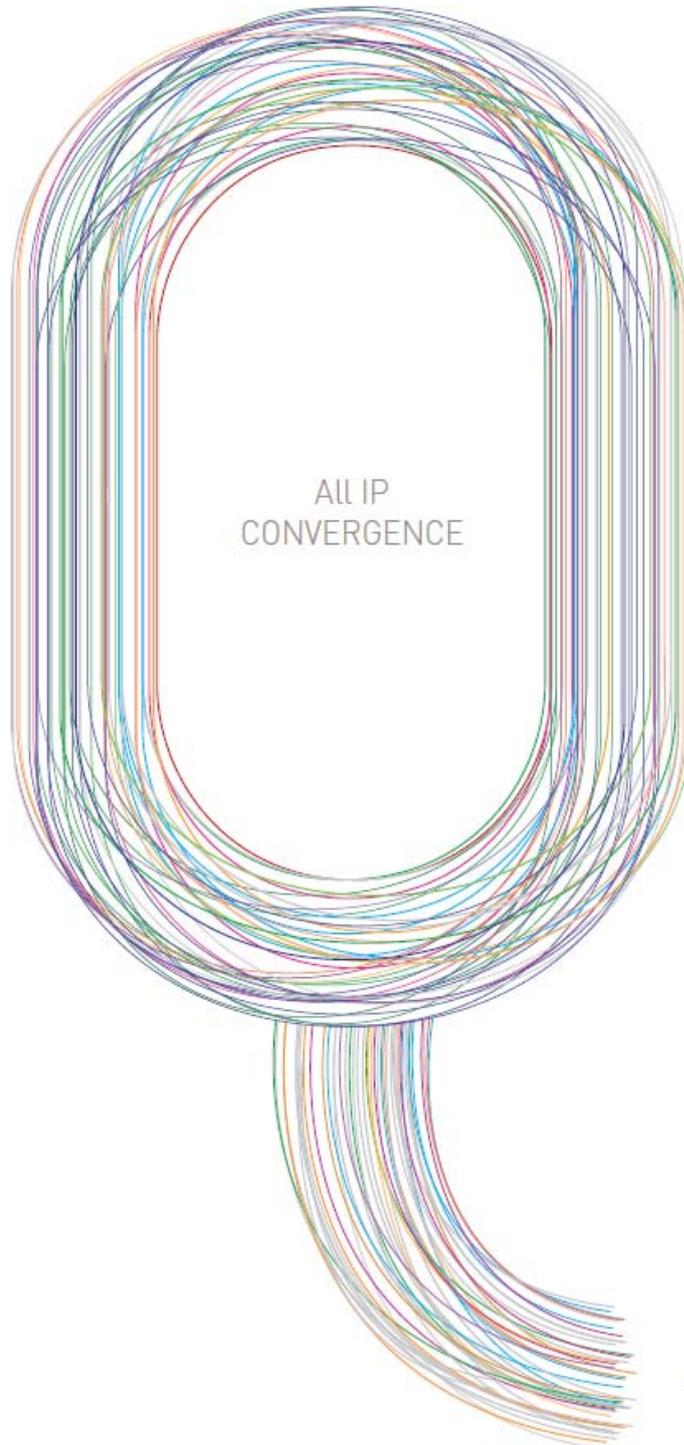


U3024B

■ User Guide



ubi**Q**uoss

U3024B

■ User Guide

ubiQuoss

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 U3024B user guide, which describes guide conventions, and lists other publications that may be useful.

Introduction

This user guide describes the details about how to configure the U3024B of ubiQuoss system.

- It describes how to configure U3024B and connect it to other devices.
- What are provided with this user guide (operation user guide, command user guide, and configuration user guide) describe the function, use, and setting of U3024B in details.

Related Documents

U3024B set includes the followings. For additional information on this equipment, refer to the following manuals.

Manual	Contents
<i>Hardware Installation Guide</i>	Hardware installation Initial operating environment configuration
<i>User Guide</i>	Operating configuration for services System operation, administration and maintenance Trouble Shooting

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.
	Warning	Warning: Optical Terminal Do not look at the optical terminal directly. It could cause serious damage to your eyes.
	Warning	Do not disassemble or assemble the product. The user must not remove/attach the product cover or disassemble/assemble the product when the power is on. Otherwise, it can cause personal injury or property loss.

Organization

The chapters of this manual are organized as follows:

Chapter 1. Overview

This chapter provides the information required for system operator to set up an operating environment and to get started with the U3024B.

Chapter 2. Interface Environment Setup

This chapter describes the following Topics

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

This chapter describes how to set DHCP Relay.

Chapter 6. IGMP Snooping

This chapter describes IGMP snooping in the U3024B switch.

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. Stacking

This chapter describes the stacking function to manage several switches with one IP address.

Chapter 9. Static Monitoring & Qos

This chapter describes the administration and management function through RMON (Remote Monitoring) to monitor the current status of the U3024B and to display the log information on the screen.

Chapter 10. System File Management

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. CPU-FILTER & SYSCTL

This chapter describes how to set CPU-Filter and SYSCTL.

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. ARP Snooping

This chapter is to explain how to configure ARP snoop function that is used to build Ethernet address information on specific IP address range.

Chapter 14. VDSL Configuration

In this chapter is the explanation upon how to set-up the VDSL2 configuration for U3000 switch. The main content includes as below:

Table of Content

Preface	III
Introduction	III
Related Documents	III
Symbols in this Guide	IV
Organization	V
Table of Content	VII
List of Table.....	XIII
Chapter 1. Overview.....	19
Edit and Help Functions	20
Command Modes	25
U3024B Operation.....	26
User Interface	27
Console Connection.....	27
Telnet Connection	28
Connection through SNMP Network Manager	28
User Authentication	29
Adding and Deleting User	29
Setting Password	30
Setting Password Encryption	31
Setting Authentication Mode	31
Setting Authentication Server.....	34
Setting Hostname	36
SNMP (Simple Network Management Protocol)	37
ACL (Access Control List).....	40
Rules to Create an Access List.....	40
Setting Standard IP Access List	40
Setting Access List for Telnet Connection	41
NTP Setup	43
Overview.....	43
Setting NTP Client Mode	43
Setting NTP Server Mode	43
Setting NTP Time Zone.....	43
Setting NTP summer time.....	44
Chapter 2. Interface Environment Setup	45
Overview.....	46
Common Command	47
Interface Name	47
Interface ID	47
Interface Mode Prompt	47
Interface-range Mode Prompt	47
Viewing Interface Information and Status.....	48
Show Interfaces	48
Show Port Status	48
Show Switchport	50
Setting Physical Port Environment.....	51

