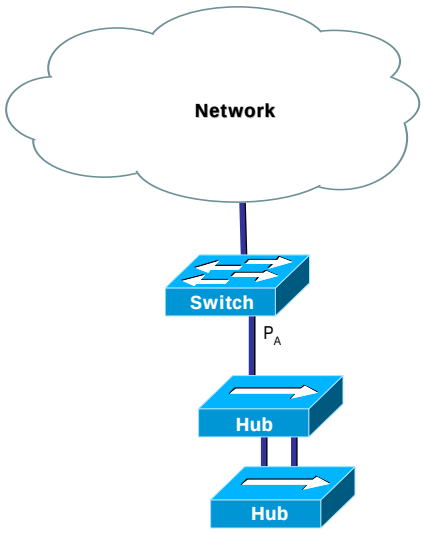
Self-loop Detection

This section describes how to set self-loop detection to detect the returned packets which have been transmitted by the switch itself.

Understanding Self-loop Detection

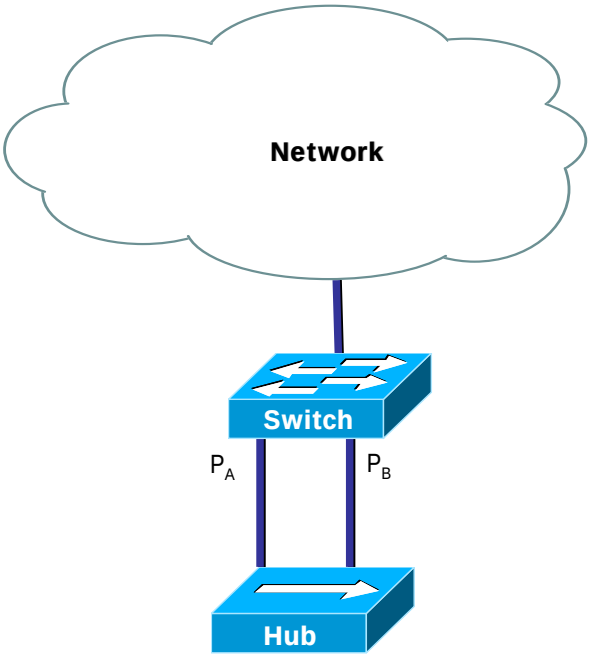
Although there are no dual paths in the user switch, a loop may be formed depending on a network configuration or on the status of cables connected to the switch.

A self-loop is formed when the packet transmitted through a port of the switch is returned through the same port. The figure below illustrates an environment where a self-loop is formed.



<Figure 19> Environment Where a Self-loop is formed

In the figure, a loop is formed by dual paths between two hubs. As STP is not enabled, the loop between those hubs would not be removed, resulting in instability of the network. In such a case, the packet transmitted through Port PA will be received through PA. If the self-loop detection feature is enabled in the switch, it detects the self-loop of port PA and makes it administrative disable status to protect other networks not connected to the switch and port PA. The loop exists in the equipment and networks connected to port PA as ever (Use STP to completely delete the loop from the network).



<Figure 20> Self-Loop Occurring Environments 2

There is loop at the ports of swtich in the above figure. In case that STP does not enable, It has still loop between port and port. So it makes unstable in the network. In this case, the packet sent via port PA is received to the port PB again and the packet sent via port PB is received to the port PA again. If self-loop detection enables on the switch, it detects the loop and protects the network by making administrative disabled status on the port PA and PB.

Configuring Self-loop Detection

This section describes how to set self-loop detection in a switch:

- Enabling Self-loop Detection
- Changing the Service Status of Port

Enabling Self-loop Detection

You can enable self-loop detection for an individual port or a range of ports of a switch. The self-loop detection feature is disabled in default.

Where a port goes shutdown state after the self-loop detection function has been enabled, it automatically changes to no shutdown state after the specified limit time. The limit time is set to 5 minutes in default and ranges from 0 to 1440 in minutes. If the limit time is set to 0, the affected port remains in shutdown state until it is manually cleared to no shutdown state.

To enable self-loop detection, go through the following steps starting in privileged EXEC mode:

<Table 103> Enabling Self-loop Detection

		Command	Purpose
Step1		**Configure terminal**	Enters global configuration mode.
Step2		**interface** *interface-name*	Enters Interface configuration mode.
Step3a		**self-loop-detection**	Enables self-loop detection. When a port goes shutdown due to a self loop detected, it will automatically go no shutdown state after 5 minutes.
Step3b		**self-loop-detection limit_time** <*0-1440*>	Enables self-loop detection. When a port goes shutdown due to a self loop detected, it will automatically go no shutdown state after the specified minutes.
Step4		**End**	Changes to privileged EXEC mode.
Step5a		**show running-config**	Views the settings.
Step5b		**show self-loop-detection**	Views the self-loop settings.
Step6		**copy running-config startup-config**	Stores the (option) settings in the configuration file.

The following shows an example of enabling self-loop detection for port fa1 with the default limit time:

```
Switch# configure terminal
Switch(config)# interface fa1
Switch(config-if-fa1)# self-loop-detection
Switch(config-if-fa1)# interface fa2
Switch(config-if-fa2)# self-loop-detection system
Switch(config-if-fa2)# end
Switch# show self-loop-detection
--------------------------------------------------------------------------
 ifname sld    link    shutdown set_time remain_time count          last-occur
--------------------------------------------------------------------------
```

fa1	**set**	up	**5 min**	0	
fa2	**sys**	down	**5 min**	0	
fa3		down		0	
fa4		down		0	
fa5		up		0	
……					
gi1		down		0	

Switch#

Changing the Service Status of Port

You can change the service-off status caused by self-loop detection to service-on status for a port with limit time set to 0.

To change the service status of a port, go through the following steps starting in privileged EXEC mode:

<Table 104> Changing the Service Status of Port

		Command	Purpose
Step1		**Configure terminal**	Enters global configuration mode.
Step2		**interface** *interface-name*	Enters Interface configuration mode.
Step3		**no shutdown**	Changes the port status to service-on.
Step4		**End**	Changes to privileged EXEC mode.
Step5		**show port status**	Views the port status information.

Disabling Self-loop Detection

You can disable self-loop detection for an individual port or for a range of ports of a switch.

If a port has automatically been shut down by self-loop detection, you can disable self-loop detection after setting the port status to ‘no shutdown’.

To disable self-loop detection, go through the following steps starting in privileged EXEC mode:

<Table 105> Disabling Self-loop Detection

		Command	Purpose
Step1		Configure terminal	Enters global configuration mode.
Step2		**interface** *interface-name*	Enters Interface configuration mode.
Step3a		**no self-loop-detection**	Disables self-loop detection. Shutdown caused by self-loop detection will automatically change to ‘no shutdown’ after 5 minutes.
Step4		**End**	Changes to privileged EXEC mode.
Step5a		**show running-config**	Views the settings.
Step5b		**show self-loop-detection**	Views the self-loop settings.
Step6		**copy running-config startup-config**	Stores the (option) settings in the configuration file.

The following shows an example of disabling self-loop detection for Port fa1:

```
Switch# configure terminal
Switch(config)# interface fa1
Switch(config-if-fa1)# no self-loop-detection
Switch(config-if-fa1)# end
Switch# show self-loop-detection
---------------------------------------------------------------------------
 ifname sld   link   shutdown set_time remain_time count        last-occur
---------------------------------------------------------------------------
 fa1      .     up        .        .          .        0            .
 fa2      .   down        .        .          .        0            .
 fa3      .   down        .        .          .        0            .
 fa4      .   down        .        .          .        0            .
 fa5      .     up        .        .          .        0            .
……
 gi1      .   down        .        .          .        0            .
Switch#
```

Displaying Self-loop Status

To display the self-loop detection settings for a port, use the privileged EXEC command **show running-config** or **show self-loop-detection**.

For **show self-loop-detection:**

- ifname : Interface name (Port name)
- sld : self-loop-detection (set)
- link : Link status (up, down)
- shutdown : Shutdown by SLD (set)
- set_time : Limit time (minutes). If limit time is set to 0, shutdown caused by SLD will remain until the affected port is manually cleared to ‘no shutdown’.
- remain_time : The remaining time until the normal state is recovered from shutdown state caused by SLD (minute:second)
- count : Number of shutdown events caused by SLD
- last-occur : The last shutdown time

The following shows an example of setting SDL to the default time, 5 minutes, for Port fa5. It can be seen that Port fa5 has been shut down on account of self loop detected by SLD on May 29 04:48:39, 2006.

```
Switch# show running-config
!
interface fa5
 self-loop-detection
!
interface vlan1
 ip address 100.1.1.1/24
!
Switch#
Switch# show self-loop-detection
---------------------------------------------------------------------------
 ifname sld   link   shutdown set_time remain_time count        last-occur
---------------------------------------------------------------------------
```

fa1	.	down	.	.	0	.
fa2	.	up	.	.	0	.
fa3	.	down	.	.	0	.
fa4	.	down	.	.	0	.
fa5	set	up	block	5 min	1	May 29 04:48:39 2007
fa6	.	down	.	.	0	.
fa7	.	down	.	.	0	.
fa8	.	down	.	.	0	.

Chapter 8. CPU-Filter & SYSCTL

CPU Filtering

The E3208E ONU supports filtering of the incoming traffic to the switch and the traffic forwarded by the switch CPU. Using the following commands, you can set filtering by IP address, by protocol and by port.

Enabling/Disabling CPU-Filtering Rule

For packet filtering, a proper rule should be defined first. A CPU-filtering rule is applicable to protocol, src/dest IP and UDP/TCP port. To apply the CPU-filtering rule, run the following command in Global mode.

<Table 106> Enabling CPU-Filtering Rule

Command	Description
cpu-filter rule *NAME* **ip { *srcIP* | *srcIP/M* | any } { *dstIP* | *dstIP/M* | any } match { permit | deny }**	CPU-filter for IP protocol Applies CPU-filter by source address and destination address Permits/denies packets using the match command
cpu-filter rule *NAME* **tcp { *srcIP* | *srcIP/M* | any } { *dstIP* | *dstIP/M* | any } { *srcPort* | any } { *dstPort* | any } match { permit | deny }**	CPU-filter for TCP protocol CPU-filter by source/destination address and source/ destination port number Permits/denies packets using the match command
cpu-filter rule *NAME* **udp { *srcIP* | *srcIP/M* | any } { *dstIP* | *dstIP/M* | any } { *srcPort* | any } { *dstPort* | any } match { permit | deny }**	CPU-filter for UDP protocol CPU-filter by source/destination address and source/ destination port number Permits/denies packets using the match command

To disable the CPU-filter rule, run the following command in configure mode.

<Table 107> Disabling CPU-Filtering Rule

Command	Description
no cpu-filter rule *NAME*	NAME : CPU-filter name

Setting a CPU-FILTER Group

To apply CPU-Filter to the system, the CPU-Filter rule should be added to a CPU-Filter group. Two groups of input group and output group can be defined in Frontier 7K. Input group is a filter group for the incoming traffic to the system, and forward group is a filter group for the traffic routed through the switch CPU. Several rules can be applied to a CPU-Filter group in the order of the rules added, and two types of CPU-Filter groups are supported. The order of rules applied can be displayed using the command **show CPU-filter group**.

Adding/Deleting an INPUT Group

To apply an input CPU-Filtering group, run the following command in Global mode.

<Table 108> Adding/Deleting an INPUT Group

Command	Description
cpu-filter group input add *NAME*	NAME : A rule name to be added
cpu-filter group input add *NAME1* **{ above | below }** *NAME2*	Adds a rule at a relative position of a rule already added NAME1 : A new rule name NAME2 : A rule name already added to a group above : Adds NAME1 above NAME2 below : Adds NAME1 below NAME2

To delete a rule from an input CPU-Filtering group, run the following command in Global mode.

Command	Description
cpu-filter group input delete *NAME*	NAME : A rule name to be deleted from the group
cpu-filter group input delete all	Deletes all rules included in the group

Add/Delete Forward Group

To apply a forward CPU-Filtering group, run the following command in Global mode.

<Table 109> Add/Delete Forward Group

Command	Description
cpu-filter group forward add *NAME*	NAME : A rule name to be added to the forward group
cpu-filter group forward add *NAME1* **{ above | below }** *NAME2*	Adds a rule at a relative position of a rule already added NAME1 : A new rule name NAME2 : A rule name already added to a group above : Adds NAME1 above NAME2 below : Adds NAME1 below NAME2

Enable CPU-FILTER Service

After defining a CPU-Filtering group, run the following command in Global mode to apply the rules to the system.

<Table 110> Enable CPU-FILTER Service

Command	Description
service cpu-filter	Enables CPU-FILTER
no service cpu-filter	Disables CPU-FILTER

Examples of Setting CPU-FILTER

The following shows an example of denying all incoming TELNET traffic to the system.

```
Switch# configure terminal
Switch(config)# cpu-filter rule telnet tcp any any any 23 match deny
Switch(config)# cpu-filter group input add telnet
Switch(config)# service cpu-filter
```

The following shows an example of denying FTP traffic routed through the switch CPU.

```
Switch# configure terminal
Switch(config)# cpu-filter rule ftp tcp any any any 20 match deny
Switch(config)# cpu-filter rule ftp-data tcp any any any 21 match deny
Switch(config)# cpu-filter group forward add ftp
Switch(config)# service cpu-filter
```

The following shows an example of showing the CPU-FILTER groups defined in the switch.

```
Switch# show cpu-filter group
----------------------
INPUT   GROUP-LIST      :
----------------------
telnet
----------------------
FOWARD GROUP-LIST       :
----------------------
ftp
----------------------
total 2group-list found
```

The following shows an example of showing the CPU-FILTER rules defined in the switch.

```
Switch# show cpu-filter
-------------------------------------------------------------------------
CPU-FILTER   PROTO SRC-IP          DST-IP          SPORT    DPORT    ACTION
-------------------------------------------------------------------------
telnet       tcp   any             any             any      23       deny
ftp          tcp   any             any             any      21       deny
ftp-data     tcp   any             any             any      20       deny
```

SYSCTL Overview

The SYSCTL command is used to define parameters associated with attack prevention of the parameters under /proc/sys/net/ipv4 provided the linux kernel

SYSCTL Command

The parameters that can be defined with the SYSCTL command can described below.

<Table 111> SYSCTL Command

Command	Description	Mode
sysctl secure_redirect INTERFACE (default|disable|enable)	Enables/Disables ICMP redirect message transfer only to the gateways in the default gateway list **Default) enable**	config
Sysctl send_redirects INTERFACE (default|disable|enable)	Enables/Disables ICMP redirect message transfer to other hosts. **Default) enable**	config
Sysctl icmp_port_unreach INTERFACE (default|disable|enable)	Enables/Disables Icmp port unreachable **Default) disable**	config
Sysctl icmp_host_unreach INTERFACE (default|disable|enable)	Enables/Disables Icmp host unreachable **Default) disable**	config
Sysctl icmp_net_unreach INTERFACE (default|disable|enable)	Enables/Disables Icmp net unreachable **Default) disable**	config
Sysctl icmp_prot_unreach INTERFACE (default|disable|enable)	Enables/Disables Icmp prot unreachable **Default) disable**	config
Sysctl tcp_max_syn_backlog VALUE	Sets a maximum value for the Tcp syn backlog queue **Default) 1024**	config
Sysctl ip_default_ttl VALUE	Sets a default TTL size **Default) 64**	config
Sysctl ipfrag_time VALUE	Sets a time to store the fragmented IP data in the memory **Default) 30**	config
Sysctl tcp_syn_retries VALUE	Sets a time to send SYN packets after the specified time for the purpose retransmission through an active TCP connection **Default) 5**	config
Sysctl tcp_retries1 VALUE	Sets a retransmission count for suspicious tcp session **Default) 3**	config
Sysctl tcp_retries2 VALUE	Sets a number of resend attempts before termination **Default)15**	config
Sysctl tcp_keepalive_time VALUE	Sets a keepalive time when keepalive is enabled **Default) 7200**	config
Sysctl tcp_fin_timeout VALUE	Sets a time to hold sockets in FIN-WAIT-2 status **Default) 60**	config
Sysctl tcp_max_tw_buckets VALUE	Sets a number of timewait sockets **Default) 18000**	config
Sysctl tcp_keepalive_probes VALUE	Sets a count to resend the keepalive	config

	probe message until connection is acknowledged **Default) 9**	
Sysctl tcp_syncookies(default|disable|enable)	Enables/Disables syn flood attack protection **Default) enable**	config
Sysctl tcp_send_reset (default|disable|enable)	Enables/Disables Tcp send reset flag **Default) enable**	config

Notice Some commands that the function of E3208E does not have for example ‘icmp unreachable’ in sysctl command.

Chapter 9. Static Monitoring & QoS

This chapter describes the administration and management function through RMON (Remote Monitoring) to monitor the current status of the E3208E ONU and to display the log information on the screen.

The statistics information provided by the E3208E ONU enables the system operator to immediately check the current operating status of the network. Through periodic management of statistics data, it is possible to estimate traffic flow in the future and take preventative actions before problems occur.

Status Monitoring

The status management function provides information on the switch. The E3208E ONU provides various types of status information on the user terminal using subcommands of the ‘show’ command.

<Table 112> Commands for Status Monitoring

Command	Description
show log	Shows the log currently managed in the system. It is possible to save up to 500 logs.
show memory usage	Shows the current memory usage of the system.
show cpu usage	Shows the current CPU usage.
show version	Shows the H/W and S/W versions of the switch.

Port Statistics

The E3208E ONU provides port statistics, showing the counter of each port of the modules being operated in the system.

You can view the port statistics using the following command:

show interface [interface name]

The E3208E ONU provides the following statistics on ports.