Shutdown.....	51
Block.....	51
Speed and Duplex	52
Port Mirroring	53
Setting Layer 2 Interface Environment	54
VLAN Trunking	54
Layer 2 Interface Mode.....	54
Layer 2 Interface Default Settings	54
Enable/Disable Layer 2 Interface.....	54
Setting Trunk Port.....	55
Setting Access Port	55
Port Group	57
Overview	57
Port Group Configuration.....	57
MAC Filtering	58
Overview	58
Setting MAC Filtering.....	58
Traffic-control	59
Overview	59
Setting Traffic-control.....	59
Chapter 3. VLAN	62
Overview of VLAN	63
VLAN Types	64
Port-Based VLANs	64
Tagged VLANs.....	66
Another advantage of tag	66
Combining Port-Based VLAN and Tagged VLAN	68
VLAN Configuration	69
VLAN ID	69
Default VLAN.....	69
Native VLAN	69
VLAN Setup	71
VLAN Setup Commands	71
Example of VLAN Setup.....	72
Viewing VLAN Configuration	74
Chapter 4. IP Environment	75
Overview	76
Assigning an IP Address to Network Interface	77
ARP (Address Resolution Protocol).....	78
Setting a Default Gateway.....	78
Example of IP Settings	79
Chapter 5. DHCP Relay	80
Configuration of DHCP Relay Function	81
Overview of DHCP Relay	81
Setting a DHCP Relay Agent.....	83
Activation of DHCP relay function.....	83

Setting DHCP server at DHCP relay agent	84
Configuring DHCP relay information option (OPTION82)	85
Setting Relay Information Policy	86
Setting DHCP Smart Relay	87
Configuring DHCP Relay Verify MAC-Address	88
Configuring DHCP relay server-id-relay	89
Monitoring and managing DHCP relay	91
DHCP Relay configuration example	91
DHCP snooping Function	93
DHCP snooping function	93
Packet Validation	94
Configuring DHCP Snooping	95
Activation of DHCP snooping function	95
Configuring DHCP Snooping Vlan	95
Configuring DHCP snooping information option (OPTION82).....	96
Setting the policy of retransmission of DHCP snooping information option	97
Configuring DHCP Snooping Trust Port.....	98
Configuring DHCP snooping max-entry	99
Configuring DHCP Snooping Entry Time	99
Configuring DHCP Snooping Rate-Limit	100
Configuring DHCP Snooping Verify MAC-Address	101
DHCP Snooping Manual Binding configuration.....	101
DHCP Snooping monitor and management	102
DHCP snooping configuration example	102
Chapter 6. IGMP Snooping.....	103
Overview of IGMP Snooping	104
Setting IGMP Snooping	105
Enable Global IGMP Snooping	105
Enable IGMP-TRAP on an interface	106
Enable IGMP Snooping on a VLAN	106
Configure IGMP Snooping Functionality	107
Setting Last-Member-Join-Interval	111
Setting TCN (Topology Change Notification).....	112
Setting IGMP Filtering	113
Setting IGMP Max-Group-Count	114
Setting IGMP Max-Reporter-Count	115
Configuring drop-igmp-ttl-over	115
Configuring snooping ignore-mpkt-upstream-forward	116
Setting IGMP Proxy-Reporting	117
Enable IGMP Proxy-Reporting	118
Enable IGMP Proxy-Reporting on a VLAN.....	119
Configure IGMP Proxy-Reporting Functionality	120
Setting Static Multicast Router Port	120
Display System and Network Statistics	121
Chapter 7. STP and SLD	123
Understanding Spanning-Tree Features	124
STP Overview	124
Bridge Protocol Data Units.....	124

Election of Root Switch.....	125
Bridge ID, Switch Priority, and Extended System ID.....	125
Spanning-Tree Timers	126
Creating the Spanning-Tree Topology	126
Spanning-Tree Interface States	127
Understanding RSTP	130
RSTP Overview	131
Port Roles and the Active Topology.....	132
Rapid Convergence	133
Bridge Protocol Data Unit Format and Processing.....	134
Configuring Spanning-Tree Features.....	135
Default STP Configuration:.....	135
STP Configuration Guidelines	136
Enabling STP.....	136
Disable per VLAN STP	136
Configuring the Port Priority.....	137
Configuring the Path Cost.....	138
Configuring the Switch Priority of a VLAN	139
Configuring the Hello Time	140
Configuring the Forwarding-Delay Time for a VLAN	141
Configuring the Maximum-Aging Time for a VLAN.....	142
Configuring the Port as Edge Port.....	143
Configuring the RSTP Mode.....	144
Specifying the Link Type to Ensure Rapid Transitions	145
Restarting the Protocol Migration Process	146
Displaying the Spanning-Tree Status.....	147
Self-loop Detection	148
Understanding Self-loop Detection	148
Configuring Self-loop Detection.....	148
Displaying Self-loop Status	151
Chapter 8. Stacking	152
Stacking Overview	153
Configuring Stacking Feature	154
Configuring the Stack VLAN	154
Configuring the Stack Member	154
Enabling the Stack.....	155
Connecting to Slave Switch.....	155
Displaying the Stacking Status.....	156
Chapter 9. Static Monitoring & Qos.....	157
Status Monitoring	158
Port Statistics	159
CPU Traffic Statistics	162
Configuring CPU Packet Counter	162
Configure terminal	164
Configure terminal	164
Displaying CPU Packet Counter.....	165

Logging	168
Contents of System Log Message	168
Default Logging Settings	169
The example of Logging configuration	171
RMON (Remote MONitoring)	173
RMON Overview	173
Setting Alarm and Event Groups of RMON	175
Qos and Packet Filtering	179
Qos Parameters	186
Scheduling	187
Congestion Avoidance	189
Filtering	190
Chapter 10. System File Management.....	191
Flash File System	192
Image/Configuration File Down/Up Load	193
Download/Upload over FTP	193
Download/Upload over TFTP	194
Configuration File Management	195
Copying a Configuration File.....	195
Deleting a Configuration File.....	196
Boot Mode Setting and System Restarting	197
Setting Boot Mode	197
Restarting the System.....	197
Chapter 11. CPU-FILTER & SYSCTL	198
CPU Filtering	199
Enabling/Disabling CPU-Filtering Rule	199
Setting a CPU-FILTER Group	199
Examples of Setting CPU-FILTER	201
SYSCTL.....	202
SYSCTL Overview	202
SYSCTL Command.....	202
Chapter 12. DAI.....	204
Understanding DAI	205
Understanding ARP	205
Understanding ARP Spoofing Attacks	205
Understanding DAI and ARP Spoofing Attacks	206
Interface Trust States and Network Security	207
Rate Limiting of ARP Packets	208
Relative Priority of ARP ACLs and DHCP Snooping Entries	209
Logging of Dropped Packets.....	209
DAI Configuration Guidelines and Restrictions	210
Configuring DAI	211
Enabling DAI on VLANs.....	211
Configuring the DAI Interface Trust State.....	212
Applying ARP ACLs for DAI Filtering.....	213
Configuring ARP Packet Rate Limiting.....	213

Enabling DAI Error-Disabled Recovery	215
Enabling Additional Validation.....	216
Configuring DAI Logging	218
DAI Logging Overview.....	218
Configuring the DAI Logging Buffer Size	218
Configuring the DAI Logging System Messages	219
Configuring the DAI Log Filtering.....	220
Displaying DAI Information	221
DAI Configuration Samples	222
Sample One: Interoperate with DHCP Snoop.....	222
Chapter 13. ARP Snooping.....	224
Understanding ARP Snoop.....	225
Understanding ARP Snoop.....	225
ARP Snoop Entry States.....	226
ARP Snoop Ageing Time	226
ARP Snoop Binding Health Check	227
ARP Snoop Probe	227
Understanding DAI and ARP Snoop.....	227
Relative Priority of ARP ACLs and ARP Snoop Entries	228
Default ARP Snoop Configuration	229
Configuring ARP Snoop.....	230
Enabling ARP Snoop	230
Configuring ARP Snoop Ageing-time.....	230
Disabling Gratuitous ARP Update without Validation	231
Disabling Health-check.....	232
Displaying ARP Snoop Information.....	232
ARP Snoop Configuration Samples	233
Sample One: ARP spoofing detection	233
Sample Two: Interoperate with DAI on DHCP Relay	234
Chapter 14. VDSL Configuration.....	237
Overview of Profile.....	238
Setting up Line Profile.....	239
Default configuration.....	239
Assigning a Profile to a Specific VDSL Port.....	239
Configuring a New Line Profile	239
Reset VDSL Port with Updated Profile	240
Setting up Line profile.....	240
Setting up Alarm profile	249
Setting up System profile.....	250
Setting up Interface	255
Identification of the VDSL profiles.....	256
Identification of Alarm-profile	256
Identification of line-profile.....	257
Identification of system-profile	259
Identification of Interface	259

List of Table

<Table 1> Command Symbols.....	23
<Table 2> Command Line Edit and Help Functions	23
<Table 3> Switch Command Modes.....	25
<Table 4> Movement between Command Modes	25
<Table 5> Commands for Adding and Deleting Switch Users.....	29
<Table 6> Commands for Setting Switch Enable Password	30
<Table 7> Commands for Setting User Authentication.....	31
<Table 8> Commands for Setting User Authentication.....	33
<Table 9> Commands for Setting RADIUS Server.....	34
<Table 10> Commands for Setting TACACS+ Server	35
<Table 11> Commands for Setting Hostname.....	36
<Table 12> Commands for Setting SNMP Environment	37
<Table 13> Commands for Setting Access List.....	40
<Table 14> Setting NTP Client Mode	43
<Table 15> Setting NTP Server Mode	43
<Table 16> Setting NTP Time Zone.....	43
<Table 17> Setting NTP summer time.....	44
<Table 18> Other NTP Commands	44
<Table 19> Interfaces Supported by U3024B.....	46
<Table 20> Common Command.....	47
<Table 21> Interface Name	47
<Table 22> Interface ID and Supported Range	47
<Table 23> Commands related to Interface Information and Status	48
<Table 24> Commands for Setting up Physical Port Environment.....	51
<Table 25> Speed and Duplex.....	52
<Table 26> Port mirroring	53
<Table 27> Layer 2 Interface Modes Supported by U3024B	54
<Table 28> Layer 2 Interface Default Settings	54
<Table 29> Layer 2 interface on/off command	54
<Table 30> Commands for Setting Trunk Ports.....	55
<Table 31> Commands for Setting Access Ports	55
<Table 32> Commands for Configuring Port Group	57
<Table 33> Commands for Setting MAC-filter	58
<Table 34> Commands for Setting Traffic-control	59
<Table 35> VLAN Setup Commands.....	71
<Table 36> Viewing VLAN Configuration.....	74
<Table 37> Available IP addresses.....	77
<Table 38> Command for Assigning an IP Address	78
<Table 39> Command for ARP Environment Setup	78
<Table 40> Command for Setting a Default Gateway	78
<Table 41> Displaying Default Gateway.....	78
<Table 42> Activation of DHCP relay function.....	83
<Table 43> Setting DHCP server at DHCP relay agent	84

<Table 44> Activation of DHCP relay information option	85
<Table 45> Setting Relay Information Policy	86
<Table 46> Setting DHCP Smart Relay	87
<Table 47> Configuring DHCP Relay Verify MAC-Address	88
<Table 48> Configuring DHCP relay server-id-relay	89
<Table 49> Commands for DHCP relay monitor and management	91
<Table 50> Field Title	92
<Table 51> Activation of DHCP Snooping function	95
<Table 52> Configuring DHCP Snooping Vlan	95
<Table 53> Activation of DHCP snooping information option function	96
<Table 54> IP DHCP snooping Information Policy	97
<Table 55> Configuring DHCP Snooping Trust Port	98
<Table 56> Configuring DHCP snooping max-entry	99
<Table 57> Configuring DHCP Snooping Entry Time	99
<Table 58> Configuring DHCP Snooping Rate-Limit	100
<Table 59> Configuring DHCP Snooping Verify MAC-Address	101
<Table 60> DHCP Snooping Manual Binding configuration	101
<Table 61> DHCP Snooping monitor and management	102
<Table 62> Enable Global IGMP Snooping	105
<Table 63> Enable IGMP-TRAP on an interface	106
<Table 64> Enable IGMP Snooping on a VLAN	106
<Table 65> Setting Report-Suppression	107
<Table 66> Setting Fast-Leave	108
<Table 67> Setting Mrouter	109
<Table 68> Setting Mrouter Port Detection over PIM/DVMRP	110
<Table 69> Setting an Aging Time	110
<Table 70> Setting Last-Member-Join-Interval	111
<Table 71> Setting TCN (Topology Change Notification)	112
<Table 72> Setting IGMP Filtering	113
<Table 73> Applying IGMP Fitering	114
<Table 74> Setting IGMP Max-Group-Count	114
<Table 75> Setting IGMP Max-Reporter-Count	115
<Table 76> Configuring drop-igmp-ttl-over	115
<Table 77> Configuring snooping ignore-mpkt-upstream-forward	116
<Table 78> Enable IGMP Proxy-Reporting	118
<Table 79> Enable IGMP Proxy-Reporting on a VLAN	119
<Table 80> Setting Static Multicast Router Port	120
<Table 81> Setting IGMP Static-Group	121
<Table 82> Commands for Monitoring IGMP Snooping	121
<Table 83> Commands for Monitoring IGMP Proxy-Reporting	122
<Table 84> Switch Priority Value and Extended System ID	126
<Table 85> Spanning-Tree Timers	126
<Table 86> Port State Comparison	132
<Table 87> RSTP BPDU Flags	134
<Table 88> Default STP Configuration	135
<Table 89> Enabling STP	136