- **Link Status** – Current link status
- **Received Packet Count (Rx Pkt Count)** – The total number of good packets that have been received by the port.
- **Received Byte Count (Rx Byte Count)** – The total number of bytes that were received by the port, including bad or lost frames. This number includes bytes contained in the Frame Check Sequence (FCS), but excludes bytes in the preamble.
- **Transmit Packet Count (Tx Pkt Count)** – The number of packets that have been successfully transmitted by the port.
- **Transmit Byte Count (Tx Byte Count)** – The total number of data bytes successfully transmitted by the port.
- **Received Broadcast (Rx Bcast)** – The total number of frames received by the port that are addressed to a broadcast address.
- **Received Multicast (Rx Mcast)** – The total number of frames received by the port that are addressed to a multicast address.
- **Transmit Collisions (Tx Coll)** – The total number of collisions seen by the port, regardless of whether a device connected to the port participated in any of the collisions.
- **Received Bad CRC Frames (RX CRC)** – The total number of frames received by the port that were of the correct length, but contained a bad FCS value.
- **Receive Oversize Frames (RX Oversize)** – The total number of good frames received by the ports that were of greater than the supported maximum length of 1,522 bytes.
- **Receive Dropped Frames (Rx Drop)** – The total number of dropped frames due to lack of system resources.

Using the command ‘Show interface’, you can view various types of statistics data as follows.

```
Switch# show interface
fa1 is down
  type 100Base-TX
  ifindex 0(k2)   BROADCAST multicast
  auto-negotiation
  speed set auto
  duplex set full

  Last clearing of counters 17:31:00
  1 minutes input rate 0 bytes/sec, 0 packets/sec
  1 minutes output rate 0 bytes/sec, 0 packets/sec
     0 packets input, 0 bytes
     Received 0 broadcasts, 0 multicasts
     0 CRC, 0 oversize, 0 dropped
     0 packets output, 0 bytes
     Sent 0 broadcasts, 0 multicasts
fa2 is down
```

```
  type 100Base-TX
  ifindex 1(k3)    BROADCAST multicast
  auto-negotiation
  speed set auto
  duplex set full


  Last clearing of counters 17:31:00
  1 minutes input rate 0 bytes/sec, 0 packets/sec
  1 minutes output rate 0 bytes/sec, 0 packets/sec
     0 packets input, 0 bytes
     Received 0 broadcasts, 0 multicasts
     0 CRC, 0 oversize, 0 dropped
     0 packets output, 0 bytes
--More--
```

<Table 113> Command for Viewing Port Statistics

Command	Description	Mode
show port counter	Shows the counters of In/Out packets of all interfaces of the system.	Interface
show port counter detail	Shows In/Out packets and accumulated octets of all the interfaces of the system.	privileged
Show port statistics *IFNAME*	Shows bit/s, bytes/s, pkts/s of Rx/Tx of an interface in the interveral of 5 seconds, 1 minute, 5 minutes.	privileged
Show port statistics allports	Shows bit/s, bytes/s, pkts/s of Rx/Tx of all the interfaces in the interveral of 5 seconds, 1 minute, 5 minutes.	privileged

The following shows an example of showing the counters of packets for all ports and the statistics data of a specific interface(fa1/1) by 5 sec, 1min and 5 min, using the command show port counter.

```
Switch# show port counter

ifname I-Kbps O-Kbps        InUpkt      InNUpkt      OutUpkt      OutNUpkt
-------------------------------------------------------------------------
fa1          0       0           0            0            0            0
fa2          0       0           0            0            0            0
fa3          0       0           0            0            0            0
fa4          0       0           0            0            0            0
fa5          0       0           0            0            0            0
fa6          0       0           0            0            0            0
fa7          0       0           0            0            0            0
fa8          0       0           0            0            0            0
gi1          0       0           0            0            0            0
-------------------------------------------------------------------------
Switch#
```

```
Switch#
Switch# show port statistics fa2

Last clearing of counters :    0 days and 00:06:24 before

-----------------------------------------------------------------
                                         TX |                              RX
                      bits/s          pkts/s |        bits/s           pkts/s
-----------------------------------------------------------------
      5sec :                0               0               0               0
      1min :                0               0               0               0
      5min :                0               0               0               0
-----------------------------------------------------------------
Switch#
```

The following commands are used to clear the counters for statistics data.

<Table 114> Commands for Clearing Port Statistics

Command	Description	Mode
clear counters	Clears the counters of all interfaces of the system.	privileged

CPU Traffic Statistics

E3208E, for the purpose of monitoring packets that come in to CPU, can identify what type of packets are arrived by using of CPU Packet Counter.

CPU Packet Counter are classified according to the ether type of packet, which are of IP protocol, TCP port, or UDP port. It shows the value of last 5 seconds of CPU packet count, last 1minute of CPU packet count, or last 5 minutes of CPU packet count.

Configuring CPU Packet Counter

In this section, you can learn how to add packet type to a switch or remove it from the switch. Packet Counter classifies packets that come into CPU according to configured packet type and it supports default packet type and new packet type which is added by user.

CPU Packet Counter has default packet type list and these types are applied constantly. It is not possible to remove them from the list. The Default packet type has four elements of Ethertype, IP protocol, TCP port, and UDP port.

Ethertype

```
ETHERTYPE_IP            0x0800    /* IP protocol */
ETHERTYPE_ARP           0x0806    /* Addr. resolution protocol */
ETH_P_IPX     0x8137    /* IPX over DIX              */
```

IP Protocol

```
IPPROTO_IP = 0,          /* Dummy protocol for TCP          */
IPPROTO_ICMP = 1,        /* Internet Control Message Protocol       */
IPPROTO_IGMP = 2,        /* Internet Group Management Protocol      */
IPPROTO_TCP = 6,         /* Transmission Control Protocol       */
IPPROTO_UDP = 17,        /* User Datagram Protocol          */
IPPROTO_IPV6     = 41,         /* IPv6-in-IPv4 tunnelling         */
IPPROTO_PIM      = 103,        /* Protocol Independent Multicast      */
IPPROTO_RAW      = 255,        /* Raw IP packets                  */
```

TCP Port

```
20 : ftp-data
21 : ftp
22 : ssh
23 : telnet
25 : smtp
```

---

42 : nameserver

53 : domain

80 : www

137 : netbios-ns

138 : netbios-dgm

139 : netbios-ssn

TCP SYN

UDP Port

53 : domain

67 : BOOTP server

68 : BOOTP client

69 : tftp

123 : ntp

137 : netbios-ns

138 : netbios-dgm

139 : netbios-ssn

161 : snmp

162 : snmp-trap

The Packet type which User can add up will basically include the default packet type and the number of packet type can be extended to the specified number as bellows. The value in parenthesis () is default value.

- Ether type : 10 (default 4)
- IP protocol : 15 (default 8)
- TCP/UDP port : 15 (tcp 11, udp 10)

The additive packet type can be removed.

<Table 115> Addition of packet type

		Command	Purpose
Step1		Configure terminal	To get in Global configuration mode.
Step2a		**cpu-packet-counter ethertype** *ETHERTYPE*	To add new ethertype
Step2b		**cpu-packet-counter ip_protocol** *IP_PROTO*	To add new IP protocol
Step2c		**cpu-packet-counter tcp_port** *PORT_NUM*	To add new TCP port
Step2d		**cpu-packet-counter udp_port** *PORT_NUM*	To add new UDP port
Step3		**end**	To get in Priviledged mode.
Step4		**show running-config**	To identify the set configuration.
Step5		**copy running-config startup-config**	To store the set options into a configuration file.

The box below shows how to add TCP port 222.

```
Switch# configure terminal
Switch(config)# cpu-packet-counter tcp_port 222
Switch(config)# end
Switch#
```

Note Make sure that the variable types of Ethertype are “unsigned short”, IP protoco is “unsigned char”, TCP/UDP port is “unsigned short”.

The packet type to be can add by user includes designated packet type by default and it can add up to set number. The value in the blank() is the set value by default.

Ether type : 10 (default 4)

IP protocol : 15 (default 8)

TCP/UDP port : 15 (tcp 11, udp 10

You can see count with setting new packet type by your need . Also you can delete it

<Table 116> Removal of packet type

		Command	Purpose
Step1		**Configure terminal**	To get in Global configuration mode.
Step2a		**no cpu-packet-counter ethertype** *ETHERTYPE*	To remove the ethertype which user has added
Step2b		**no cpu-packet-counter ip_protocol** *IP_PROTO*	To remove the IP protocol which user has added
Step2c		**no cpu-packet-counter tcp_port** *PORT_NUM*	To remove the TCP port which user has added

Step2d		**no cpu-packet-counter udp_port** *PORT_NUM*	To remove the UDP port which user has added
Step3		**end**	To get back to Privilideged mode.
Step4		**show running-config**	To identify the set configuration.
Step5		**copy running-config startup-config**	To store the set options into a configuration file.

Displaying CPU Packet Counter

In order to refer the packet type which User has configured, you can use the privileged EXEC commands of “show running-config” or “show packet-counter type-list”.

The commands for referencing CPU packet counter are summarized in <table 43>.

<Table 117> Display cpu packet counter

Command	Purpose
show cpu-packet-counter	To display the content of cpu packet count of the interfaces regarding the basic protocols of Arp, tcp, udp, icmp, igmp, tcp syn.
show cpu-packet-counter *IFNAME*	To display the content of cpu packet count of the SPECIFIED interfaces regarding the basic protocols of Arp, tcp, udp, icmp, igmp, tcp syn.
show cpu-packet-counter bps	To display the content of cpu packet count of the interfaces regarding the basic protocols of Arp, tcp, udp, icmp, igmp, tcp syn. in terms of bps.
show cpu-packet-counter bps *IFNAME*	To display the content of cpu packet count of the SPECIFIED interfaces regarding the basic protocols of Arp, tcp, udp, icmp, igmp, tcp syn. in terms of bps.
show cpu-packet-counter pps	To display the content of cpu packet count of the interfaces regarding the basic protocols of Arp, tcp, udp, icmp, igmp, tcp syn. in terms of pps.
show cpu-packet-counter pps *IFNAME*	To display the content of cpu packet count of the SPECIFIED interfaces regarding the basic protocols of Arp, tcp, udp, icmp, igmp, tcp syn. in terms of pps.
show cpu-packet-counter total	To display all the packet counts which come up to CPU
show cpu-packet-counter ethertype *IFNAME*	To display all the packet counts which come up to CPU from the specified interface according to ethertype.
show cpu-packet-counter ip_protocol *IFNAME*	To display all the packet counts which come up to CPU from the specified interface according to IP protocol.
show cpu-packet-counter tcp_port *IFNAME*	To display all the packet counts which come up to CPU from the specified interface according to TCP port.
show cpu-packet-counter	To display all the packet counts which come up to

udp_port *IFNAME*	CPU from the specified interface according to UDP port.
show cpu-packet-counter type-list	To display all the types of packet that are refered in counting packets.
clear cpu-packet-counter	To clear all the stored cpu packet count.

Logging

The E3208E ONU log shows all environment setup information and alarm information. The system message logging software stores log messages in the switch memory and transfers them to other devices. The system message logging function supports the following features:

- Enables users to select logging data to be collected.
- Enables users to select a device to send the collected logging data.

The E3208E ONU stores logs in the debug level in the internal buffer and on the system console. Uses can control the logged system messages using CLI. Up to 500 log messages are stored in the system buffer. The system operator can perform remote monitoring by viewing the logs of the Syslog server or the system messages over Telnet or through the console.

The E3208E ONU supports severity levels 0-7.

<Table 118> Log Levels of E3208E ONU

Severity Level	Description
Emergencies (0)	System shutdown
Alerts (1)	Immediate actions required
Critical (2)	Critical state
Errors (3)	Error message
Warnings (4)	Warning message
Notifications (5)	Important information in normal condition
Informational (6)	Information message provided for users
Debugging (7)	Debugging message

Contents of System Log Message

A system log message of the E3208E ONU provides the following information:

Timestamp
Timestamp logs the month, data, year and time of an event in the followingformat: HH:MM:SS MM/DD/YYYY.

Severity level

- Level of 3600 switch log message defined in <Table 45>
- A number from 0 to 7

Log description

- A character string containing detailed information on the event

The following shows a log message displayed upon system booting.

```
May  6 11:53:48  [5] %REMOTE-CONNECT: login from console as lns
May  6 11:54:01  [5] IFM-NOTICE: Rate limit ra creation
May  7 02:10:24  [5] %REMOTE-CONNECT: login from console as lns
May  7 02:10:40  [5] IFM-NOTICE: Flow xx classified
May  7 02:10:48  [5] IFM-NOTICE: Flow xx match rate 10
May  7 05:17:56  [5] %REMOTE-CONNECT: login from console as lns
May  7 05:23:10  [5] IFM-NOTICE: Service pa add interface fa1
```

Default Logging Settings

<Table 119> System Log Default Settings

Parameter	Default Setting
Show logging on the console	Enabled
Show logging on a Telnet session	Disabled
Logging buffer size	250kb
Show Time-Stamp	enabled
Logging Server	Disabled
Syslog server IP address	None configured
Server facility	LOCAL7
Server severity	Warnings(4)
Console severity	Debuggings(7)
Telnet severity	info(6)
Save the logging into Flash	disable
Size of Flash buffer	25KB

<Table 120> Commands for Setting up System Message Logging Environment

Command	Description
logging console {*enable*|*disable*|*level*}	To configure the displaying the logging message into console and environment.
logging facility {*auth*|*cron*|*daemon*|*kernel*|*local0*| *local1*|*local2local3*|*local4*|*local5*| local6|local7|lpr|mail|news|syslog| user|uucp}	To configure the Facility parameter
logging flash {*enable*|*disable*|*level*|*size*}	To configure whether to store the syslog message into flash.
logging server *A.B.C.D*	To configure whether to send the syslog message to external syslog server
logging session {*enable*|*disable*|*level* }	To configure whether to display the logging message onto current session.
logging size BYTE	To set the size of syslog to be saved.
logging source-ip *A.B.C.D*	To set the source ip of syslog packet.

logging trap {<0-7>|*alert*|*crit*|*debug*|*emerg*|*err*| info|notice|warn}	To set the logging level of syslog server.
show logging {<0-7>|*back*|*flash* }	To display the logging buffer and verify the logging configuration.

The example of Logging configuration

When the administration monitor is connected to Console port and if you want to display log message which is Log level notice(5) and downward on console, you can configure as the box below. When you want to stop displaying log message on console, you can use “logging console disable” command.

```
Switch# configure terminal
Switch(config)# logging console enable
Switch(config)# logging console level notice
Switch(config)#
Switch(config)# end
Switch#
Switch# configure terminal
Switch(config)# logging console disable
Switch(config)#
```

When the administration monitor is connected via Telnet and if you want to display log message which is Log level warn(4) and downward onto telnet session, you can configure as the box below. When you want to stop displaying log message over Telnet session, you can use “logging session disable” command.

```
Switch#
Switch# configure terminal
Switch(config)# logging session enable
Switch(config)# logging session level warn
Switch(config)#
Switch(config)# end
Switch#
Switch# configure terminal
Switch(config)# logging session disable
Switch(config)#
```

When you want to save the log message which is Log level err(3) and downward into flash, you can configure as the box below. And when you want to stop saving log message into flash, you can use “logging flash disable” command.

```
Switch#
Switch# configure terminal
Switch(config)# logging flash enable
Switch(config)# logging flash level err
Switch(config)#
Switch(config)# end
Switch# configure terminal
Switch(config)# logging flash disable
Switch(config)#
```

When you want to send the log message which is Log level err(5) and downward to the Log server 100.10.1.1 you can configure as the box below. And when you want to stop sending the log message to the log server, you can use “no logging server” command.

```
Switch# configure terminal
Switch(config)# logging server 100.10.1.1
Switch(config)# logging trap err 100.10.1.1
Switch(config)# end
Switch#
Switch# configure terminal
Switch(config)# no logging server 100.10.1.1
Switch(config)#
```

RMON (Remote MONitoring)

The system operator can operate the system more efficiently and reduce load on the network using the RMON (Remote Monitoring) feature provided by the E3208E ONU.

The following sections describe the concept of RMON and the RMON service provided by the E3208E ONU.

RMON Overview

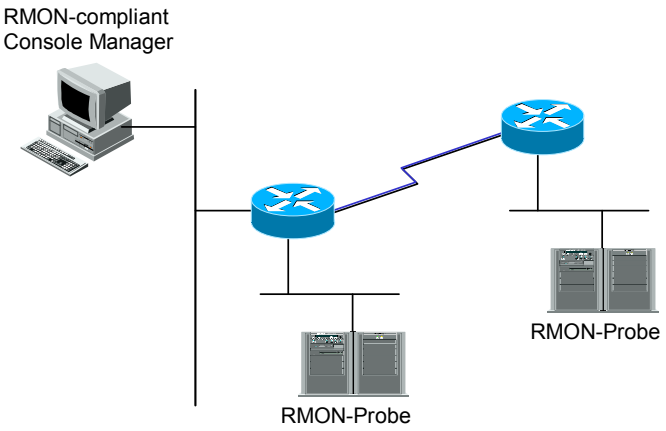
RMON enables the system operator to remotely manage the network in accordance with the international specifications defined in RFC 1271 and RFC 1757 of IETF (Internet Engineering Task Force). Typically, RMON consists of the two elements below:

RMON Probe

- An intelligent device or software agent remotely controlled to collect statistics data on LAN segments or VLAN.
- The collected data is transmitted to the host on demand or automatically according to the predefined environment.

RMON Manager

- Collects statistics information by communicating with RMON probes.
- A ROM manager is not always included in the same network as RMON probes but controls RMON probes through in-band or out-of-band control.



<Figure 21> RMON Manager and RMON Probes

While SNMP MIB are implemented for devices themselves equipped with an SNMP agent, RMON MIBs are implemented for the LAN segments connected to such devices. In other words, RMON MIBs provide information on traffic of all LAN segments, traffic of each host connected to the segments and traffic between hosts.