<Table 90> Disable per VLAN STP	136
<Table 91> Configuring the Port Priority	137
<Table 92> Configuring the Path Cost	138
<Table 93> Configuring the Switch Priority of a VLAN	139
<Table 94> Configuring the Hello Time	140
<Table 95> Configuring the Forwarding-Delay Time for a VLAN	141
<Table 96> Configuring the Maximum-Aging Time for a VLAN	142
<Table 97> Configuring the Port as Edge Port	143
<Table 98> Configuring the RSTP Mode	144
<Table 99> Specifying the Link Type to Ensure Rapid Transitions	145
<Table 100> Displaying the Spanning-Tree Status	147
<Table 101> Enabling Self-loop Detection	149
<Table 102> Changing the Service Status of Port	149
<Table 103> Disabling Self-loop Detection	150
<Table 104> Configuring the Stack VLAN	154
<Table 105> Configuring the Stack Member	154
<Table 106> Enabling the Stack	155
<Table 107> Connecting to Slave Switch	155
<Table 108> Displaying the Stacking Status	156
<Table 109> Commands for Status Monitoring	158
<Table 110> Command for Viewing Port Statistics	160
<Table 111> > Commands for Viewing Port Statistics	161
<Table 112> Commands for Clearing Port Statistics	161
<Table 113> Addition of packet type	164
<Table 114> Removal of packet type	164
<Table 115> Display cpu packet counter	165
<Table 116> Command to Clear the Statistics on CPU Traffic	166
<Table 117> Log Levels of U3024B	168
<Table 118> System Log Default Settings	169
<Table 119> Commands for Setting up System Message Logging Environment	169
<Table 120> Displaying Log	170
<Table 121> RMON Groups	174
<Table 122> Commands for Setting RMON Alarm and Event	175
<Table 123> Commands for Setting RMON Statistics and History	177
<Table 124> Command for Creating/Deleting a Flow-Rule and Setting a Mode	180
<Table 125> Commands for Flow-Rule Classification	180
<Table 126> Commands for Applying Flow-Rule	181
<Table 127> Mask-Calculator Commands	183
<Table 128> Command for Creating and Adding a Policy-Map	184
<Table 129> Commands for Deleting the Policy-Map or a Specific Flow-Rule	184
<Table 130> Commands for Enabling/Disabling Policy-Map	184
<Table 131> Commands for Showing Flow-Rules	184
<Table 132> Commands for Setting Qos Related Marking/Remarking Table	186
<Table 133> Commands for Viewing Qos Related Marking/Remarking Table	186
<Table 134> Commands for Changing Queue-Mode	188
<Table 135> Commands for Changing Wrr-Method Queue Weight	188

<Table 136> Command to Show Queue-Method and Weight for All Interfaces ..	188
<Table 137> Commands for Filtering.....	190
<Table 138> Commands for File Management.....	192
<Table 139> Commands for Downloading/Uploading over FTP	193
<Table 140> Commands for Downloading/Uploading over TFTP	194
<Table 141> Commands for Configuration Management.....	195
<Table 142> Commands for Setting Boot Mode and Restarting the System	197
<Table 143> Enabling/Disabling CPU-Filtering Rule	199
<Table 144> Disabling the CPU-filter rule.....	199
<Table 145> Adding/Deleting an INPUT Group	200
<Table 146> Disabling All Rule	200
<Table 147> Add/Delete Forward Group	200
<Table 148> Enable CPU-FILTER Service	201
<Table 149> SYSCTL Command.....	202
<Table 150> Default DAI Configuration	209
<Table 151> Enabling DAI on VLANs.....	211
<Table 152> Configuring the DAI Interface Trust State	212
<Table 153> Applying ARP ACLs for DAI Filtering.....	213
<Table 154> Configuring ARP Packet Rate Limiting	214
<Table 155> Enabling DAI Error-Disabled Recovery	215
<Table 156> Enabling Additional Validation	216
<Table 157> Configuring the DAI Logging Buffer Size	218
<Table 158> Configuring the DAI Logging System Messages	219
<Table 159> Configuring the DAI Log Filtering.....	220
<Table 160> Displaying DAI Information	221
<Table 161> Initializing and Displaying the DAI Statistics	221
<Table 162> Initializing and Displaying the DAI log buffer.....	221
<Table 163> Steps of Using DAL Function	222
<Table 164> Types of ARP that updates ARP cache.....	225
<Table 165> ARP Snoop Entry States	226
<Table 166> Default ARP Snoop Configuration.....	229
<Table 167> Enabling ARP Snoop.....	230
<Table 168> Configuring ARP Snoop Ageing-time	231
<Table 169> Disabling Gratuitous ARP Update without Validation.....	231
<Table 170> Disabling Health-check	232
<Table 171> Displaying ARP Snoop Information.....	232
<Table 172> ARP Snoop Configuration	233
<Table 173> DAI on DHCP Relay.....	234
<Table 174> Assigning a Profile to a Specific VDSL Port.....	239
<Table 175> Configuring a New Line Profile	239
<Table 176> Reset VDSL Port with Updated Profile	240
<Table 177> Setting up Line profile	240
<Table 178> Setting up pbo-config	240
<Table 179> Setting up Optional band	241
<Table 180> Setting up band-modifier.....	242
<Table 181> Setting up G.HS.....	243

<Table 182> Setting up ife-tx-filter and ife-rx-filter	243
<Table 183> Setting up line type	244
<Table 184> Setting up line type manually	244
<Table 185> Setting up power-mode	245
<Table 186> Setting up rate-adaptation-mode	245
<Table 187> Setting up max-margin, min-noise-margin, target-noise-margin	246
<Table 188> Setting up VDSL port transmission speed	247
<Table 189> Setting up Interleave	248
<Table 190> Setting up min-ohm-rate	249
<Table 191> Setting up Alarm profile	249
<Table 192> Adjusting the Threshold Value	249
<Table 193> Setting up System profile	250
<Table 194> Setting up band-plan	251
<Table 195> Setting up rfi-band	252
<Table 196> Setting up adsl-safe-mode, tlan-safe-mode	252
<Table 197> Setting up psd-mask-level	253
<Table 198> Setting up Ham-band	254
<Table 199> Setting up Interface	255
<Table 200> VDSL Parameters	255
<Table 201> Identification of Alarm-profile	256
<Table 202> Identification of line-profile	257
<Table 203> Identification of system-profile	259
<Table 204> Identification of Interface	259

Chapter 1. Overview

This chapter provides the information required for system operator to set up an operating environment and to get started with the U3024B.

- Edit and help functions
- Command modes
- U3024B operation
- U3024B 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 U3024B 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 U3024B 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 U3024B 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 U3024B 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) <i>address</i>
():	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 (<i>cos-queue-map cos-remarking</i>)
[]:	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 [<i>ifname</i>]
:	Vertical bar	Represents exclusive parameters in the parameter list
<i>Italic</i>		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 U3024B 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 U3024B 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- <i>vd1</i>)# Switch(config-if- <i>vlan1</i>)#	Used to change interface environment settings



Notice

Command prompt uses the U3024B 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 U3024B switch. 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 <i>ifname</i>	Moves from Config mode to Interface mode
exit	Moves to the previous mode
End	Moves from a certain mode to Privileged mode No movement occurs in User mode.

U3024B Operation

When the U3024B 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 U3024B 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 U3024B (*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 U3024B 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.