An RMON agent should support statistics data, history data, host related data, host matrix, filtering to filter specific packets to expect and preclude problems, alarm notification to automatically issue an alarm in the event the traffic reaches the specified threshold, and event generation function.

The E3208E ONU supports only statistics, history, alarm and event groups of the 9 RMON groups defined in the <Table 48>. All RMON settings are disabled in default.

<Table 121> RMON Groups

Group	Description
Statistics	Provides statistics on packet/byte count, broadcast/multicast count, collision count, packet count by length and various errors(fragment, CRC alignment, jabber, undersize, oversize) occurred in a segment.
History	Provides the information on traffic and errors occurred during a time period specified by the operator Sets a short/long term interval of 1-3600 sec. Provides utilization by time zone and comparison with other segments.
Alarm	A specific parameter is periodically monitored and reported to the operator when the value reaches a threshold. A threshold can be defined with an absolute value or a relative value. An alarm is to be issued only at low/high limit over so as to prevent repeated alarm activation.
Host	Manages the traffic and number of errors occurred in each device connected to the segment.
Top n hosts	Searches the hosts in the host table that caused heavy traffic during a specified period. The operator can get information by setting desired data type, time period and number of hosts.
Traffic matrix	Collects information on traffic generated between two hosts and errors based on the data link hierarchy, that is, MAC addresses. Users who use a specific host most frequently can be seen from this information. Since traffic to a host connected to other segment is usually routed, actual users of such host would be unknown.
Filter	Used for the operator to monitor a specific packet.
Packet capture	Enables the operator to collect and analyze packets generated in a segment.
Event	Logs a specific event and sends an alarm message to the operator. Trapping and logging are optional.

Setting Alarm and Event Groups of RMON

Users can configure RMON through the CLI or SNMP manager, using the following command in Privileged mode.

<Table 122> Commands for Setting RMON Alarm and Event

Command	Description	Mode
rmon alarm *index* ifEntry *variable ifIndex interval* {delta|absolute} rising-threshold *value* [*event-number*] falling-threshold *value* [*event-number*] [owner *string*]	Adds an alarm to the alarm table of RMON Index : An integer from 1 to 65535. Variable: MIB object 'interval' indicates a time period specified in seconds to monitor the alarm variable 'delta' indicates monitoring a difference between samples of MIB variable and 'absolute' indicates monitoring the absolute value of MIB variable. Sets a rising-threshold and a falling-threshold respectively. Event setting is an option. An event occurs when the delta value or the absolute value of an alarm variable reaches the rising-threshold or the falling threshold. Alarm owner can be defined.	Config
rmon event *index* [log] [trap community *string*] [owner *string*] [description *string*]	Adds an event to the RMON event table. 'log' specifies whether or not to create a RMON log when an event occurs. 'Trap' specifies trap transmission when an event occurs.	Config
no rmon alarm *alarm-index*	Deletes an alarm from the RMON alarm table.	Config
no rmon event *event-index*	Deletes an event from the RMON event table.	Config
show rmon alarm	Shows the RMON alarm table.	Privileged
show rmon event	Shows the RMON event table.	Privileged
show rmon log	Shows the RMON log table.	Privileged

Switch# **configure terminal**
Switch(config)# **rmon alarm 10 ifEntry inErrors 1 20 delta rising-threshold 15 1 falling-threshold 0 owner hong**
Switch(config)# **rmon event 1 log trap community rmontrap owner hong description "Noti : Too Much InErrors"**

```
Switch(config)# exit
Switch# show rmon alarm
-------------------------------------
            Alarm Configurations
-------------------------------------

The index of alarm      : 10
The interval            : 20
The type of Packets     : inErrors
The interface           : fa1
The type of Sample      : deltaValue
alarmValue              : 0
The status of starting: RISING_FALLING_ALARM
alarmRisingThreshold    : 15
alarmFallingThreshold : 0
alarmRisingEventIndex   : 1
alarmFallingEventIndex : 1
alarmOwner              : hong

Switch# show rmon event
-------------------------------------
            Event Configurations
-------------------------------------
The Index of event : 1
eventDescription    : "Noti:TooMuchInErrors"
eventType           : log and trap
Community           : rmontrap
eventOwner          : hong
Switch#
```

<Table 123> Commands for Setting RMON Statistics and History

Command	Description	Mode
rmon history *index* ifEntry *ifIndex* [buckets *bucket-number*] [interval seconds] [owner *string*]	Collects history by the specified number of buckets with the given interval 'index' ranges from 1 to 65535. The default number of buckets is 50.	Config
no rmon history *index* ifEntry *ifindex*	Disables collecting history data.	Config
show rmon history	Shows RMON history table.	Privileged
show rmon statistics	Shows RMON statistics table.	Privileged

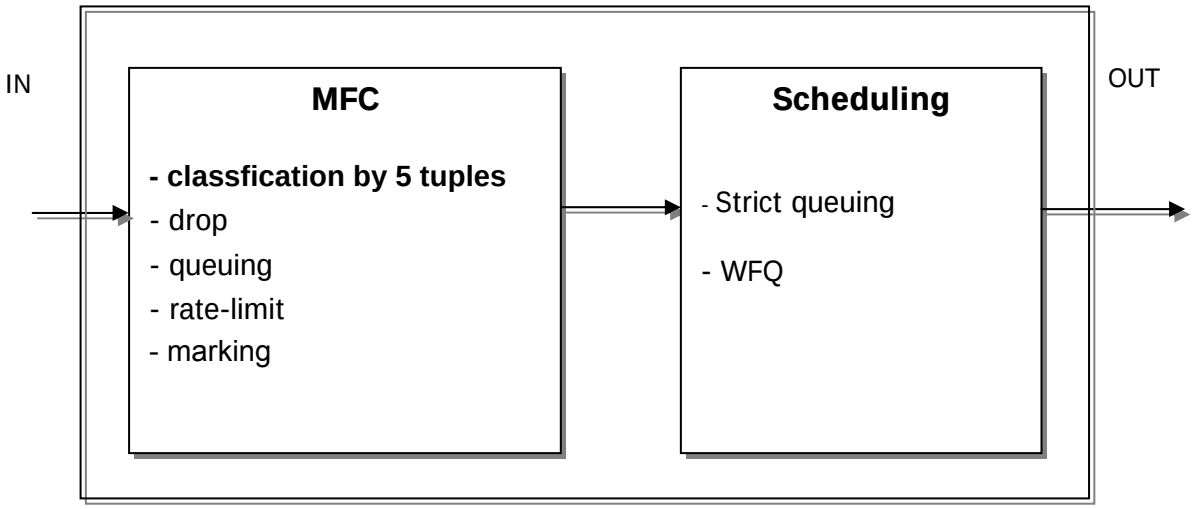
```
Switch# configure terminal
Switch(config)# rmon history 1 ifEntry 9 buckets 100 interval 5 owner park
Swtich(config)# end
Switch# show rmon history
-------------------------------------
```

```
                SHOW HISTORY
-------------------------------------


====== fa1 ======
Control-index        : 1
ifindex              : 9
interval             : 5
buckets              : 50
owner                : park

--- fa2 : bucket 1 ---
DropEvents           : 0
Octets               : 0
!
!
Switch# show rmon statistics
-------------------------------------------------------------------------------
                RMON STATISTICS
-------------------------------------------------------------------------------

The Index of stats    : 1 (fa1)
DropEvents            :          0   Jabbers              :          0
Octets                :          0   Collisions           :          0
Pkts                  :          0   Pkts64Octets         :          0
BroadcastPkts         :          0   Pkts65to127Octets    :          0
MulticastPkts         :          0   Pkts128to255Octets   :          0
CRCAlignErrors        :          0   Pkts256to511Octets   :          0
UndesizePkts          :          0   Pkts512to1023Octets  :          0
OversizePkts          :          0   Pkts1024to1518Octets :          0
Fragments             :          0
-------------------------------------------------------------------------------

The Index of stats    : 2 (fa2)
DropEvents            :          0   Jabbers              :          0
Octets                :          0   Collisions           :          0
Pkts                  :          0   Pkts64Octets         :          0
BroadcastPkts         :          0   Pkts65to127Octets    :          0
MulticastPkts         :          0   Pkts128to255Octets   :          0
CRCAlignErrors        :          0   Pkts256to511Octets   :          0
UndesizePkts          :          0   Pkts512to1023Octets  :          0
OversizePkts          :          0   Pkts1024to1518Octets :          0
Fragments             :          0
-------------------------------------------------------------------------------
!
!
Switch# show rmon statistics fa8
```

RMON STATISTICS

The Index of stats	: 8 (fa8)				
DropEvents	:	0	Jabbers	:	0
Octets	:	3331342	Collisions	:	0
Pkts	:	33150	Pkts64Octets	:	15428
BroadcastPkts	:	18579	Pkts65to127Octets	:	13300
MulticastPkts	:	14164	Pkts128to255Octets	:	3992
CRCAlignErrors	:	22	Pkts256to511Octets	:	206
UndesizePkts	:	0	Pkts512to1023Octets	:	398
OversizePkts	:	0	Pkts1024to1518Octets	:	92
Fragments	:	0			

Qos and Packet Filtering



The E3208E ONU supports the following features for Qos and packet filtering.

- MFC (Multi-Field Classifier)

  MFC carries out classification with the specified protocol, src/dest IP, UDP/TCP port, etc. to determine flow-rules and takes specific actions such as drop, queuing, rate-limit and marking accordingly. The results of classification are also used for filtering.

- Scheduling

  In the event of traffic overload, a scheduling algorithm is applied to process traffic according to the given conditions.

- - Strict Queuing Method

  This algorithm is applied to preferentially process important data. As data is processed according to the given priorities, data with a higher priority would be processed preferentially. Traffic with lower priorities would not be forwarded but queued, provided the entire bandwidth is filled with data of a higher priority.

- - WRR (Weighted Round Robin Method)

  This algorithm supplements disadvantage of SPQ by processing data according to the weights queued in accordance with the user environment.

MFC (Multi-Field Classifier)

Enabling/Disabling Flow-Rule

It is needed to classify flow-rules to determine the action for handling packets. Flow-rule classification can be carried out using the specified values such as src/dest mac, vlan, cos, ethertype, protocol, src/dest IP, UDP /TCP Port, dscp, tos and Tcp sync.

<Table 124> Commands for Flow-Rule Classification

Command	Description	Mode
flow-rule *NAME* **classify mac** {H.H.H|any} {H.H.H|any}	Enables classification using Mac.	Config
flow-rule *NAME* **classify mac mask** H.H.H H.H.H **mask** H.H.H H.H.H	Enables classification using Mac mask.	Config
flow-rule *NAME* **classify vlan <1-4094>**	Enables classification using Vlan	Config
flow-rule *NAME* **classify cos <0-7>**	Enables classification using Cos.	Config
flow-rule *NAME* **classify ethetype** *WORD*	Enables classification using Ethertype.	Config
flow-rule *NAME* **classify ipaddr** {A.B.C.D/M|any} {A.B.C.D/M|any}	Enables classification using IP address.	Config
flow-rule *NAME* **classify protocol** {<0-255>|icmp|igmp|ip|ospf|pim|tcp|udp}	Enables classification using Protocol.	Config
flow-rule *NAME* **classify dscp <0-63>**	Enables classification using DSCP.	Config
flow-rule *NAME* **classify tos <0-7>**	Enables classification using Tos.	Config
flow-rule *NAME* **classify l4port** {<0-65535>|any} {<0-65535>|any}	Enables classification using L4 port number.	Config
flow-rule *NAME* **classify l4port mask** *XXXX XXXX* **mask** *XXXX XXXX*	Enables classification using L4 port mask.	Config
flow-rule *NAME* **classify tcp-control** *VALUE MASK*	Enables classification using Tcp control flag.	Config
no flow-rule *NAME* **classify mac**	Disables classification using Mac.	Config
no flow-rule *NAME* **classify vlan**	Disables classification using Vlan.	Config
no flow-rule *NAME* **classify cos**	Disables classification using Cos.	Config
no flow-rule *NAME* **classify ethetype**	Disables classification using Ethertype.	Config
no flow-rule *NAME* **classify ipaddr**	Disables classification using IP address.	Config
no flow-rule *NAME* **classify protocol**	Disables classification using Protocol.	Config
no flow-rule *NAME* **classify dscp**	Disables classification using DSCP.	Config
no flow-rule *NAME* **classify tos**	Disables classification using Tos.	Config
no flow-rule *NAME* **classify l4port**	Disables classification using L4 port number.	Config
no flow-rule *NAME* **classify tcp-control**	Disables classification using Tcp	Config

	control fla.	

Notice Marking dscp, marking tos and cos-to-tos would not be concurrently applied but one of them will be applied in the order of dscp, tos and cos-to-tos.

A specific action is applicable to the flow-rule classified by the given condition.

For Qos, the Cos queue field may be marked or an action such as rate-limit may be applied.

<Table 125> Commands for Applying Flow-Rule

Command	Description	Mode
flow-rule *NAME* **match drop**	Drops the packets matching with the rule.	Config
flow-rule *NAME* **match queuing <0-7>**	Queues the packets matching with the rule.	Config
flow-rule *NAME* **match marking cos <0-7>**	Marks a packet matching with the rule with the specified Cos value.	Config
flow-rule *NAME* **match marking dscp <0-63>**	Marks a packet matching with the rule with the specified dscp value.	Config
flow-rule *NAME* **match marking tos <0-7>**	Marks a packet matching with the rule with the specified tos value.	Config
flow-rule *NAME* **match cos-to-tos**	Marks the tos value of a packet matching with the rule referring to the cos value of the packet.	Config
flow-rule *NAME* **match tos-to-cos**	Marks the cos value of a packet matching with the rule referring to the tos value of the packet.	Config
flow-rule *NAME* **match mirror**	Copies the packets matching with the rule to the specified mirror port.	Config
flow-rule *NAME* **match replace-vlan <1-4094>**	Marks the vlan of a packet matching with the rule with the specified value.	Config
flow-rule *NAME* **match redirect {all|unicast| not-unitcast}** *INTERFACE* **{ tag | untag }**	Redirects the packets matching with the rule to the specified INTERFACE.	Config
flow-rule *NAME* **match trap-cpu**	Traps the packets matching with the rule to the CPU.	Config
flow-rule *NAME* **match control-cpu-trap**	Traps the packets matching with the rule to the CPU with high priority and drops them at the same time.	Config
flow-rule *NAME* **match drop-precedence**	Assigns drop-precedence to the packets matching with the rule.	Config
flow-rule *NAME* **match metering**	Counts the packets matching with the rule.	Config
flow-rule *NAME* **match rate-limit** <64-1048576>	Applies rate-limit to the packets matching with the rule.	Config

no flow-rule *NAME* **match drop**	Permits the packets matching with the rule.	Config
no flow-rule *NAME* **match queuing**	Clears queuing of the packets matching with the rule.	Config
no flow-rule *NAME* **match marking cos**	Clears marking of the packets matching with the rule.	Config
no flow-rule *NAME* **match marking dscp**	Clears marking of the packets matching with the rule.	Config
no flow-rule *NAME* **match marking tos**	Clears marking of the packets matching with the rule.	Config
no flow-rule *NAME* **match cos-to-tos**	Clears marking of the packets matching with the rule.	Config
no flow-rule *NAME* **match tos-to-cos**	Clears marking of the packets matching with the rule.	Config
no flow-rule *NAME* **match mirror**	Clears mirroring of the packets matching with the rule.	Config
no flow-rule *NAME* **match replace-vlan**	Clears replace-vlan of the packets matching with the rule.	Config
no flow-rule *NAME* **match redirect**	Clears redirection of the packets matching with the rule.	Config
no flow-rule *NAME* **match trap-cpu**	Clears trap-cpu of the packets matching with the rule.	Config
no flow-rule *NAME* **match control-cpu-trap**	Clears trap-cpu of the packets matching with the rule.	Config
no flow-rule *NAME* **match drop-precedence**	Clears drop-precedence of the packets matching with the rule.	Config
no flow-rule *NAME* **match metering**	Clears metering of the packets matching with the rule.	Config
no flow-rule *NAME* **match rate-limit**	Clears rate-limit of the packets matching with the rule.	Config

Notice Several of the actions above can be simultaneously applied to flow-rules, but this may not be true depending on actions. For instance, queuing and marking cos can be applied simultaneously but drop and queuing would not be applied at the same time. Priorities of actions follow the Broadcom chipset.

Notice 'control-cpu-trap' traps packets with high-priority of cpu and drops those packets at the same time. It is recommended to set trap to concerned packets in order to perform Igmp snooping.

port range checker

Port range checker is the function to classify L4port range easy. Before classify L4port range, you define port range with the following commands.

<Table 126> port range checker Command

Command	Description	Mode
flow-rule l4port-range-checker *<1-16>* (*src*|*dst*) *<0-65535> <0-65535>*	Identify of L4port-range-checker is 1-16. Sets direction, range of port.	Privileged

You can define l4port-range-checker up to maximum 16 number. Each l4port-range-checker can be set only one between source port and destination port.

To help your understanding, two examples to fulfill the following conditions are given below.

e.g. 1) Apply the following conditions to Port fa1.
Drop tcp src 6000~10000

```
Switch#configure terminal
Switch(config)# flow-rule l4port-range-checker 1 src 6000 10000
Switch(config)# flow-rule f1 classify tcp any any l4port-range-checker 1 any
Switch(config)# flow-rule f1 match drop
Switch(config)#
Switch(config)# policy-map p1 flow-rule f1
Switch(config)#
Switch(config)# service-policy fa1 ingress p1
Switch(config)#
```

Creating/Adding Policy-Map

You can create and apply a policy-map to apply flow-rules to an interface. Since several flow-rules can be included in a policy-map, several actions may be applied to an interface. The order of adding flow-rules is very important because they are applied in the order of being added to the policy-map.