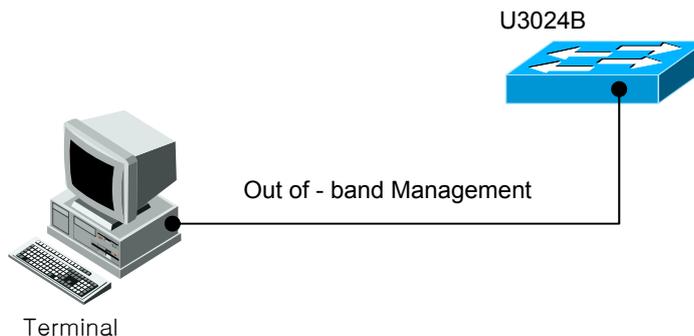
For operation and management, the U3024B supports multiple links as follows:

- 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 U3024B switch.

>, connect a terminal to the console port provided by the U3024B switch. Then, the prompt will appear and the login process will run.



<Figure 1> Connection between a Terminal and the U3024B



Notice

For details of terminal setup and console port pin settings, see the U3024B hardware installation guide.

Telnet Connection

The system operator can access the U3024B 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 U3024Bswitch 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 U3024Bswitch 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](#) >.

<Table 5> Commands for Adding and Deleting Switch Users

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

<code>class access-list-num</code>	access-list-num : <1-99>, indicating standard ip access list	
<code>no username userID access-class</code>	Clears the access list applied to the user.	Config
<code>no username userID</code>	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 U3024Bswitch 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
<code>enable password password</code>	Sets privileged mode password	Config
<code>no enable password</code>	Deletes privileged mode password	Config
<code>service password-encryption</code>	Enables password encryption mode	Config
<code>no service password-encryption</code>	Disables password encryption mode	Config



Notice

For user password setting commands, refer to < [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 U3024Bswitch 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 U3024B 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, tacacs) to be applied. Several authentication modes can be selected.	Config
no authentication login enable	Disables the selected authentication mode.	Config

(radius tacacs)	Local mode is normally enabled.	
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 <i>userID</i>	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 U3024B 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 U3024B 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)	Selects 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 U3024B 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 than 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 <i>encryption-key</i>	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 <i>encryption-key</i>	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 <i>encryption-key</i>	Sets a general key to be used for radius-server access. The general key is used when no keys are defined in the server.	Config
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)# radius-server key test123
Switch(config)# radius-server host 192.168.0.2 key Ins
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
<code>tacacs-server host A.B.C.D key <i>encryption-key</i></code>	Sets tacacs -server. Sets an encryption key to be used for server access.	Config
<code>no tacacs-server host A.B.C.D</code>	Deletes tacacs -server.	Config
<code>tacacs-server host A.B.C.D timeout <1-1000> key <i>encryption-key</i></code>	Sets tacacs -server. Sets timeout to receive response packet. Sets an encryption key to be used for server access	Config
<code>tacacs-server host A.B.C.D timeout <1-1000></code>	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 U3024Bswitch uses the default hostname “Switch”, which can be changed by user.

<Table 11> Commands for Setting Hostname

Command	Description	Mode
hostname <i>string</i>	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  
U3024B (config)# end  
Switch#
```

```
Switch# configure terminal  
Switch(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 U3024B 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 <i>agent-addr</i>	Sets an origination IP for the snmp packet transferred from the equipment	Config
no snmp-server agent-address <i>agent-addr</i>	Skips origination IP for the snmp packet transferred from the equipment	Config
snmp-server contact <i>string</i>	Changes system contact information	Config
snmp-server contact <i>string</i>	Changes system contact information	Config
no snmp-server contact <i>string</i>	Deletes system contact information	Config
snmp-server location <i>string</i>	Changes system location information	Config
no snmp-server location <i>string</i>	Deletes system location information	Config
snmp-server community <i>string</i> [ro rw [access-class <i>number</i>]]	Sets an SNMP community <i>ro</i> : read only <i>rw</i> : read write <i>number</i> : Standard IP access-list <1-99>	Config
no snmp-server community <i>string</i>	Deletes SNMP community	Config
snmp-server enable traps [<i>notification-type</i>] [<i>notification-option</i>]	Sets SNMP Traps to be transferred to Trap-Host <i>notification-type</i> : Trap type (config, environ, perform, resource, security, snmp) <i>notification-option</i> : Trap option	Config
no snmp-server enable traps	Sets SNMP Traps not to be transferred to Trap-Host	Config
snmp-server trap-host <i>A.B.C.D</i> community <i>string</i>	Sets a community to be used to send SNMP Trap Host and traps	Config
no snmp-server trap-host <i>A.B.C.D</i>	Deletes SNMP Trap Host	Config

Setting SNMP Community

Community string provides a simple authentication function between the system and the remote network manager. The U3024B 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 U3024B 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#
```

Setting System Administrator

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

```
Switch# configure terminal
Switch(config)# snmp-server contact "ubiquosshyd@locusnet.com"
Switch(config)# end
Switch# show running-config
```

```
!  
snmp-server contact "ubiquoss hyd"  
Switch#
```

Setting System Configuration Location

```
Switch# configure terminal  
Switch(config)# snmp-server location "ubiquoss, Hyderabad,India."  
Switch(config)# end  
Switch# show running-config  
!  
snmp-server location "ubiquoss, Hyderabad,India."  
!  
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 U3024B 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 <i>address ::= {any A.B.C.D/M}</i>	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 <i>address</i>	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 <i>stratum</i>	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 <i>HH:MM</i>	Adds the given time period to the Coordinated Universal Time (UTC) to represent the current time.
ntp timezone minus <i>HH:MM</i>	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 <i>week day month hh:mm week day month hh:mm</i>	Apply the start and finish date and time of Summer time period.
no ntp summer-time	Dismiss the set time for Summer time.

<Table 18> Other NTP Commands

Command	Description
ntp poll-interval <i>number</i>	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

```
Switch (config)# ntp server 203.248.240.103
Switch (config)# exit
Switch # show ntp
-----
Current time      : Thu Jan 12 20:40:25 2005
-----
NTP master       : disable
NTP stratum      : unspecified
Poll interval    : 6(power of 2)
NTP timezone     : GMT
-----
The list of NTP Server is below.

-----
[1] 203.248.240.103
-----
Switch #
```

Chapter 2. Interface Environment Setup

This chapter describes the following Topics

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

Overview

The U3024B supports the interfaces listed below.

<Table 19> Interfaces Supported by U3024B

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

You can set up an interface environment as follows.

- Enter the Config mode from the Privileged mode using the command “**configure terminal**”.
- Enter the interface mode using the command “**interface**”.
- 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 <i>ifname</i>	Enter the interface mode. <i>ifname</i> : Specifies an interface for environment setup.

Interface Name

The U3024B 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
VDSL line interface	VDSL	“vd” + port_number	vd1
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 U3024B models. The following 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.)
U3024	Fast Ethernet	port id	port id: 1-26	fa1, fa26
	VDSL	port id	port id: 1-24	vd1, vds24
	Port group	port id	1 – 7	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-if-vd1)#
```

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-ifrange)#

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 23> Commands related to Interface Information and Status

Command	Description	Mode
show interfaces [<i>ifname</i>]	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.