You can display the order of flow-rules using the command **show flow-rule**.

<Table 127> Command for Creating and Adding a Policy-Map

Command	Description	Mode
policy-map *PNAME* **flow-rule** *FNAME*	Creates a new policy-map where PNAME is not specified or adds the flow-rule FNAME to the end where the policy PNAME has already been created.	Config

Use the following command to delete the entire policy-map or a flow-rule applied to the policy-map.

<Table 128> Commands for Deleting the Policy-Map or a Specific Flow-Rule

Command	Description	Mode
No policy-map *PNAME*	Deletes the policy-map PNAME.	Config
No policy-map *PNAME* **flow-rule** *FNAME*	Deletes the flow-rule FNAME from the policy-map PNAME.	Config

The commands for enabling/disabling the created policy-map for a vlan interface are described below.

<Table 129> Commands for Enabling/Disabling Policy-Map

Command	Description	Mode
service-policy *IFNAME* **{ingress|egress}** *PNAME*	Enables the policy-map PNAME in the specified direction of a specific port interface.	Config
no service-policy *IFNAME*	Disables the policy-map applied to a specific interface.	Config

Notice Since just one policy-map is applied to each port interface, care should be taken to the order of flow-rules when creating a policy-map including several flow-rules.

Notice The drop rule will be applied preferentially when a drop rule and other match rules of a policy-map are applied simultaneously.

You can view flow-rule settings using the following commands.

<Table 130> Commands for Showing Flow-Rules

Command	Description	Mode
show flow-rule	Shows the information on flow-rules and policy-map.	Config
show service-policy	Shows the current policy-map and vlan interface.	Config

To help your understanding, two examples to fulfill the following conditions are given below.

e.g. 1) Apply the following conditions to Port fa1.
Drop tcp port 6000
Src ip 20.1.1.0/24 queuing 2
Queuing 3 (highest) and marking for Tcp port 23

Switch#configure terminal
Switch(config)# **flow-rule f1 classify tcp any any 6000 any**
Switch(config)# **flow-rule f1 match drop**
Switch(config)# **flow-rule f2 classify ip 20.1.1.0/24 any**
Switch(config)# **flow-rule f2 match queuing 2**
Switch(config)# **flow-rule f3 classify tcp any any 23 any**
Switch(config)# **flow-rule f3 match cos-and-queue 7**
Switch(config)#
Switch(config)# **policy-map p1 flow-rule f1**
Switch(config)# **policy-map p1 flow-rule f2**
Switch(config)# **policy-map p1 flow-rule f3**
Switch(config)#
Switch(config)# **service-policy fa1 ingress p1**
Switch(config)# Switch(config)# **service-policy fa1**
Switch(config)#

e.g. 2) Apply the following conditions to Port fa2.

Set rate limit 10Mbps to tcp port 4010
Set rate limit 20Mbps to tcp port 5010

```
Switch# conf t
Switch(config)# flow-rule f4 classify tcp any any 4010 any
Switch(config)# flow-rule f4 match rate-limit 10000
Switch(config)# flow-rule f5 classify tcp any any 5010 any
Switch(config)# flow-rule f5 match rate-limit 20000
Switch(config)#
Switch(config)# policy-map p2 flow-rule f4
Switch(config)# policy-map p2 flow-rule f5
Switch(config)#
Switch(config)# service-policy fa2 ingress p2
Switch#
```

Qos Parameters

An L2 packet with tag assigned in accordance with IEEE 802.1p standard carries a cos value indicating a packet priority, which is also used for queuing. It is also possible to set/clear the cos value ranging from 0 to 7.

An L3 packet carries a dscp value, which is also used for queuing.

The E3208E ONU provides 8 queues for each interface, and system-wide mapping tables are maintained between them.

You can change the marking/remarking table using the following commands.

<Table 131> Commands for Setting Qos Related Marking/Remarking Table

Command	Description	Mode
qos cos-queue-map *<0-7> <0-7>*	Sets a new queue value for mapping with a cos value of the packet applied to the rule. This value can be viewed using the command **show qos cos**.	Config
qos cos-remarking *<0-7> <0-7>*	Sets a new cos value for remarking with a queue value of the packet applied to the rule.	Config
qos dscp-dp-map *<0-63> <0-1>*	Sets a new dp value for mapping with a dscp value of the packet applied to the rule. This value can be viewed using the command **show qos dscp**.	Config
qos dscp-pri-map *<0-63> <0-7>*	Sets a new pri value for mapping with a dscp value of the packet applied to the rule. This value can be viewed using the command **show qos dscp**.	Config

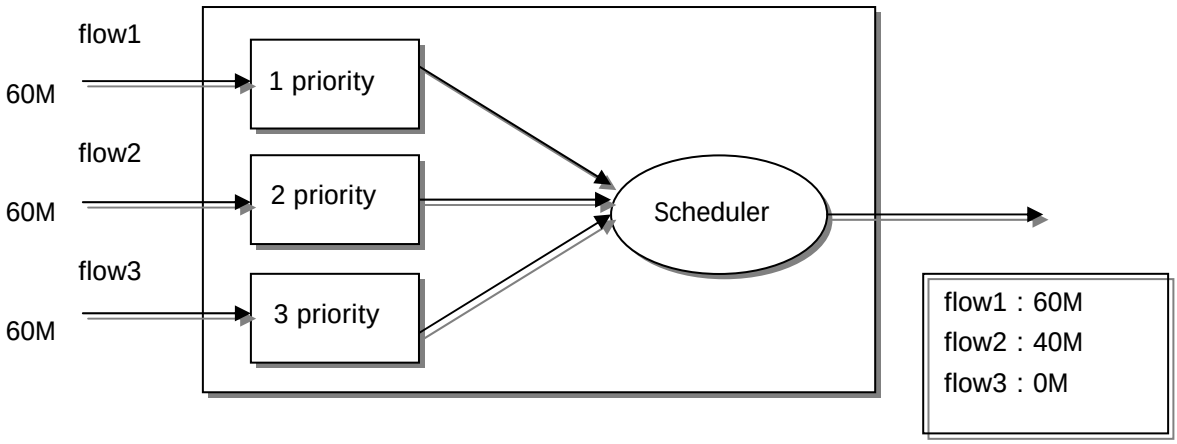
<Table 132> Commands for Viewing Qos Related Marking/Remarking Table

Command	Description	Mode
show qos cos	Shows the mapping/remaking table with a cos value of the packets applied to the rule.	Privileged
show qos dscp	Shows the mapping/remaking table with a dscp value of the packets applied to the rule.	Privileged

Scheduling

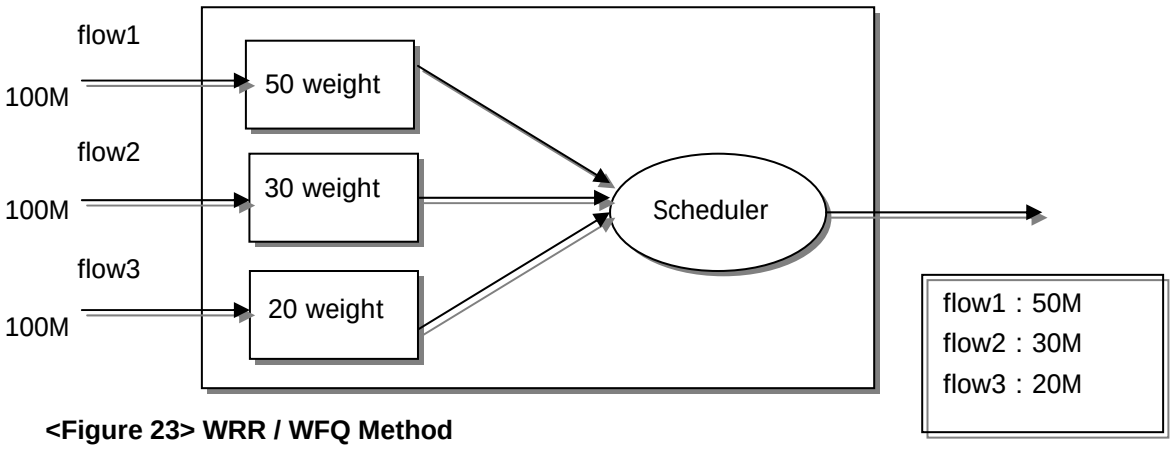
The E3208E ONU provides SPQ (Strict Priority Queue), WRR (Weighted Round Robin) and WFQ(Weighted Fair Queuing) methods for scheduling. The default setting is SPQ.

The figure below illustrates differences between SPQ and WFQ.



<Figure 22> SPQ (Strict Priority Queue) Method

As the SPQ (Strict Priority Queue) method preferentially processes packets with a higher priority, there might be a case where all packets of flow1 are forwarded and the packets of flow3 with a lower priority are not forwarded at all.



<Figure 23> WRR / WFQ Method

In the example above, in contrast to SPQ, the WRR/WFQ method forwards traffic based on the weight defined for each port. WFQ does not forward traffic with a fair weight like in WRR but, depending on traffic conditions, can assign more traffic than the weight value in the queue of a higher priority.

The E3208E ONU provides 8 queues for scheduling. The following commands are used to define queue-mode for a specific interface.

<Table 133> Commands for Changing Queue-Mode

Command	Description	Mode
queueing-mode {**strict** |**rr** |**wrr**| **wfq** }	Changes the queue-mode of a specific interface to Strict mode or RR / WRR / WFQ. The default mode is Strict.	Interface

queueing-method *<0-7>* **{ strict |wrr| wfq }**	Changes the queue mode of a specific interface from WRR or WFQ to strict.	Interface

Notice Of the 8 queues in SPQ, a larger number has a higher priority.

The following commands are used to change weight in the queues in WRR / WFQ mode.

<Table 134> Commands for Changing Wrr-Method Queue Weight

Command	Description	Mode
queueing-profile wfq-weight *<0-7> <1-2047>*	Sets wfq weight of a specified queue for a port set to wfq mode.	Interface
no queueing-profile wfq-weight	Clears wfq weight of a specified queue for a port set to wfq mode.	Interface
queueing-profile wrr-weight *<0-7> <1-15>*	Sets wrr weight of a specified queue for a port set to wrr mode.	Interface
no queueing-profile wrr-weight	Clears wrr weight of a specified queue for a port set to wrr mode.	Interface

Notice wrq weight 1 indicates 64kbps in case of 100M port and 2Mbps in case of Giga port.

The following command is used to show scheduling for each port.

<Table 135> Command to Show Queue-Method and Weight for All Interfaces

Command	Description	Mode
show port qos	Shows the queue-method and weight of all interfaces in the system.	Privileged

Congestion Avoidance

Congestion frequently appears in the output queue due to queue overflow incurred by discordance of transfer rate between input and output links in the network. In the event of queue overflow, it is important to discard packets in the buffer and to maintain delay time of packets to a desired value in order to make the resources in the buffer available.

The E3208E ONU preferentially discards packets with a higher drop priority marked by the flow classifier or traffic conditioner. In the E3208E, the parameters used for this purpose can be set for each queue by traffic types.

Filtering

Netbios filter can be defined for an individual interface. If the Netbios filter is enabled, the Netbios / Netbeui / NBT protocol will be blocked.

Dhcp filter can also be defined for an individual interface. If Dhcp filter is enabled, DHCP server packets of the affected interface will be blocked.

The commands used for filtering are described below.

Filtering settings can be displayed using the command ‘show interface’.

<Table 136> Commands for Filtering

Command	Description	Mode
filter netbios	Enables the netbios filtering for an interface.	Interface
no filter netbios	Disables the netbios filtering for an interface.	Interface
filter dhcp	Enables the dhcp filtering for an interface.	Interface
no filter dhcp	Disables the dhcp filtering for an interface.	Interface
filter private-ip [10|172|192|all]	Enables the private IP filtering for an interface.	Interface
no filter private-ip [10|172|192|all]	Disables the private IP filtering for an interface.	Interface
filter src-ip-all-f	Enables the filtering of packets with src IP of all f (255.255.255.255) for an interface.	Interface
no filter src-ip-all-f	Disables the filtering of packets with src IP of all f (255.255.255.255) for an interface.	Interface
filter src-ip-loopback	Enables the filtering of packets with loopback ip (127.0.0.0/8) for an interface.	Interface
no filter src-ip-loopback	Disables the filtering of packets with loopback ip (127.0.0.0/8) for an interface.	Interface

Chapter 10. Saving Configuration and Upgrading Software

Flash File System

This chapter describes flash file system management for the system. The flash file system stores the OS image and configuration files of the system, which will be loaded to the system upon system booting.

- Commands for operation of the flash file system
- Commands for management of OS image and configuration files
- Commands for setting booting mode

The E3208E ONU builds a flash file system for storing OS images and setting up environment. This chapter summarizes the flash file system of the switch.

The flash file system stores OS images and configuration in files. Each file is recorded in the flash memory area. You can specify a filename using the rename command or delete a file stored in the flash file system using the erase command. When erasing or renaming a file, pay attention whether the file is an image or configuration file to be booted upon reloading.

The basic commands for system file management are given below:

<Table 137> Commands for File Management

Command	Description	Mode
show flash	Shows the status of flash files.	Privileged
erase *filename*	Deletes a configuration file stored in the flash memory.	Privileged

The following shows an example of running the show flash command. The E3208E ONU shows the information on flash file system such as file name and size, current (-) and next booting modes (*) and OS or configuration file information.

```
Switch# show flash

  flash info
-length- ----------type/info---------- CN path
6684094    1.0.0                        -* p33xx.100
6684094    1.0.0                        -* p33xx.100_b
105          Configuration              B* cfg.txt
256 Kbytes available (7124 Kbytes used)

Switch#
```

Image/Configuration File Down/Up Load

The E3208E ONU can download or upload OS image and configuration files required for operation over FTP or TFTP. It can store new files in the flash file system or apply them as OS image or configuration files upon booting. In addition, it can store the OS image or configuration files required for operation in the FTP/TFTP server. This chapter describes how to down/upload files over FTP/TFTP. running-config and startup-config given below are described in the chapter “Configuration File Management”.

Warning Since the images to be upgraded should be carefully selected depending on the system model and version, follow the instructions of the company.

Warning The configuration to be applied over FTP/TFTP will be added or updated in the current configuration of the system. That is, the current configuration of the system would not be entirely replaced with the downloaded configuration.

Download/Upload over FTP

The table below describes the commands for downloading/uploading files over FTP.

<Table 138> Commands for Downloading/Uploading over FTP

Command	Description	Mode
copy ftp flash	Copies an OS image file from the FTP server to the flash memory.	Privileged
copy flash ftp	Copies an OS image file from the flash memory to the FTP server.	
copy ftp config-file	Copies a configuration files from the FTP server to the flash memory.	Privileged
copy ftp running-config	Applies a configuration file in the FTP server as the current running-config.	Privileged
copy running-config ftp	Copies the current running-config being applied in the system to the FTP server.	Privileged

The following shows an example of downloading a file over FTP.

```
Switch# copy ftp flash
IP address of remote host ? 192.168.0.1
User ID ? Ins
Password ?
Source file name ? p33xx.100
Destination file name ? p33xx.100

FTP::192.168.0.1//p33xx.100-->image file[p33xx.100]
Proceed [yes/no]?    yes
!
```

Download/Upload over TFTP

The table below describes the commands for downloading/uploading files over TFTP.

<Table 139> Commands for Downloading/Uploading over TFTP

Command	Description	Mode
copy tftp flash	Copies an OS image file from the TFTP server to the flash memory.	Privileged
copy flash tftp	Copies an OS image file from the flash memory to the TFTP server.	
copy tftp config-file	Copies a configuration file from the TFTP server to the flash memory.	Privileged
copy tftp running-config	Applies a configuration file in the TFTP server as the current running-config.	Privileged
copy running-config tftp	Copies the current running-config being applied in the system to the TFTP server.	Privileged

The following shows an example of uploading a file to the TFTP server.

```
Switch# copy flash tftp
IP address of remote host ? 192.168.0.1
filename to write on tftp host? p33xx.100

TFTP send: -> 192.168.0.1// p33xx.100
Proceed [yes/no]? yes
!
```

Configuration File Management

Environment settings are a set of various parameters defined by the system operator while operating the E3208E ONU. The configuration of E3208E ONU consists of startup-config and running-config. startup-config is stored in the flash memory and loaded upon booting the switch, and running-config includes the environment settings running in the DRAM. This section describes storing, deleting and downloading files required for configuration file management.

<Table 140> Commands for Configuration Management

Command	Description	Mode
show startup-config	Shows the environment settings of the bootingconfiguration stored in the flash memory.	Privileged
show running-config	Shows the current environment settings.	Privileged
copy running-config startup-config	Stores the running configuration file currently being executed in the system as a startup file.	Privileged
erase startup-config	Deletes the current startup configuration file.	Privileged

Copying a Configuration File

When the system operator changes the environment settings, the updated configuration is stored in the DRAM and the configuration information stored in the DRAM would not be maintained upon system rebooting. Therefore, to maintain the configuration information upon system rebooting, the configuration file should be stored in the flash memory. The following shows an example of showing the current running configuration and copying the current running-config to startup-config.

```
Switch# show running-config
Current configuration...

Building system configuration...


interface vlan1
  ip address 192.168.51.1/24
!
!
Switch#
Switch# copy running-config startup-config
Building system configuration...

Write system configuration to system.cfg...

Saving system configuration to system.cfg completed
Switch# show startup-config
Startup configuration...

interface vlan1
ip address 192.168.51.1/24
        ... <skipped > ....
```

```
Switch#
```

Deleting a Configuration File

The E3208E ONU reloads the startup-config stored in the flash memory upon system restart. If you want to reboot the system with a configuration file other than the current one, you can delete startup-config and reboot the system with a desired file, as seen in the example below.

```
Switch# erase test.cfg
Switch#
```

Boot Mode Setting and System Restarting

You can configure the OS image and configuration files required for operation of the E3208E ONU with the booting file described below. Care should be taken because the OS image and configuration files configured like this will be applied to system restart. The following sections describe how to set booting mode for the OS image and configuration files and to restart the system.

<Table 141> Commands for Setting Boot Mode and Restarting the System

Command	Description	Mode
boot flash *filename*	Sets an OS image to be applied to rebooting.	Privileged
boot config *filename*	Sets a configuration file to be applied to rebooting.	Privileged
Reload	Restarts the system.	Privileged

Setting Boot Mode

When setting boot mode for the OS image and configuration file in the E3208E ONU, care should be taken on the following points. The command 'boot flash' should be applied only to the OS image file applicable to the E3208E ONU. In addition, the command 'boot config' should be applied to the configuration file applicable to the E3208E ONU. Note that only the files in the current flash file system are applicable to the switch.

```
Switch#
Switch# boot flash p3k.r101
Switch#
Switch# boot config lns.cfg
Switch#
```

Restarting the System

You can restart the system by E3208E ONU power on/off or using the following command on the console.

Warning Before restarting the system, make sure to save the current configuration in the flash memory.

Warning Do not restart the system forcibly while the system is storing files in the flash file system.

```
Switch# reload

WARNING !!!
  You must save current configuration or you will lose it...
"continue to reboot [yes/no]? yes
Switch#
```

Chapter 11. Utility

This chapter describes other functions required for operation of the system.

Packet Dump

E3208E ONU provides the function of automatic execution of tcpdump and generation of log file for the traffic in case the switch would go beyond the predefined threshold level for cpu usage.

Condition for automatic execution

When cpu usage goes beyond the pre-defined threshold, tcpdump shall be executed as a background process and to be saved into a file. Later if the condition would be met, for example, a certain number of packets or lapse of minutes, then it will be terminated automatically.

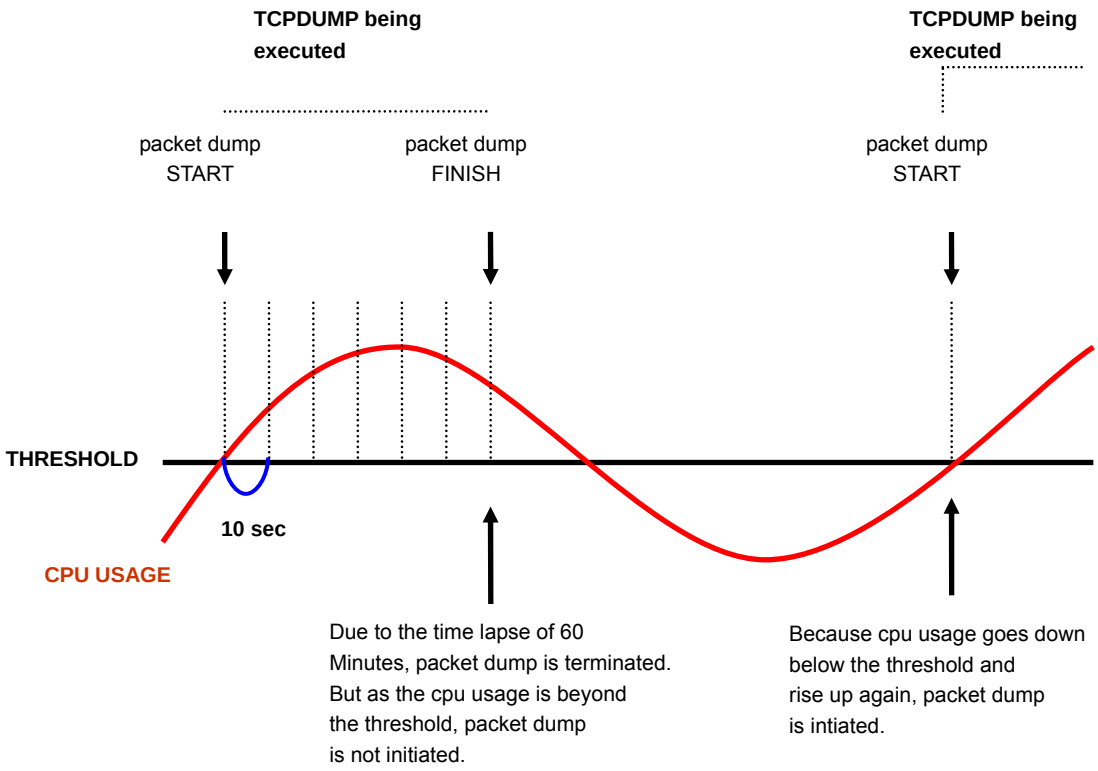
Compulsive termination has nothing to do with tcpdump command that is input by user. And after the termination, if the cpu usage is beyond the threshold, the switch consider it to be the similar traffic which had been already dumped and will not execute until the cpu usage is below the threshold.

Condition for inability of automatic execution

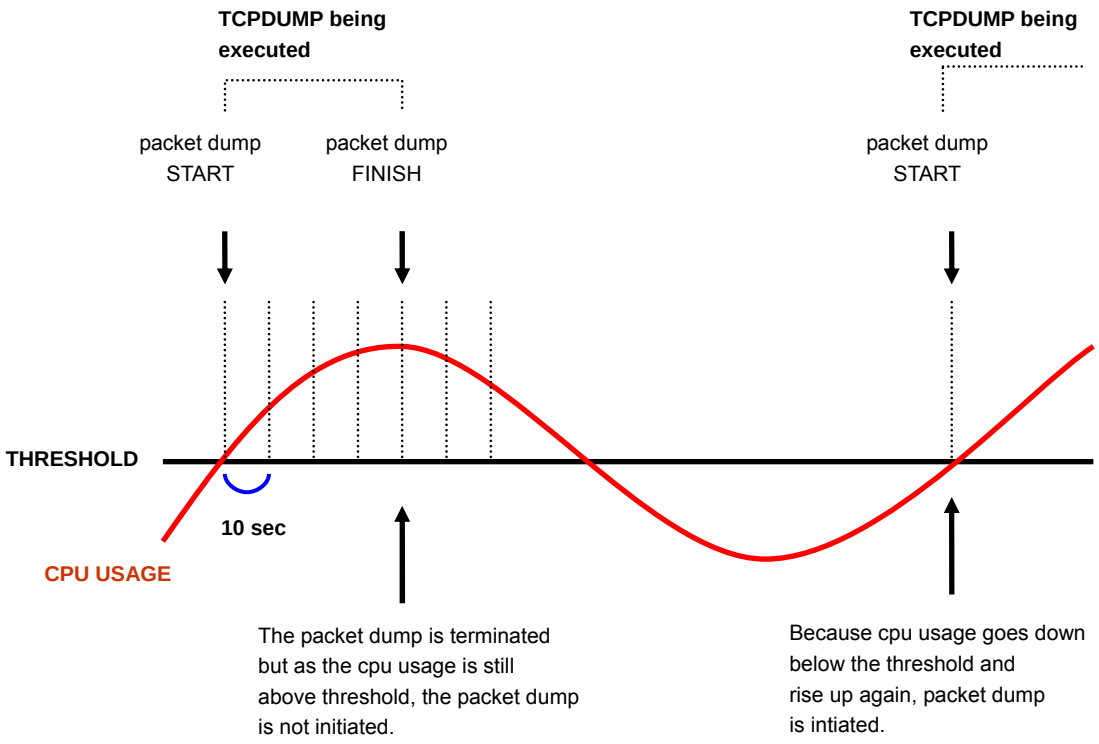
- When the automatically executed tcpdump is finished or terminated, if the cpu usage is still beyond the threshold, the system will not execute again tcpdump because it considers the traffic have not been changed (if the cpu usage would go down below the threshold and then rise up again above the threshold, tcpdump will be initiated.)
- If the threshold is set to 0, automatic execution will not be initiated.

The following descriptions are some examples of execution.

In case the tcpdump is automatically terminated because the number of arrived packets is below the predefined number for 60 second duration, and the cpu usage is beyond the threshold.



In case the tcpdump is compulsively terminated because the predefined number of packets have been received within 60 seconds (assuming the condition was reached after 40 seconds in this example), and after the termination the cpu usage is still above the threshold.



Config setting, initialization and referencing

<Table 142> Commands for setting, removing and referencing the threshold

Command	Description	Mode
dump traffic threshold <0-100>	To set the threshold for packet dump.	config
no dump traffic threshold	To initialize the threshold (set to '0')	config
dump traffic count <100-500>	To set the number of packets to dump per each execution.	config
no dump traffic count	To set the number of packets to dump to be 100 (default)	config
dump traffic interface INTERFACE	To configure interface for the packet dump.	config
no dump traffic interface	To configure interface to be any (e.g. all interface, this is default)	config
dump traffic enable	To activate the packet dump.	config
dump traffic disable	To disactivate packet dump.	config
show dump config	To display the threshold.	Privileged

The box below shows how a packet dump is executed when threshold is set to be 20. (in case the cpu usage is above 20, packet dump is to be initiated, and 100 packets will be dumped with respect to all interface.)

```
switch#
switch# configure terminal
switch(config)# dump traffic threshold 20
switch(config)# dump traffic enable
switch(config)# end
switch#
switch# show dump config
dump traffic threshold is 20
dump traffic count is 100
dump traffic interface is any
dump traffic is enabled
switch#
```

The following box shows an example how a packet dump is executed when threshold is 20, packet count is 500, and the interface is specified to be vlan1. One thing you note is the interface should be the ones that are eligible for assigning ip address (e.g. vlan, eth0).

```
switch#
switch# configure terminal
switch(config)# dump traffic threshold 20
switch(config)# dump traffic count 500
switch(config)# dump traffic interface vlan1
switch(config)# dump traffic enable
switch(config)# end
switch#
switch# show dump config
dump traffic threshold is 20
dump traffic count is 500
dump traffic interface is vlan1
dump traffic is enabled
switch#
```

The following box shows how the packet dump is disabled. Even when the threshold, count, or interface would be configured, packet dump is not initiated.

```
switch#
switch# configure terminal
switch(config)# dump traffic disable
switch(config)# end
switch#
switch# show dump config
dump traffic threshold is 20
dump traffic count is 500
dump traffic interface is vlan1
dump traffic is disable
switch#
```

The following box shows how the configuration is initialized.

```
switch#
switch# show dump config
dump traffic threshold is 20
dump traffic count is 500
dump traffic interface is vlan1
dump traffic is disabled
switch#
switch# configure terminal
switch(config)# no dump traffic threshold
switch(config)# no dump traffic count
switch(config)# no dump traffic interface
switch(config)# end
switch#
switch# show dump config
dump traffic threshold is 0
dump traffic count is 100
dump traffic interface is any
dump traffic is disabled
switch#
```

Displaying Log File

<Table 143> Displaying Log File

Command	Description	Mode
show dump-file FileName	To display the content of the specified log file.	privileged
show dump-file FileName OPTION	To display the content of the specified log file according to additive tcpdump option.	privileged

The packet dump file is saved in flash memory, and you can identify the file name and its created date by use of show flash command.

Example) pktdump_1(Jan 14 02:41:50)

```
Switch# show flash

-length- ----------type/info---------- CN path
4400546    1.0.0                          B* e32xx.r100
4157943    1.0.0                          -- e32xx.r100_bt
13315      text file                   -- pktdump_1(Jan 15 03:39:08)
976        text file                   B* config.txt

1480 Kbytes available (15294 Kbytes used)

Switch#
```

The following box shows how the file, ‘pktdump_1’ is referred.

```
switch#
switch# show dump-file pktdump_1
01:01:39.652358 [fa1(1)] 10.0.0.1 > 224.0.0.18: ip-proto-112 20
01:01:40.662453 [fa1(1)] 10.0.0.1 > 224.0.0.18: ip-proto-112 20
01:01:41.672519 [fa1(1)] 10.0.0.1 > 224.0.0.18: ip-proto-112 20
01:01:42.682603 [fa1(1)] 10.0.0.1 > 224.0.0.18: ip-proto-112 20
01:01:43.692650 [fa1(1)] 10.0.0.1 > 224.0.0.18: ip-proto-112 20
01:01:44.702824 [fa1(1)] 10.0.0.1 > 224.0.0.18: ip-proto-112 20
01:01:45.712877 [fa1(1)] 10.0.0.1 > 224.0.0.18: ip-proto-112 20
01:01:46.155500 [fa1(1)] 192.168.0.181 > 224.0.0.5: OSPFv2-hello 44: area 0.0.0.1 dr
192.168.0.181 [tos 0xc0] [ttl 1]
01:01:46.723229 [fa1(1)] 10.0.0.1 > 224.0.0.18: ip-proto-112 20
01:01:47.732996 [fa1(1)] 10.0.0.1 > 224.0.0.18: ip-proto-112 20
01:01:48.743046 [fa1(1)] 10.0.0.1 > 224.0.0.18: ip-proto-112 20
01:01:49.753138 [fa1(1)] 10.0.0.1 > 224.0.0.18: ip-proto-112 20
01:01:50.392509 [fa1(1)] 192.168.0.29.138 > 192.168.0.255.138: udp 201
01:01:50.763271 [fa1(1)] 10.0.0.1 > 224.0.0.18: ip-proto-112 20
01:01:51.773442 [fa1(1)] 10.0.0.1 > 224.0.0.18: ip-proto-112 20
01:01:52.783324 [fa1(1)] 10.0.0.1 > 224.0.0.18: ip-proto-112 20
01:01:53.793428 [fa1(1)] 10.0.0.1 > 224.0.0.18: ip-proto-112 20
01:01:54.803500 [fa1(1)] 10.0.0.1 > 224.0.0.18: ip-proto-112 20
01:01:55.813607 [fa1(1)] 10.0.0.1 > 224.0.0.18: ip-proto-112 20
01:01:56.156198 [fa1(1)] 192.168.0.181 > 224.0.0.5: OSPFv2-hello 44: area 0.0.0.1 dr
192.168.0.181 [tos 0xc0] [ttl 1]
01:01:56.824045 [fa1(1)] 10.0.0.1 > 224.0.0.18: ip-proto-112 20
01:01:57.833789 [fa1(1)] 10.0.0.1 > 224.0.0.18: ip-proto-112 20
```

Because the dumped packets are stored in the tcpdump raw file, you can only see the basic information when you display the file. Thus in order to retrieve other information you are supposed to use the tcpdump options as explained in section 12.1.4.

The following box shows how the file, pktdump_1 is referred by use of additional options.

```
switch# show dump-file tcpdump_19700116195734 ve
01:01:39.652358 [fa1(1)] 0:0:5e:0:1:1 1:0:5e:0:0:12 0800 54: 10.0.0.1 > 224.0.0.18: ip-
proto-112 20 (ttl 255, id 36074)
01:01:40.662453 [fa1(1)] 0:0:5e:0:1:1 1:0:5e:0:0:12 0800 54: 10.0.0.1 > 224.0.0.18: ip-
proto-112 20 (ttl 255, id 36075)
01:01:41.672519 [fa1(1)] 0:0:5e:0:1:1 1:0:5e:0:0:12 0800 54: 10.0.0.1 > 224.0.0.18: ip-
proto-112 20 (ttl 255, id 36076)
01:01:42.682603 [fa1(1)] 0:0:5e:0:1:1 1:0:5e:0:0:12 0800 54: 10.0.0.1 > 224.0.0.18: ip-
proto-112 20 (ttl 255, id 36077)
01:01:43.692650 [fa1(1)] 0:0:5e:0:1:1 1:0:5e:0:0:12 0800 54: 10.0.0.1 > 224.0.0.18: ip-
proto-112 20 (ttl 255, id 36078)
01:01:44.702824 [fa1(1)] 0:0:5e:0:1:1 1:0:5e:0:0:12 0800 54: 10.0.0.1 > 224.0.0.18: ip-
proto-112 20 (ttl 255, id 36079)
01:01:45.712877 [fa1(1)] 0:0:5e:0:1:1 1:0:5e:0:0:12 0800 54: 10.0.0.1 > 224.0.0.18: ip-
```

```
proto-112 20 (ttl 255, id 36080)
01:01:46.155500 [fa1(1)] 0:7:70:33:11:5 1:0:5e:0:0:5 0800 78: 192.168.0.181 > 224.0.0.5:
OSPFv2-hello 44: area 0.0.0.1 E mask 255.255.255.0 int 10 pri 1 dead 40 dr 192.168.0.181
nbrs [tos 0xc0] [ttl 1] (id 4346)
01:01:46.723229 [fa1(1)] 0:0:5e:0:1:1 1:0:5e:0:0:12 0800 54: 10.0.0.1 > 224.0.0.18: ip-
proto-112 20 (ttl 255, id 36081)
01:01:47.732996 [fa1(1)] 0:0:5e:0:1:1 1:0:5e:0:0:12 0800 54: 10.0.0.1 > 224.0.0.18: ip-
proto-112 20 (ttl 255, id 36082)
01:01:48.743046 [fa1(1)] 0:0:5e:0:1:1 1:0:5e:0:0:12 0800 54: 10.0.0.1 > 224.0.0.18: ip-
proto-112 20 (ttl 255, id 36083)
01:01:49.753138 [fa1(1)] 0:0:5e:0:1:1 1:0:5e:0:0:12 0800 54: 10.0.0.1 > 224.0.0.18: ip-
proto-112 20 (ttl 255, id 36084)
01:01:50.392509 [fa1(1)] 0:15:f2:27:e7:1 ff:ff:ff:ff:ff:ff 0800 243: 192.168.0.29.138 >
192.168.0.255.138: udp 201 (ttl 128, id 29631)
01:01:50.763271 [fa1(1)] 0:0:5e:0:1:1 1:0:5e:0:0:12 0800 54: 10.0.0.1 > 224.0.0.18: ip-
proto-112 20 (ttl 255, id 36085)
01:01:51.773442 [fa1(1)] 0:0:5e:0:1:1 1:0:5e:0:0:12 0800 54: 10.0.0.1 > 224.0.0.18: ip-
proto-112 20 (ttl 255, id 36086)
01:01:52.783324 [fa1(1)] 0:0:5e:0:1:1 1:0:5e:0:0:12 0800 54: 10.0.0.1 > 224.0.0.18: ip-
proto-112 20 (ttl 255, id 36087)
01:01:53.793428 [fa1(1)] 0:0:5e:0:1:1 1:0:5e:0:0:12 0800 54: 10.0.0.1 > 224.0.0.18: ip-
proto-112 20 (ttl 255, id 36088)
01:01:54.803500 [fa1(1)] 0:0:5e:0:1:1 1:0:5e:0:0:12 0800 54: 10.0.0.1 > 224.0.0.18: ip-
proto-112 20 (ttl 255, id 36089)
01:01:55.813607 [fa1(1)] 0:0:5e:0:1:1 1:0:5e:0:0:12 0800 54: 10.0.0.1 > 224.0.0.18: ip-
proto-112 20 (ttl 255, id 36090)
01:01:56.156198 [fa1(1)] 0:7:70:33:11:5 1:0:5e:0:0:5 0800 78: 192.168.0.181 > 224.0.0.5:
OSPFv2-hello 44: area 0.0.0.1 E mask 255.255.255.0 int 10 pri 1 dead 40 dr 192.168.0.181
nbrs [tos 0xc0] [ttl 1] (id 4347)
01:01:56.824045 [fa1(1)] 0:0:5e:0:1:1 1:0:5e:0:0:12 0800 54: 10.0.0.1 > 224.0.0.18: ip-
proto-112 20 (ttl 255, id 36091)
01:01:57.833789 [fa1(1)] 0:0:5e:0:1:1 1:0:5e:0:0:12 0800 54: 10.0.0.1 > 224.0.0.18: ip-
proto-112 20 (ttl 255, id 36092)
```

- ‘e’ option is for link-level header information.
- ‘v’ option is for TTL, identification, and total length.
- ‘t’ option is for timestamp.