```
U3024# show interface vd1
vd1 is link up.
 type VDSL-100-100
 line-profile is test
 alarm-profile (co) is defval
 alarm-profile (remote) is
 up speed set 100M by line-profile
 down speed set 100M by line-profile
 current speed is 100M/100M
 cpu-mac-filter disable

Last clearing of counters 436:15:33
1 minutes input rate 0 bytes/sec, 0 packets/sec
1 minutes output rate 31 bytes/sec, 0 packets/sec
 0 packets input, 0 bytes
  Received 0 broadcasts, 0 multicasts
  0 CRC, 0 oversize, 0 dropped
 784,985 packets output, 50,239,040 bytes
  Sent 784,985 broadcasts, 0 multicasts
U3024#
```

Show Port Status

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

```
U3024# show port status
-----
ifname      type shut block link  cur-speed flow-ctrl linkup-time
```

vd1	VDSL	.	.	up	100M/100M	enable	Fri Dec 16 00:05:07
vd2	VDSL	.	.	up	100M/100M	enable	Fri Dec 16 00:05:39
vd3	VDSL	.	.	down	-	enable	-
vd4	VDSL	.	.	down	-	enable	-
vd5	VDSL	.	.	down	-	enable	-
vd6	VDSL	.	.	down	-	enable	-
vd7	VDSL	.	.	down	-	enable	-
vd8	VDSL	.	.	down	-	enable	-
vd9	VDSL	.	.	down	-	enable	-
vd10	VDSL	.	.	down	-	enable	-
vd11	VDSL	.	.	down	-	enable	-
vd12	VDSL	.	.	down	-	enable	-
vd13	VDSL	.	.	down	-	enable	-
vd14	VDSL	.	.	down	-	enable	-
vd15	VDSL	.	.	down	-	enable	-
vd16	VDSL	.	.	down	-	enable	-
vd17	VDSL	.	.	down	-	enable	-
vd18	VDSL	.	.	down	-	enable	-
vd19	VDSL	.	.	down	-	enable	-
vd20	VDSL	.	.	down	-	enable	-
vd21	VDSL	.	.	down	-	enable	-
vd22	VDSL	.	.	down	-	enable	-
vd23	VDSL	.	.	down	-	enable	-
vd24	VDSL	.	.	down	-	enable	-

ifname	type	shut	block	link	nego	set-speed	cur-speed	linkup-time
gi1	GE-T	.	.	down	auto	auto/full	.	-
gi2	GE-T	.	.	down	auto	auto/full	.	-

U3024#

 **Notice** The CLI capture screens for the examples given below are based on U3024B. See the interface ID <Table 22> 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.

```
U3024# show switchport
```

```
IFNAME    SWMODE N-VLAN TAGGED-VLAN-LIST
```

```
-----
```

vd1	access	1
vd2	access	1
vd3	access	1
vd4	access	1
vd5	access	1
vd6	access	1
vd7	access	1
vd8	access	1
vd9	access	1
vd10	access	1
vd11	access	1
vd12	access	1
vd13	access	1
vd14	access	1
vd15	access	1
vd16	access	1
vd17	access	1
vd18	access	1
vd19	access	1
vd20	access	1
vd21	access	1
vd22	access	1
vd23	access	1
vd24	access	1
gi1	access	1
gi2	access	1

```
-----
```

```
total 26 interfaces listed
```

```
U3024#
```

Setting Physical Port Environment

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

<Table 24> 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	<ul style="list-style-type: none"> ▪ 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 vd1
U3024B (config-if-vd1)# shutdown          <- disable port
U3024B (config-if-vd1)# 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 vd1
U3024B(config-if-vd1)# block             <- block port
U3024B(config-if-vd1)# no block         <- unblock port
```

Speed and Duplex

The speeds supported by each interface of U3024B are listed below.

<Table 25> Speed and Duplex

Type	Auto-negotiation	Speed	Duplex
100Base-TX	on	10/100/auto	full/half/auto
	off	10/100	full/half
100Base-FX	off	100	full
1000Base-T	on	10/100/1000/auto	full/half/auto
	off	1000	full
1000Base-X	on	1000	full
	off	1000	full

Note the following when setting speed and duplex.

- In case of 1000Base-FX, speed setting is unnecessary but only auto-negotiation on/off setting is applicable. In case of auto-negotiation on, link down will be detected on both sides even an optical cable line is shut down (remote fault detection)
- 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.

U3024B can mirror rx and tx traffic from several source ports to one target port.

<Table 26> Port mirroring

Command	Description	Mode
mirroring target <i>ifname</i>	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 U3024B 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 U3024B 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 U3024B include trunk mode and access mode.

<Table 27> Layer 2 Interface Modes Supported by U3024B

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 U3024B provides the default settings as follows.

<Table 28> 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 29> 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 30> 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 vd1
Switch(config-if-vd1)# switchport           ! Set layer2 interface
Switch(config-if-vd1)# switchport mode trunk ! Set trunk port
Switch(config-if-vd1)# switchport trunk native 2 ! Set native vlan
Switch(config-if-vd1)# switchport trunk add 3 ! Add tagged vlan
Switch(config-if-vd1)# switchport trunk add 4
Switch(config-if-vd1)# 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 31> 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 (VLAN 1)	interface
----------------------------------	---	-----------

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

```
Switch # configure terminal
Switch (config)#interface vd1
Switch(config-if-vd1)# switchport           ! Set layer2 interface
Switch(config-if-vd1)# switchport mode access ! Set access port
Switch(config-if-vd1)# 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 U3024B, a port group interface can be used as a Layer 2 interface.

The number of port groups applicable to the U3024B is given below.

Model	Port Groups	Maximum ports per group
U3024B	7	8

Port Group Configuration

The commands to configure a port group are listed below.

<Table 32> 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 33> Commands for Setting MAC-filter

Command	Description	Mode
mac-filter <i>vlan-id mac-addr</i>	Adds MAC filter	config
no mac-filter <i>vlan-id mac-addr</i>	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 34> 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 observing-period 2
Switch(config)# interface vd1
Switch(config-if-vd1)# traffic-control pps unicast inbound 100000 50000 alarm-only
Switch(config-if-vd1)# traffic-control pps broadcast inbound 100000 50000 alarm-only
Switch(config-if-vd1)# end
Switch # show traffic-control
Traffic Control Status
```

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

```
Interface : vd1
Status    : Normal
```

	High Threshold	Low Threshold	Average Rate	1 Minute Rate	Alarm 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

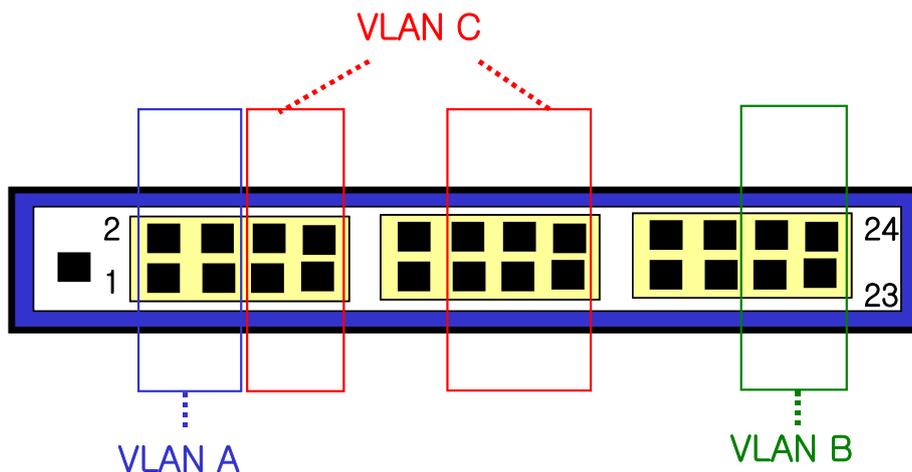
The U3024B can support up to 256 VLANs. VLAN is created according to the following conditions:

- 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 U3024B shown in <Figure >, 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> An Example of Port-Based VLAN Configuration of U3024B Switch

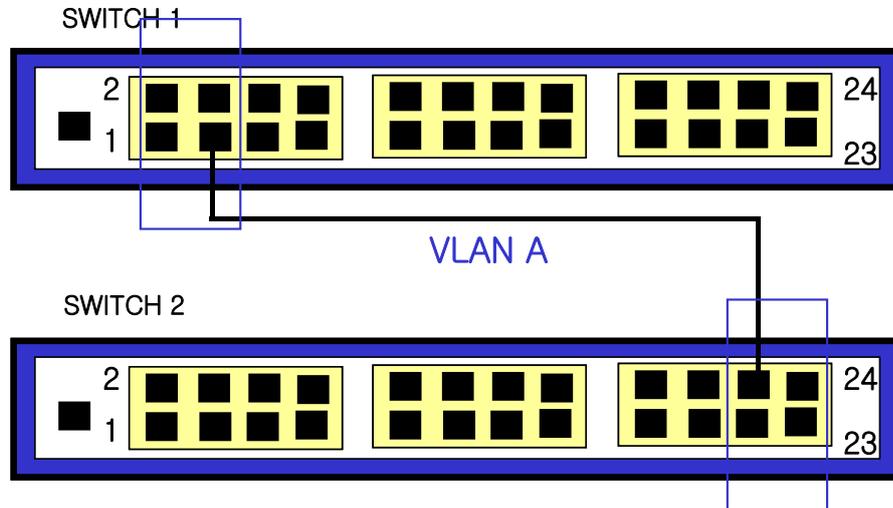
For communication between members of different VLANs, frames should be routed through the switch although they are physically a part of the same I/O module. This means that each VLAN should be defined as a router interface with a unique IP address.

Grouping Switches into Port-Based VLAN

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

1. Assign an access port for VLAN in each switch.
2. 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.

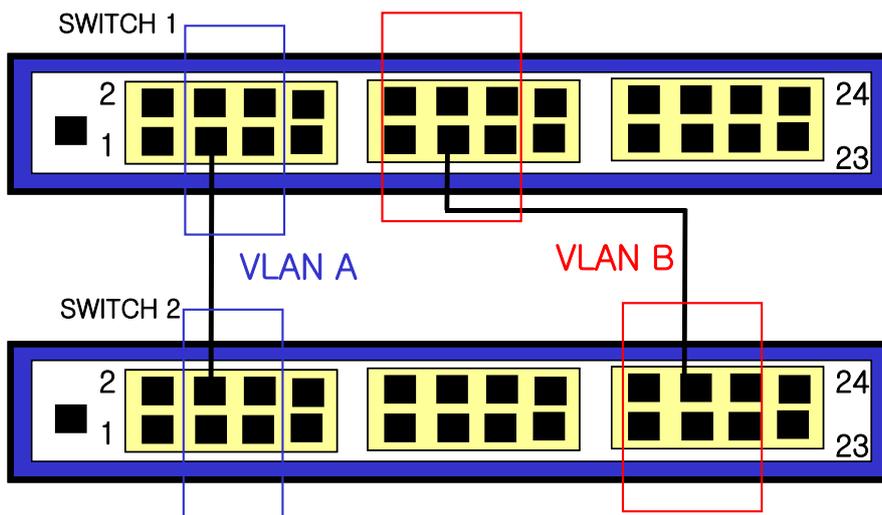
<Figure 3> shows an example of grouping two U3024B switches into one VLAN. Four ports of U3024B-1 are assigned to VLAN A, and four ports of U3024B 2 are assigned as access ports of VLAN A. As seen in <Figure 3>, the two switches are connected to form one broadcast domain.



<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.

<Figure 4> shows two VLANs configured using two U3024B switches. 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, U3024B- 1 is connected to U3024B- 2 through port 3 of U3024B- 1 and port 4 of U3024B- 2. In VLAN B, U3024B- 1 is connected to U3024B- 2 through port 11 of U3024B- 1 and port 20 of U3024B- 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 <Figure 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

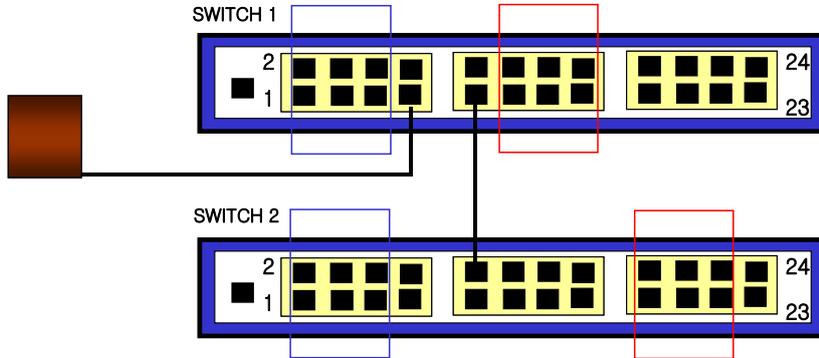
When a VLAN is created, it is assigned with VLANid. A port defined as a trunk port of tagged VLAN uses frames with 802.1Q VLAN tag attached. In this case, VLANid of the tagged VLAN is used as a tag for those frames.

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.

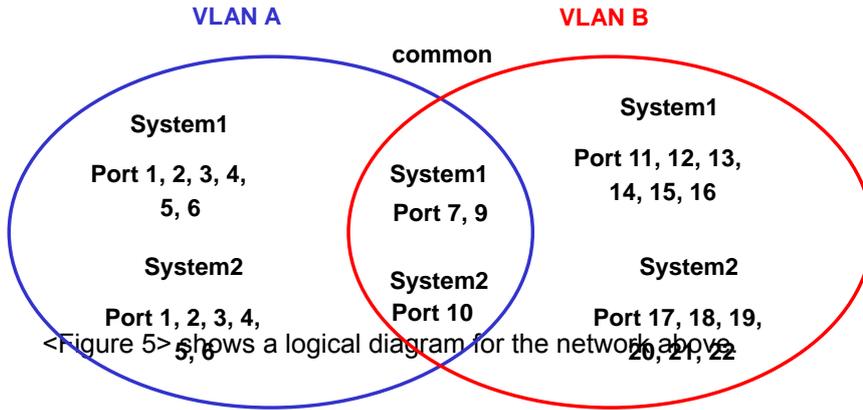
**Notice**

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



<Figure 5> shows a logical diagram for the network above.