Managing Log File

The maximum number of saved files for the log is 3. If the number of saved files would be over 3, then the oldest one shall be deleted before a new log file is created.

Chapter 12. DAI

This chapter describes the function of dynamic Address Resolution Protocol (ARP) inspection (DAI) which is used for inspecting ARP packet.

This chapter consists of the following sections:

- Understanding DAI
- Default DAI Configuration
- DAI Configuration Guidelines and Restrictions
- Configuring DAI
- DAI Configuration Samples

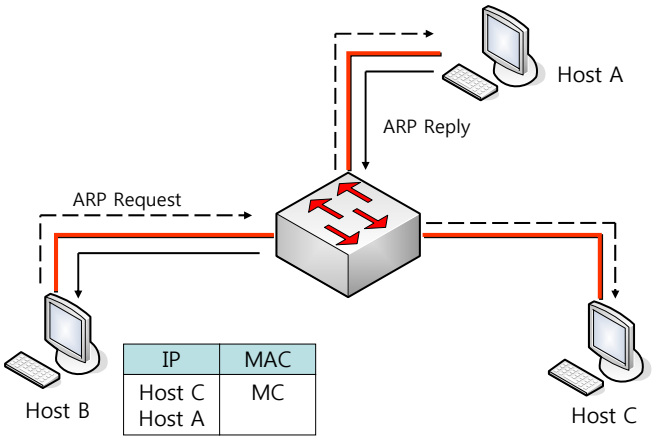
Understanding DAI

This section describes the basic function of DAI and the method to protect the ARP spoofing attack by using of DAI function. This section comprises following subsections.

- Understanding ARP
- Understanding ARP Spoofing Attacks
- Understanding DAI and ARP Spoofing Attacks
- Interface Trust States and Network Security
- Rate Limiting of ARP Packets
- Relative Priority of ARP ACLs and DHCP Snooping Entries
- Logging of Dropped Packets

Understanding ARP

ARP makes it possible to correlate IP address and MAC address by putting into a mapping table so that IP communication can be conducted within Layer 2 broadcast domain. For example, when host B wants to transmit data to host A, let's assume that there would be no registered information of host A within the ARP table in host B.

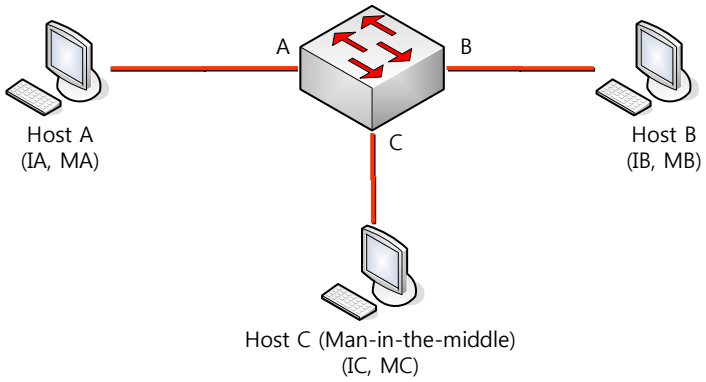


In order for host B to find out the MAC address for host A's IP address, host B sends out broadcast massage (ARP request) to all the hosts in the broadcast domain. Then all the hosts in the broadcast domain shall receive the ARP request which was sent by host B and host A will reply to host B with its MAC address.

Understanding ARP Spoofing Attacks

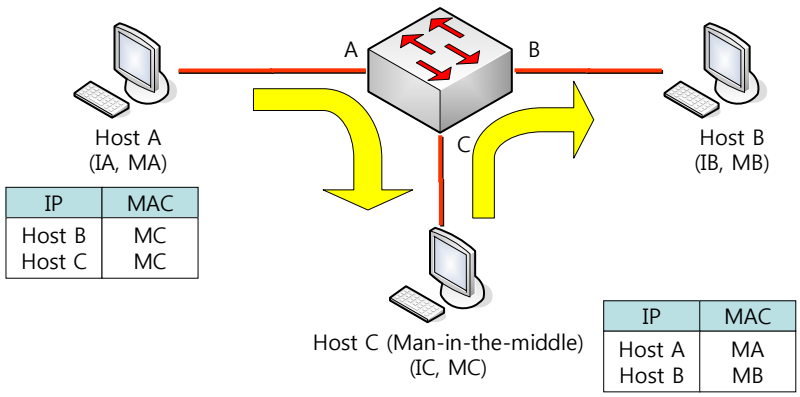
ARP unintentionally gets to have ARP table changed by the gratuitous reply which is sent by a host who has not received ARP request. Due to this defect, the ARP spoofing attack or ARP cache poisoning might happen. After this attack, the traffic of the victimized switch shall be transferred to other routers, switches or hosts via the attacker's computer.

ARP spoofing attack affects the ARP cache of the host, switch, or router which are connected in the Layer 2 network. And it intercepts the traffics which are intended for other network. The following figure shows the example of ARP cache poisoning.



Host A, B and C are interconnected through the interfaces A, B, and C of the switch centered in the picture, and they are all in same subnet. The IP address and MAC address are shown in parenthesis in the figure. For example, host A uses IP address, 'IA' and MAC address, 'MA'. When host A needs to communicate with host B in IP layer, in order to know the related MAC address of IP address 'IB' it sends out ARP request in broadcast manner. And if the switch and host B receive the ARP request, they update their ARP cache so as to replace the IP address IA and MAC address MA with latest values.

Host C may pollute the ARP cache of host A and host B by which it sends out broadcasted ARP response that includes the faked MAC address, 'MC' at here for IP address IA (or IB). The host that has a polluted ARP cache shall use the MAC address of MC as the destination for the traffic which is intended to be heading for IA or IB. This means that host C intercepts the traffic. Host C knows the genuine MAC address of IA and IB, it can forward the intercepted traffic by inserting the right MAC address to the originally targeted host. Thus host C is placed in between host A and host B, and we call this symptom as '*man-in-the middle* attack'.



Understanding DAI and ARP Spoofing Attacks

DAI is a security function that is used to check out ARP packet. DAI inspects invalid IP-to-MAC address binding and drop the ARP packet after logging the relevant information. This feature protects network from the main-in-the-middle attack.

DAI makes sure the ARP table be changed only by valid ARP request and response. The switch that is enabled for DAI function behaves as the following:

- Check out and inspect all ARP packets that come through the untrusted ports.
- Check out the received packets whether it has the valid IP-to-MAC address binding before updating its own ARP cache.
- Drop the invalid ARP packets.

When DAI checks out the validity of ARP packet, it utilizes the reliable data in the DHCP snooping binding database.

Note When switch and VLAN are enabled for DHCP snooping, by DHCP snooping the DHCP snooping binding database is created.

Switch behaves as follow according to the characteristics of the interface which receives the ARP packet:

- Switch does not inspect the ARP packet that come through the trusted interface.
- Switch permits only the valid packets in case the packets have arrived through the untrusted interface.

DAI may use ARP access control lists (ACLs) which administrator has defined with respect to a host that has statically assigned IP address. The switch may leave a log for the discarded packets.

In case of following condition, DAI may be configured to discard ARP packets:

- When the IP address of the packets are invalid – for example 0.0.0.0, 255.255.255.255 or IP multicast address.
- When the MAC address in ARP packet body and the address of Ethernet header is not consistent.

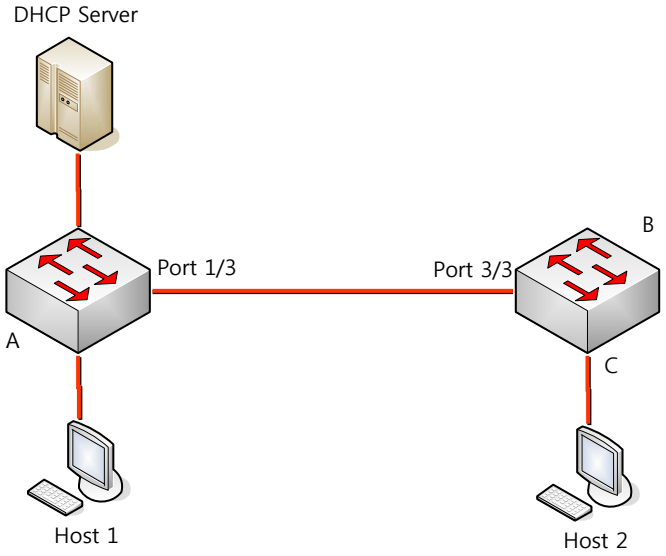
Interface Trust States and Network Security

DAI basically maintains the information of trust status of each interface in the switch. With respect to the packets that come through the trusted interface, DAI will not take any forms of DAI inspection. On the contrary, for the packets from Untrusted interface, DAI inspection will duly take place.

In a typical network formation, the switch ports which are connected to a host are to be configured as ‘untrusted’ and the switch ports to another switch are to be configured as ‘trusted’. In this configuration, all the coming ARP packets into the switch will be inspected. And no more validity inspections in VLAN or other network segment will be needed. To configuring trust setting, you can use the command ‘**ip arp inspection trust’**.

Caution For security check purpose, if you want to have the switch inspect all the ARP packets, a particular function is required. That is to say, DAI should be able to have the switch CPU get trapped to process the inspection work. This trap functions are basically dependant upon individual platform.

In the figure below, consider that the DAI would be enabled for the VLAN which contains host 1 and host 2 of switch A and switch B respectively. If host 1 and host 2 have been assigned IP address from the DHCP server that is connected to switch A, then only switch A has the IP-to-MAC address mapping information for host 1. Therefore, if the interface between switch A and switch B would be untrusted, then the ARP packet that host 1 has sent out will be discarded at switch B. Thus, host 1 and host 2 cannot communicate each other.



If there would be any unreliable device within the network when an interface is set to be trusted, there could be a certain kinds of security defects. If DAI is not enabled in switch A, host 1 might pollute the ARP cache of switch B (And if the interface between the switches is set to trusted, then as many as including host 2). This kind of anomaly would happen even when DAI in switch B is in active.

A switch that is enabled to execute DAI prevents its connected hosts from polluting other host's ARP cache. However, DAI is not able to prevent the unwanted pollution that might affect other hosts which are in DAI active.

In this case, you need to configure the interface between DAI-enabled switch and DAI-disabled switch to be untrusted. And to make sure to inspect the packets from the DAI-disabled switch, you need to set the ARP ACLs in DAI-enabled switch. If this configuration would be unable to be set, you ought to separate switches as to whether it uses DAI or not.

Note E3208E supports the DAI features that inspect all ARP packets.

Rate Limiting of ARP Packets

The DAI-enabled switch will control the number of ARP packets that come into the switch CPU. As a default value, with respect to untrusted interface, 15 ARP packets per second (15 pps) are allowed meanwhile there is no limitation on the rate for trusted interface. You can configure the setting by use of the command **ip arp inspection limit**.

If the rate of ARP packets at a specified port would be over the predefined value, the switch will discard all the received ARP packets at the port. This behavior shall be maintained until user would change the configuration. By use of the command **ip arp inspection limit auto-recovery**, you can make the port get back to available status after a certain amount of time.

Note The rate limit function toward ARP packets are performed at CPU in software manner, you cannot count on it for Denial-of-Service (DoS) attack.

Relative Priority of ARP ACLs and DHCP Snooping Entries

When DAI checks out the IP-to-MAC address mapping, it used DHCP snooping binding database.

ARP ACLs are used for inspection before DHCP snooping binding database. The switch will use ACL only when it is configured by '**ip arp inspection filter'** command. The switch will inspect ARP packets with ARP ACLs. If the ARP packet is consistent with the deny condition of ARP ACLs, the packet will be discarded even when there is valid binding that has been made by valid DHCP snooping.

Logging of Dropped Packets

The switch will keep the information about the discarded packets at log buffer and generate system message according to the ratio that has been set in advance. Once the message is generated, the corresponding information at the log buffer will be deleted. In each log there are the flow information including received VLAN id, port number, source and destination IP address, source and destination MAC address.

By use of global configuration command '**ip arp inspection log-buffer'** you can adjust the size of buffer and number of log per unit time so as to control the total volume of created messages. And with the global configuration command '**ip arp inspection vlan loggin**g' you can specify the type of packets to log.

Default DAI Configuration

The following table shows the default DAI configuration.

<Table 144> Default DAI Configuration

Feature	Default Setting
DAI	'Inactive' for all VLAN.
Interface trust state	'Untrusted' for all interfaces.
Rate limit of incoming ARP packets	15 pps for untrusted interfaces. In case of Trusted interfaces, there is no limitation on rate. Burst interval is 1second. The rate limit for interfaces is in 'Disabled' status.
ARP ACLs for non-DHCP environments	ARP ACLs is not defined.
Validation checks	No inspection is to be conducted.
Log buffer	When DAI is enabled, all ARP packet which is denied or dropped will be logged. The number of log entry is 32. The number of system message generated is 5 per second. The period of logging-rate 1 second .
Per-VLAN logging	All ARP packet which is denied or dropped will be logged.

DAI Configuration Guidelines and Restrictions

When DAI is configured, you have to keep the followings in mind:

DAI basically takes care of the ARP table only in the switch. As a better method to protect whole network, the trap function which will have ARP packet to be processed in CPU.

DAI is intended to be used as an ingress security tool. You ought not to use it at an egress port.

DAI is not effective for the hosts that are connected to the DAI-disenabled switch. As the man-in-the-middle attack is confined to a single Layer 2 broadcast domain, you ought to seperate a domain which adopts DAI from other domains which don't use DAI. This will make sure that the ARP table of the switch that are in DAI activated domain.

DAI uses the DHCP snooping binding database in order to check the IP-to-MAC address binding of the coming ARP request and ARP response packets. To allow the ARP packets which will have dynamically assigned IP address, you ought to activate DHCP snooping.

Note In case DAI is in use together with DHCP server, it can use the binding information of the DHCP server.

If DHCP snooping is inactive or DHCP is not in use, then you can utilize ARP ACL to permit or deny packets.

Configure to set the rate of ARP packets considering the characteristics of the port.

Configuring DAI

In this section, the way to configure DAI is explained:

- Enabling DAI on VLANs (Mandatory)
- Configuring the DAI Interface Trust State (Optional)
- Applying ARP ACLs for DAI Filtering (Optional)
- Configuring ARP Packet Rate Limiting (Optional)
- Enabling DAI Error-Disabled Recovery (Optional)
- Enabling Additional Validation (Optional)
- Configuring DAI Logging (Optional)
- Displaying DAI Information

Enabling DAI on VLANs

When DAI is enabled for a VLAN, the switch will inspect the ARP packet that come through the VLAN as following:

- Broadcasted ARP
- ARP request packets that ask for switch's MAC address.
- Reply packets that answer to the requesting ARP request.
- All unicast ARP packets that are transferred among terminals.

After checking out these packets, it only replies to the valid packets and updates the ARP table.

To make DAI work on a VLAN, execute the following commands:

<Table 145> Enabling DAI on VLANs

Command	Purpose
Switch# **configure terminal**	To get in global configuration mode.
Switch(config)# **ip arp inspection vlan** *vlan-id* Switch(config)# **no ip arp inspection vlan** *vlan-id*	To enable DAI on a VLAN. To disable DAI from a VLAN.
Switch# **show ip arp inspection**	To check out current setting.

Note When you enable DAI on a VLAN, all the ARP packets that flow through the VLAN will be inspected. In other words, the ARP cache of the switch and network are to be protected.

The following example shows how to enable DAI on VLAN 200:

```
Switch# configure terminal
Switch(config)# ip arp inspection vlan 200
```

The following example shows how to retrieve current settings:

```
Switch# show ip arp inspection
DHCP Snoop Bootstrap            : Disabled
Source MAC Validation           : Disabled
Destination MAC Validation : Disabled
IP Address Validation           : Disabled
ARP Field Validation            : Disabled
Vlan    Config      Operation   ACL Match                 Static ACL   ACL Log     DHCP Log
----    --------    ---------   --------------------      ----------   ---------   --------
 200    Enabled     Active+                               No           Deny        Deny
```

Configuring the DAI Interface Trust State

Switch will not inspect the ARP packets that come through the trusted interface.

The received ARP packets that come through the untrusted interface will be inspected to verify whether it has valid IP-to-MAC address mapping. Switch will discard invalid packets and save a packet log in log buffer by use of '**ip arp inspection vlan logging'** command.

In order to configure the trust status of an interface, the following are to be executed:

<Table 146> Configuring the DAI Interface Trust State

Command	Purpose
Switch# **configure terminal**	To get in global configuration mode.
Switch(config)# **interface** *ifname*	To specify the interfaces that are connected to other switches and also get in the mode of configuring interface.
Switch(config-if-fa1/1)# **ip arp inspection trust** Switch(config-if-fa1/1)# **no ip arp inspection trust**	To configure the interface to be trusted. (default: untrusted) To configure the interface to be untrusted.
Switch(config-if-fa1/1)# **end**	To get back to Enable mode.
Switch# **show ip arp inspection interfaces**	To retrieve current settings.

The following example shows how to configure Fast Ethernet port 2/1 to be set as a trusted port:

```
Switch# configure terminal
Switch(config)# interface fa2/1
Switch(config-if-fa2/1)# ip arp inspection trust
Switch(config-if-fa2/1)# end
Switch# show ip arp inspection interfaces
Interface          Trust State    Rate (pps)    Burst Interval    Auto Recovery
---------------    -----------    ----------    --------------    -------------
fa2/1              Trusted        None          1                 Disabled
fa2/2              Untrusted      15            1                 Disabled
```

Applying ARP ACLs for DAI Filtering

To utilize ARP ACL feature, the following steps are to be executed:

<Table 147> Applying ARP ACLs for DAI Filtering

Command	Purpose
Switch# **configure terminal**	To get in global configuration mode.
Switch(config)# **ip arp inspection filter** *arp_acl_name* **vlan** *vlan-id* [**static**]	To apply ARP ACL to a VLAN.
Switch(config)# **end**	To get back to Enable mode.
Switch# **show ip arp inspection**	To retrieve current settings.

The following example shows how to apply the ARP ACL whose name is example_arp_acl to VLAN 200:

```
Switch# configure terminal
Switch(config)# ip arp inspection filter example_arp_acl vlan 200
Switch(config)# end
Switch# show ip arp inspection
DHCP Snoop Bootstrap           : Disabled
Source MAC Validation          : Disabled
Destination MAC Validation : Disabled
IP Address Validation          : Disabled
ARP Field Validation           : Disabled
Vlan   Config      Operation   ACL Match                Static ACL   ACL Log     DHCP Log
----   --------    ---------   ---------------------    ----------   ---------   --------
 200   Enabled     Active      example_arp_acl          No           Deny        Deny
```

Configuring ARP Packet Rate Limiting

Once DAI is enabled then all ARP packets are to be inspected, which will take a lot of CPU capability. Then consequently the switch will be vulnerable to the DoS attack which mainly bombarded ARP packets. Thus by putting a certain amount of limitation on the CPU it can control the amount of ARP packets to be processed rate and lessen the burden of CPU.

	Note	The ARP rate limit that is provided by DAI is a software feature, so it cannot control the usage rate of CPU in direct measure. However by reducing the ARP packets which are to be handled by DAI, the CPU usage rate by DAI can be lowered.

To configure the rate limit upon ARP packets for a port, the following steps are to be executed:

<Table 148> Configuring ARP Packet Rate Limiting

Command	Purpose
Switch# **configure terminal**	To get in global configuration mode.
Switch(config)# **interface** *ifname*	To specify the interfaces that are connected to other switches and also get in the mode of configuring interface.
Switch(config-if-fa1/1)# **ip arp inspection limit** {**rate** *pps* [**burst interval** *seconds*] **| none**} Switch(config-if-fa1/1)# **no ip arp inspection limit**	(Optional) To set the rate limit upon ARP packet. To get back to default configuration.
Switch(config-if-fa1/1)# **ip arp inspection limit enable** Switch(config-if-fa1/1)# **no ip arp inspection limit enable**	To enable the ARP rate limit of an interface. To disable the ARP rate limit of an interface .
Switch(config)# **end**	To get back to Enable mode.
Switch# **show ip arp inspection interfaces**	To retrieve current settings.

When you configure the ARP packet rate limit, you have to keep the followings in mind:

- Default value for untrusted interface is 15 pps (packet per second), and for trusted interface is no limitation at all.
- **rate** is the upper limit value in terms of *pps* which may have between 0 to 2048.
- **rate none** means there is no limitation on the rate of received ARP packets.
- (Optional) **burst interval** *seconds* (default is 1) is the time duration for which the system will watch to see if ARP packet rate is over the upper limit. Thus, if the value of **rate** is reached during the time lapse of **burst interval** , then the incoming ARP packets will be restricted. The range is 1 ~ 15.
- If the incoming ARP packet rate is over the predefined value, the switch will discard all the received ARP packets at the port. This setting will be maintained until the operator would change the setting.
- While the rate-limit of an interface is not changed, if the trust status of an interface is changed, then the default value of the rate-limit of an interface will be changed. Once rate-limit value is changed, then even though the trust status would be changed, the configured value will be maintained. By use of the command '**no ip arp inspection limit'** the rate-limit of an interface will be returned to default value.
- After configuring by use of the command '**ip arp inspection limit enable'** the rate limit for ARP packet will be activated.

The following example shows how to configure ARP packet rate limit upon fa2/1 port.

```
Switch# configure terminal
Switch(config)# interface fa1
Switch(config-if-fa2/1)# ip arp inspection limit rate 20 burst interval 2
Switch(config-if-fa2/1)# ip arp inspection limit enable
Switch(config-if-fa2/1)# end
Switch# show ip arp inspection interfaces
Interface          Trust State    Rate (pps)   Burst Interval   Auto Recovery
---------------    -----------    ----------   --------------   -------------
fa1                Untrusted          20               2          Disabled
fa2                Untrusted          15               1          Disabled
```

Enabling DAI Error-Disabled Recovery

To restore the restricted port, which has been restricted due to rate limit for ARP packets, to normal the following steps are to be executed:

<Table 149> Enabling DAI Error-Disabled Recovery

Command	Purpose
Switch# **configure terminal**	To get in global configuration mode.
Switch(config)# **interface** *ifname*	To specify the interfaces that are connected to other switches and also get in the mode of configuring interface.
Switch(config-if-fa1/1)# **ip arp inspection limit auto-recovery** *seconds* Switch(config)# **no ip arp inspection limit auto-recovery**	(Optional) To enable the automatic recovery function. To disable the automatic recovery function.
Switch(config)# **end**	To get back to Enable mode.
Switch# **show ip arp inspection interfaces**	To retrieve current settings.

The following example shows how to restore the interface fa2/1 to normal automatically after 10 seconds:

```
Switch# configure terminal
Switch(config)# interface fa2/1
Switch(config-if-fa2/1)# ip arp inspection limit auto-recovery 10
Switch(config-if-fa2/1)# ip arp inspection limit enable
Switch(config-if-fa2/1)# end
Switch# show ip arp inspection interfaces
Interface          Trust State    Rate (pps)   Burst Interval   Auto Recovery
---------------    -----------    ----------   --------------   -------------
fa2/1              Untrusted          20               2              10
fa2/2              Untrusted          15               1          Disabled
```

Enabling Additional Validation

DAI can verify the validity of ARP packet's destination MAC address, sender and target IP address, source MAC address.

For validity check for IP address or MAC address, the following steps are to be executed:

<Table 150> Enabling Additional Validation

Command	Purpose
Switch# **configure terminal**	To get in global configuration mode.
Switch(config)# **ip arp inspection validate** {**dst-mac** | **ip** | **src-mac**} Switch(config)# **no ip arp inspection validate** {**dst-mac** | **ip** | **src-mac**}	(Optional) To enable additive validity check. (default: none) To disable additive validity check.
Switch(config)# **end**	To get back to Enable mode.
Switch# **show ip arp inspection**	To retrieve current settings.

To enable additive validity check, you have to keep the followings in mind:

- At least one keyword among the options ought to be used.
- Each '**ip arp inspection validate'** command nullify the former command. If, **ip arp inspection validate** command has enabled **src-mac** and **dst-mac** inspection first, and then the second command '**ip arp inspection validate'** enables only **ip** inspection, then the **src-mac** and **dst-mac** inspection will be disabled and only the **ip** inspection will be in its effect.
- Additive validity inspections according to command arguments are as below:

  - **dst-mac** – With respect to the ARP response packet, it makes comparison between the destination MAC address in Ethernet header and the target MAC address in ARP body.

  - **ip –** It checks out the invalid IP address in ARP body. Thus addresses like 0.0.0.0 or 255.255.255.255 or multicast IP address will be discarded. It also verifies the sender IP address of ARP request and the sender/target IP address of ARP response.

  - **src-mac** – With respect to all ARP packets, it makes comparison between the source MAC address in Ethernet header and the sender MAC address in ARP body.

The following example shows how to enable the additive validity inspection as to the command argument 'src-mac':

```
Switch# configure terminal
Switch(config)# ip arp inspection validate src-mac
Switch(config)# end
Switch# show ip arp inspection
DHCP Snoop Bootstrap          : Disabled
Source MAC Validation         : Enabled
Destination MAC Validation : Disabled
IP Address Validation         : Disabled
ARP Field Validation          : Disabled
Vlan   Config      Operation   ACL Match                Static ACL   ACL Log     DHCP Log
----   --------    ---------   --------------------     ----------   ---------   --------
 200   Enabled     Active                               No           Deny        Deny
```

The following example shows how to enable the additive validity inspection as to the command argument 'dst-mac':

```
Switch# configure terminal
Switch(config)# ip arp inspection validate dst-mac
Switch(config)# end
Switch# show ip arp inspection
DHCP Snoop Bootstrap           : Disabled
Source MAC Validation          : Disabled
Destination MAC Validation : Enabled
IP Address Validation          : Disabled
ARP Field Validation           : Disabled
Vlan   Config      Operation   ACL Match                 Static ACL   ACL Log     DHCP Log
----   --------    ---------   --------------------   ----------   --------- --------
 200   Enabled     Active                                No           Deny        Deny
```

The following example shows how to enable the additive validity inspection as to the command argument ‘ip’:

```
Switch# configure terminal
Switch(config)# ip arp inspection validate ip
Switch(config)# end
Switch# show ip arp inspection
DHCP Snoop Bootstrap           : Disabled
Source MAC Validation          : Disabled
Destination MAC Validation : Disabled
IP Address Validation          : Enabled
ARP Field Validation           : Disabled
Vlan   Config      Operation   ACL Match                 Static ACL   ACL Log     DHCP Log
----   --------    ---------   --------------------   ----------   --------- --------
 200   Enabled     Active                                No           Deny        Deny
```

The following example shows how to enable the additive validity inspection as to the command arguments ‘src-mac’ and ‘dst-mac’ :

```
Switch# configure terminal
Switch(config)# ip arp inspection validate dst-mac src-mac
Switch(config)# end
Switch# show ip arp inspection
DHCP Snoop Bootstrap           : Disabled
Source MAC Validation          : Enabled
Destination MAC Validation : Enabled
IP Address Validation          : Disabled
ARP Field Validation           : Disabled
Vlan   Config      Operation   ACL Match                 Static ACL   ACL Log     DHCP Log
----   --------    ---------   --------------------   ----------   --------- --------
 200   Enabled     Active                                No           Deny        Deny
```

Configuring DAI Logging

The explanation about DAI logging feature is presented in this section, which is consisted of as below:

- DAI Logging Overview
- Configuring the DAI Logging Buffer Size
- Configuring the DAI Logging System Messages
- Configuring DAI Log Filtering

DAI Logging Overview

Switch saves the information about the discarded packets into log buffer and generates system message according to the pre-configured generation rate. Once the message is generated, the related information in the log buffer shall be deleted. Each log has the flow information like the received VLAN id, port number, source and destination IP address, source and destination MAC address.

Any one log buffer entry can hold information about more than one packet. For example, if there come a lot of packets through a same interface which have same ARP parameters and VLAN id, DAI will create a log buffer entry for these packets and generate a system message.

Configuring the DAI Logging Buffer Size

To adjust the size of DAI log buffer, you need to execute the following steps:

<Table 151> Configuring the DAI Logging Buffer Size

Command	Purpose
Switch# **configure terminal**	To get in global configuration mode.
Switch(config)# **ip arp inspection log-buffer entries** *number* Switch(config)# **no ip arp inspection log-buffer entries**	To set the size of DAI log buffer (range: 0 ~ 1024). To return to default value (The default size: 32)
Switch(config)# **end**	To get back to Enable mode.
Switch# **show ip arp inspection log**	To retrieve current settings.

The following example shows how to adjust the size of DAI log buffer to be 64:

```
Switch# configure terminal
Switch (config) # ip arp inspection log-buffer entries 64
Switch (config) # end
Switch# show ip arp inspection log
Total Log Buffer Size: 32
Syslog rate: 5 entries per 1 seconds.
No entries in log buffer.
```

Configuring the DAI Logging System Messages

To configure the log message that DAI generates, you need to execute the following steps:

<Table 152> Configuring the DAI Logging System Messages

Command	Purpose
Switch# **configure terminal**	To get in global configuration mode.
Switch(config)# **ip arp inspection log-buffer logs** *number_of_messges* **interval** *length_in_seconds* Switch(config)# **no ip arp inspection log-**	To configure the DAI log buffer. To return to default value.

buffer logs	
Switch(config)# **end**	To get back to Enable mode.
Switch# **show ip arp inspection log**	To retrieve current settings.

When you configure the logging system message of DAI, you have to be aware of the followings:

- As to '**logs** *number_of_messges'*, the range of value is 0 ~ 1024, and default is 5. If you set it to be 0, then log message will not be generated.
- As to '**interval** *length_in_seconds'*, the range of value is 0 ~ 86400 (one day), and default is 1. If you set it to be 0, then log message will be generated immediately (Thus, the log buffer is empty constantly).
- The system log message shall be generated in the ratio of '*number_of_messages'* times *per 'length_in_seconds'* duration.

The following example shows how to configure to generate 12 DAI log messages per every 2 seconds:

```
Switch# configure terminal
Switch(config)# ip arp inspection log-buffer logs 12 interval 2
Switch(config)# end
Switch# show ip arp inspection log
Total Log Buffer Size: 32
Syslog rate : 12 entries per 2 seconds.
No entries in log buffer.
```

Configuring the DAI Log Filtering

After inspecting the ARP packets, you can selectively collect the result of the inspection so as to generate the system message.

To configure the log filtering function for DAI, execute the following steps:

<Table 153> Configuring the DAI Log Filtering

Command	Purpose
Switch# **configure terminal**	To get in global configuration mode.
Switch(config)# **ip arp inspection vlan** *vlan-id* {**acl-match** {**matchlog** | **none**} | **dhcp-bindings** {**all** | **none** | **permit**}}	To apply the log filtering to a VLAN.
Switch(config)# **end**	To get back to Enable mode.
Switch# **show running-config**	To retrieve current settings.

When you configure the logging system message of DAI you have to be aware of the followings:

- All the denied packets will be logged as Default.
- **acl-match matchlog** — it makes logging work based upon ACL setting. If '**matchlog'** is specified and '**log'** keyword is used in the **permit** or **deny** command of ARP access-list configuration, the ARP packets that are permitted or denied by ACL will be logged.
- **acl-match none** — it will NOT log for the packets that are consistent with ACL.
- **dhcp-bindings all** — it will do log for the packets that are consistent with DHCP binding.
- **dhcp-bindings none** — it will NOT log for the packets that are consistent with DHCP binding.
- **dhcp-bindings permit** — it will do log for the packets that are allowed by DHCP binding.

The following example shows how to configure not to generate log message for the packets that are consistent with ACL:

```
Switch# configure terminal
Switch(config)# ip arp inspection vlan 200 logging acl-match none
Switch(config)# end
Switch# show ip arp inspection
DHCP Snoop Bootstrap            : Disabled
Source MAC Validation           : Disabled
Destination MAC Validation : Disabled
IP Address Validation           : Disabled
ARP Field Validation            : Disabled
Vlan    Config       Operation    ACL Match                 Static ACL    ACL Log      DHCP Log
----    --------    ---------    --------------------    ----------    --------- --------
 200    Enabled      Active                                    No             None         Deny
```

Displaying DAI Information

To retrieve the information about DAI, use the following commands:

<Table 154> Displaying DAI Information

Command	Description
show arp access-list	To display the information about ARP ACL.
show ip arp inspection interfaces	To display the trust status of the interface.
show ip arp inspection vlan [*vlan-id*]	To display the DAI configuration and its behavior of a VLAN.
show ip arp inspection arp-rate	To display the rate information of ARP packet reception in the interface.

To display or initialize the DAI statistics, use the following commands:

Command	Description
clear ip arp inspection statistics	To initialize DAI statistics.
show ip arp inspection statistics [**vlan** *vlan-id*]	To display the DAI statistics about ARP packets.

To display or initialize the DAI logging information, use the following commands:

Command	Description
clear ip arp inspection log	To initialize DAI log buffer.
show ip arp inspection log	To display the configuration and content of DAI log buffer.

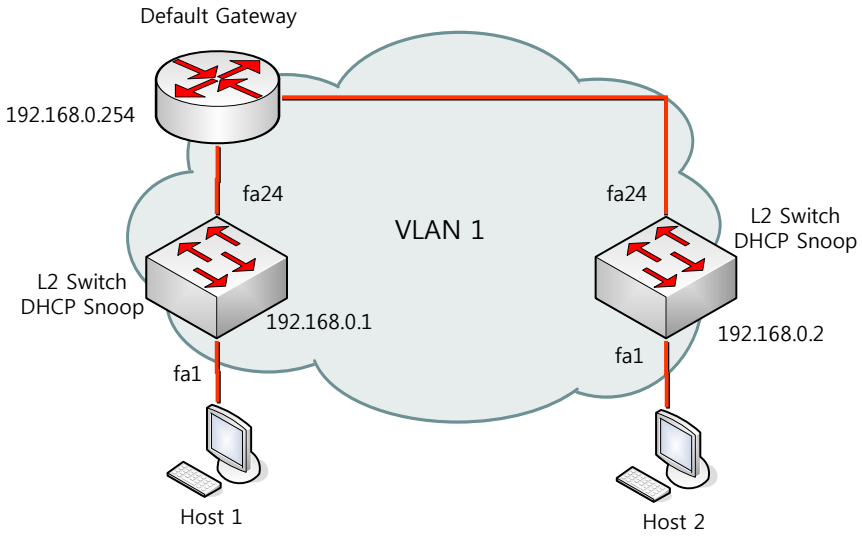
DAI Configuration Samples

This section includes the following example:

- Sample One: Interoperate with DHCP Snoop

Sample One: Interoperate with DHCP Snoop

This example explains how you can configure DAI upon a switch that uses DHCP snoop function. Consider the network in the figure below:



Caution In order to use DAI in a L2 switch that has hosts, you ought make sure all the associated L2 switches are in use of DAI. If there is any one L2 switch that does not support DAI, there might be communication error.

The L2 switch that is enabled for DHCP snoop is connected with the Default gateway and other L2 switch or hosts in same VLAN. The L3 switch and L2 switch use permanent IP address. Meanwhile host 1 and host 2 are assigned IP addresses via DHCP.

Note In this network composition, DAI is solely dependant upon DHCP snooping binding information to get the IP-to-MAC binding information.

In order to use DAI function in a switch that is enabled for DHCP snoop function, you need to configure it as the following steps:

<Table 155> Enabled for DHCP Snoop Function

Step 1	**Activate DHCP snooping within VLAN 1 to build up the IP-to-MAC binding information of a host.** Switch# **configure terminal**

	Switch(config)# **ip dhcp snooping vlan 1** Switch(config)# **ip dhcp snooping**
Step 2	**Configure the port where the switch is connected to be 'Trust port'. All the ARP packets that come through the Trust port shall be permitted always.** Switch# **configure terminal** Switch(config)# **interface fa24** Switch(config-if-fa24)# **ip arp inspection trust**
Step 3	**Activate DAI upon VLAN 1.** Switch# **configure terminal** Switch(config)# **ip arp inspection vlan 1** Switch(config)# **end** To identify that the configuration has been set correctly. Switch# **show ip arp inspection vlan 1**
Step 4	**Create flow rule and policy map to block ARP packets.** Switch# **configure terminal** Switch(config)# **flow-rule arp classify ethertype 0806** Switch(config)# **flow-rule arp match drop** Switch(config)# **flow-rule arp match trap-cpu** Switch(config)# **policy-map arp-trap flow-rule arp** Switch(config)# **end**
Step 5	**Apply the flow rule to the port that is connected to host.** Switch# **configure terminal** Switch(config)# **service-policy fa1 ingress arp-trap** Switch(config)# **end**

Chapter 13. Auto-Reset

This chapter describes how to set reset function when equipment has specific situation or some problem.

Auto-reset

This section describes how to set reset function when equipment has specific situation or some problem.

Understanding Auto-reset

It may happen that the system does not run normal because the unexpected case occurs on running system.

Auto-reset function looks into the reasons to occur the problem. When it comes out, this function resets equipment automatically.

To look into the condition for auto-reset, the reasons are as follows:

1. High CPU utilization (%)
2. low free_memory (%) resulting from the use of high memory
3. Network function problem.
4. Process Non-Operating

Because the above items come out the critical effects for normal system running, they are used for condition to run auto-reset.

Default Auto-reset Configuration

The following table shows the default setting of auto-reset.

<Table 156> Default Auto-reset Configuration

Feature	Default Setting
Auto-reset by Config Set	Disable
Auto-reset by Cpu Threshold	Disable
Auto-reset by Memory Threshold	Disable
Auto-reset by GateWay Ping Threshold	Disable
Auto-reset by Process-monitor	Disable
Auto-reset by CPU-Network	Disable
Auto-reset by Max Limit Count	Disable
Auto-reset by force-reboot	Disable

Configuring auto-reset

This section describes how to set auto-reset function to the switch.

- Enabling auto-reset by Config Set
- Enabling auto-reset by Cpu Threshold
- Enabling auto-reset by Memory Threshold
- Enabling auto-reset by GateWay Ping Threshold
- Enabling auto-reset by Process Monitor
- Enabling auto-reset by CPU-Network Threshold
- Enable auto-reset by Max Limit Count
- Enable auto-reset by force-reboot

Enabling auto-reset by Config Set

To enable auto-reset function, do the following procedure in privileged EXEC mode.

If you do not enable, the auto-reset function does not work about cpu, memory and process.

<Table 157> Enabling auto-reset by Config Set

		Command	Purpose
Step1		*Configure terminal*	Enters Global configuration mode Enters the Global configuration.
Step2		**Auto-reset enable**	Enables auto-reset function.
Step3		**End**	Changes privileged EXEC mode. Changes privileged EXEC mode.
Step4		**show auto-reset status**	Shows the setting. Shows the setting
Step5		**copy running-config startup-config**	Saves setting to configuration file. Saves setting to configuration file.

The following example shows how to enable auto-reset.

```
Switch# configure terminal
Switch(config)# auto-reset enable
Switch(config)# end
Switch# show auto-reset status
Auto-reset                    : Enabled
Auto-reset maximum count : 1
Auto-reset current count : 3
Enable    Reset_Time      Status    Reset_Count    Last_Reset_Time
-------------------------------------------------------------------------
CPU       No   immediately      unset          0              none
Network   No   immediately      unset          0              none
Memory    No   immediately      unset          0              none
Process   No   immediately      unset          0              none
Force-reboot        No
```

To disable auto-rest, do the following commands.

```
Switch# configure terminal
Switch(config)# auto-reset disable
Switch(config)# end
```

Enabling auto-reset by CPU Threshold

To enable auto-reset function by high-cpu-load, do the following procedure in privileged EXEC mode.

<Table 158> Enabling auto-reset by high-cpu-load

		Command	Purpose
Step1		*Configure terminal*	Enters Global configuration mode Enters Global configuration mode.
Step2		**auto-reset cpu threshold high** < 1-100> **low** <1-100> **time** <1-3600> **at** HH:MM	Enables auto-rest function with system CPU threshold. **High :** Threshold for system booting. **Low** : Sets CPU threshold value to show log message. **time** : Sets the threshold maintaining time to come out result about high and low value. **At(option) :** If threshold condition is satisfied, the system reloads at the time.
Step3		**End**	Changes privileged EXEC mode.
Step4		**show auto-reset status**	Shows the setting.
Step5		**copy running-config startup-config**	Saves setting to configuration file.

The following example shows how to set auto-reset command when CPU Threshold continues more than low 80% for 60 seconds and more than high 90%.

```
Switch# configure terminal
Switch(config)# auto-reset cpu threshold high 90 low 80 time 60 at 23:00
Switch(config)# end
Switch# show auto-reset status
Auto-reset                    : Enabled
Auto-reset maximum count : 1
Auto-reset current count : 3
                Enable     Reset_Time       Status    Reset_Count     Last_Reset_Time
-------------------------------------------------------------------------------
           CPU      Yes          23:00        unset              0               none
       Network       No    immediately        unset              0               none
        Memory       No    immediately        unset              0               none
       Process       No    immediately        unset              0               none
Force-reboot       No
```

The following example shows how to disable the setting.

```
Switch# configure terminal
Switch(config)# no auto-reset cpu
Switch(config)# end
```

Enabling auto-reset by MEMORY Threshold

To enable auto-reset function by memory threshold, do the following steps in the privileged EXEC.

<Table 159> Enabling auto-reset by low-free-memory

		Command	Purpose
Step1		*Configure terminal*	Enters Global configuration mode
Step2		**auto-reset memory threshold high** < 1-100> **low** <1-100> **time** <1-3600> **at** HH:MM	Enables auto-rest function with threshold value. **High :** Threshold for system booting **Low** : Sets memory threshold value to show log message. **time** : Sets the threshold maintaining time to come out result about high and low value. **At(option) :** If threshold condition is satisfied, the system reloads at the time.
Step3		**End**	Changes privileged EXEC mode.
Step4		**show auto-reset status**	Shows the setting.
Step5		**copy running-config startup-config**	Saves setting to configuration file.

The following example shows how to set auto-reset command when memory threshold continues more than low 70% for 60 seconds and more than high 80%.

```
Switch# configure terminal
Switch(consfig)# auto-reset memory threshold high 80 low 70 time 60 at 23:00
Switch(config)# end
Switch# show auto-reset
Auto-reset                    : Enabled
Auto-reset maximum count : 1
Auto-reset current count : 3
                Enable    Reset_Time      Status   Reset_Count    Last_Reset_Time
-------------------------------------------------------------------------------
           CPU     Yes         23:00      unset             0              none
       Network      No     immediately    unset             0              none
        Memory     Yes         23:00      unset             0              none
       Process      No     immediately    unset             0              none
Force-reboot       No
```

The way to disable is as follows:

```
Switch# configure terminal
Switch(config)# no auto-reset memory
Switch(config)# end
```

Enabling auto-reset by ICMP Ping fail

To enable auto-rest function by ICMP Ping fail, do the following steps in the privileged EXEC mode.

<Table 160> Enabling auto-reset by ICMP Ping fail

		Command	Purpose
Step1		*Configure terminal*	Enters Global configuration mode
Step2		**auto-reset network-monitor interval <1-60> count <1-60> at HH:MM** **auto-reset network-monitor target-ip A.B.C.D**	Enables auto-reset function by imcp ping fail. **Interval (sec)**: packet transmission interval. **Count** : Ping Loss Count **At(option) :** If threshold condition is satisfied, the system reloads at the time. **TargetIP(A.B.C.D)** : Target address
Step3		**End**	Changes privileged EXEC mode.
Step4		**show auto-reset status**	Shows the setting. Shows the setting.
Step5		**copy running-config startup-config**	Saves setting to configuration file.

The following example shows how to set auto-reset command when it fails to send packet as 20 times for 5 seconds to destination address 10.1.20.253.

```
Switch# configure terminal
Switch(config)# auto-reset network-monitor interval 5 count 20 at 23:00
Switch(config)# auto-reset network-monitor target-ip 10.1.20.254
Switch(config)# end
Switch# show auto-reset status
Auto-reset                    : Enabled
Auto-reset maximum count : 1
Auto-reset current count : 3
                Enable    Reset_Time      Status   Reset_Count    Last_Reset_Time
-------------------------------------------------------------------------------
           CPU  Yes          23:00        unset          0              none
       Network  Yes          23:00          set          0              none
        Memory  Yes          23:00        unset          0              none
       Process   No    immediately        unset          0              none

Force-reboot     No
```

The way to disable is as follows:

```
Switch# configure terminal
Switch(config)# no auto-reset network-monitor
Switch(config)# end
```

Enabling auto-reset by Process-Monitor

When specific process does not work, do the following steps in privileged EXEC mode to enable auto-reset function.

<Table 161> Enabling auto-reset by Process-monitorat

		Command	Purpose
Step1		Configure terminal	Enters Global configuration mode
Step2		**auto-reset process-monitor at 23:00**	Enables auto-reset function by process monitor. **At (option):** If threshold condition is satisfied, the system reloads at the time.
Step3		**End**	Changes privileged EXEC mode.
Step4		**show auto-reset status**	Shows the setting.
Step5		**copy running-config startup-config**	Saves setting to configuration file.

The following example shows how to set auto-reset command when process deamon shut down.

```
Switch# configure terminal
Switch(config)# auto-reset process-monitor at 23:00
Switch(config)# end
Switch# show auto-reset status
Auto-reset                    : Enabled
Auto-reset maximum count : 1
Auto-reset current count : 3
              Enable   Reset_Time     Status   Reset_Count   Last_Reset_Time
-------------------------------------------------------------------------
         CPU    Yes        23:00      unset          0             none
     Network    Yes        23:00      unset          0             none
      Memory    Yes        23:00      unset          0             none
     Process    Yes        23:00      unset          0             none
Force-reboot    No
```

The way to disable is as follows:

```
Switch# configure terminal
Switch(config)# no auto-reset process-monitor
Switch(config)# end
```

Enabling auto-reset by CPU-Network

If you enable auto-rest function in case of satisfying two conditions about CPU and Network, do the following steps in the privileged EXEC mode.

<Table 162> Enabling auto-reset by Process-monitor

		Command	Purpose
Step1		Configure terminal	Enters Global configuration mode
Step2		**auto-reset cpu-network at HH:MM** **auto-reset cpu-network cpu threshold high** < 1-100> **low** <1-100> **time** <1-3600> **auto-reset cpu-network network-monitor interval <1-60> count <1-60>** **auto-reset network-monitor target-ip A.B.C.D**	Enables auto-reset function by process-monitor. **At(option) :** If threshold condition is satisfied, the system reloads at the time. **High :** Threshold for system booting **Low** : Sets CPU threshold value to show log message. **time** : Sets the threshold maintaining time to come out result about high and low value. **Interval (sec)**: Packet transmittion interval **Count** : Ping Loss Count **At(option) :** If threshold condition is satisfied, the system reloads at the time. **TargetIP(A.B.C.D)** : Destination address
Step3		**End**	Changes privileged EXEC mode.
Step4		**show auto-reset status**	Shows the setting.
Step5		**copy running-config startup-config**	Saves setting to configuration file.

The following example shows how to set auto-reset command, when Preocess Deamon shut down.

```
Switch# configure terminal
Switch(config)# auto-reset cpu-network at 23:00
Switch(config)# auto-reset cpu-network cpu    threshold high 90 low 80 time 60
Switch(config)# auto-reset cpu-network network-monitor interval 5 count 20
Switch(config)# auto-reset network-monitor target-ip 10.1.20.254
Switch(config)# end
Switch# show auto-reset status
Auto-reset                    : Enabled
Auto-reset maximum count : 1
Auto-reset current count : 3
Enable     Reset_Time       Status    Reset_Count     Last_Reset_Time
-------------------------------------------------------------------------
CPU-Network       Yes          23:00        unset              0                  none
Memory        Yes          23:00        unset              0                  none
Process       Yes          23:00        unset              0                  none
Force-reboot        No
```

The way to disable is as follows:

```
Switch# configure terminal
Switch(config)# no auto-reset cpu-network
Switch(config)# end
Enabling Limit Count of auto-reset
```

Auto-reset suppress is the function to block occurring auto-reset by count.

To enable auto-reset suppress function, do the following steps in the privileged EXEC mode.

<Table 163> Enabling Suppression of auto-reset

		Command	Purpose
Step1		Configure terminal	Enters Global configuration mode
Step2		**auto-reset reset-count** <1-100 | unlimited >	Enables auto-rest function with Reset-count. **Reset-Count:** Maximum reset count to permit auto-reset per one day.
Step3		**End**	Changes privileged EXEC mode.
Step4		**show auto-reset status**	Shows the setting.
Step5		**copy running-config startup-config**	Saves setting to configuration file.

The following example shows how to limit auto-reset count as maximum 5 times during one day. After auto-reset comes out more than 5 times, it does not work.

```
Switch# configure terminal
Switch(config)# auto-reset reset-count 5
Switch(config)# end
Switch# show auto-reset status
Auto-reset                    : Enabled
Auto-reset maximum count : 5
Auto-reset current count : 3

Enable     Reset_Time       Status   Reset_Count     Last_Reset_Time
-------------------------------------------------------------------------
CPU-Network       Yes          23:00        unset              0                  none
Memory       Yes          23:00        unset              0                  none
Process      Yes          23:00        unset              0                  none
Force-reboot      No
```

Note It is initialized bycurrent count “0” at 24:00 with standardzing function off or system clock.

Enable force-reboot auto-reset

You can enable auto-reset at setting time regardless auto-reset condition.

<Table 164> Enabling force-reboot auto-reset

		Command	Purpose
Step1		Configure terminal	Enters Global configuration mode
Step2		**auto-reset force-reboot at <1-12> <1-31> <year> HH:MM:SS**	Delay auto-reset work with setting delay-time. You can set it as month, day, year, hour, minute, and second. You can set more than maximum 128 days. Set the time after current time.
Step3		**End**	Changes privileged EXEC mode.
Step4		**show auto-reset status**	Shows the setting.
Step5		**copy running-config startup-config**	Saves setting to configuration file.

The following example shows how to set auto-reset to reset at the setting time.

```
Switch# configure terminal
Switch(config)# auto-reset force-reboot at 1 12 2012 00:00:00
Switch(config)# end
Switch# show auto-reset
Auto-reset: Enabled
Auto-reset maximum count : 5
Auto-reset current count : 3

Enable     Reset_Time       Status   Reset_Count     Last_Reset_Time
-------------------------------------------------------------------------
CPU-Network       Yes          23:00        unset              0                  none
Memory       Yes          23:00        unset              0                  none
Process      Yes          23:00        unset              0                  none
Force-reboot      Yes    Jan 12 2012 00:00:00
```

The way to disable is as follows:

```
Switch# configure terminal
Switch(config)# no auto-reset force-reboot
Switch(config)# end
```