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

In <Figure 5> and

<Figure >:

- 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

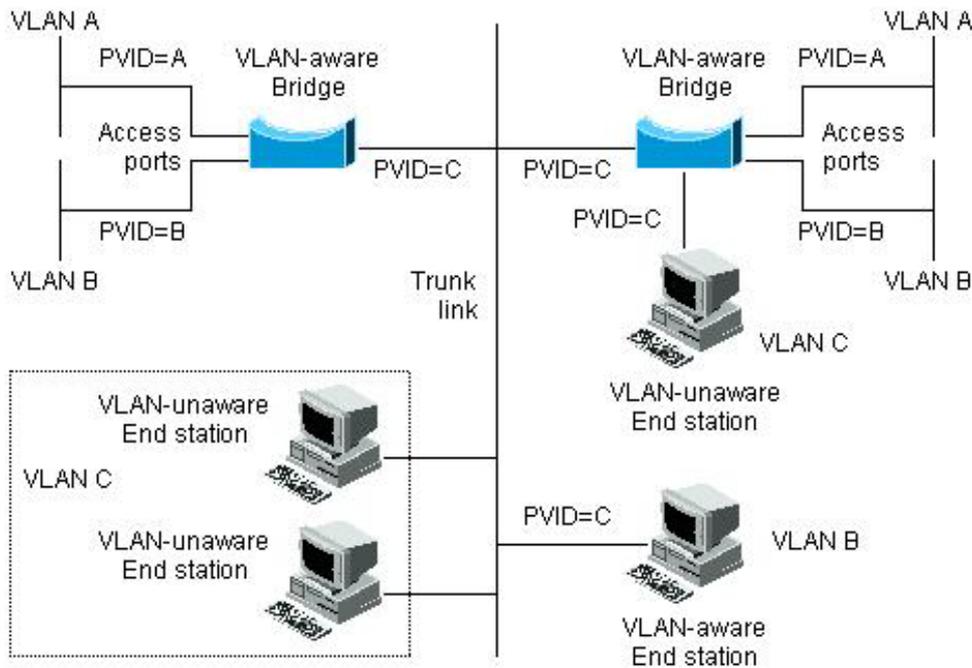
Default VLAN defined in a switch is featured as follows.

- 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 <Figure , 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 <Figure 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 U3024B switch. 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 35> VLAN Setup Commands

Command	Description	Mode
<code>vlan <i>vlanid</i></code>	Creates deletes and modifies VLAN parameters. 1 is reserved for the default VLAN. <i>vlanid</i> : A value between 2 and 4094.	config
<code>switchport mode {access trunk}</code>	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
<code>switchport access vlan <i>vlanid</i></code>	Sets an access port of VLAN. The port set to access mode will act as a member of VLAN. <i>vlanid</i> : A value between 1 and 4094	Interface
<code>switchport trunk add <i>vlanid</i></code>	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. <i>vlanid</i> : A value between 2 and 4094. The default VLAN(VLANid=1) is port-based VLAN.	Interface
<code>switchport trunk native <i>vlanid</i></code>	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. <i>vlanid</i> : A value between 1 and 4094.	Interface
<code>switchport trunk remove {<i>vlanid</i> all}</code>	Removes a member of VLAN for the specified port. <i>vlanid</i> : A value between 2 and 4094. all : Deletes the member from all VLANs.	Interface

Example of VLAN Setup

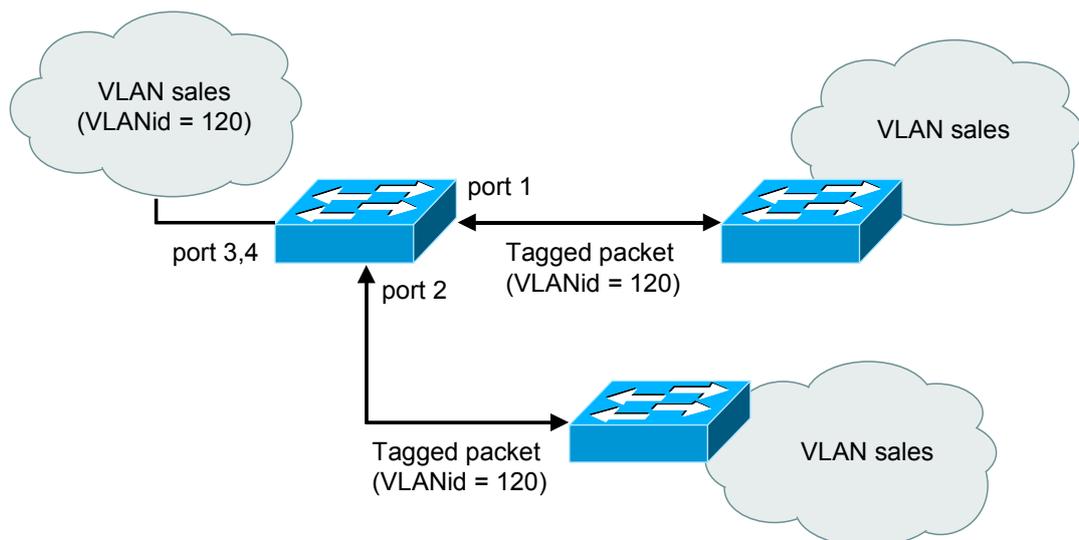
The following shows an example of setting VLANid to 1000 and IP address 132.15.121.1 to VLAN and assigning port 2 and port 4 to VLAN.

```
Switch(config)# vlan 1000
Switch(config)# interface vlan1000
Switch(config-int-vlan)# ip address 132.15.121.1/24
Switch(config-int-vlan)# interface vd2
Switch(config-int-vd2)# switchport mode access
Switch(config-int-vd2)# switchport access vlan 1000
Switch(config-int-vd2)# interface vd4
Switch(config-int-vd4)# switchport mode access
Switch(config-int-vd4)# 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 vd1
Switch(config-int-vd1)# switchport mode trunk
Switch(config-int-vd1)# switchport trunk add 2000
Switch(config-int-vd1)# interface vd2
Switch(config-int-vd2)# switchport mode trunk
Switch(config-int-vd2)# 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 vd1
```

```
Switch(config-int-vd1)# switchport mode trunk
Switch(config-int-vd1)# switchport trunk add 120
Switch(config-int-vd1)# interface vd2
Switch(config-int-vd2)# switchport mode trunk
Switch(config-int-vd2)# switchport trunk add 120
Switch(config-int-vd2)# interface vd3
Switch(config-int-vd3)# switchport access vlan 120
Switch(config-int-vd3)# interface vd4
Switch(config-int-vd4)# 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 vd1
Switch(config-int-vd1)# switchport mode trunk
Switch(config-int-vd1)# switchport trunk native 200
Switch(config-int-vd1)# switchport trunk add 400
```

The switch will transfer untagged frames received through the port vd1/1 to member port of VLAN *marketing*.

Viewing VLAN Configuration

Use the following command to view the VLAN setup information.

<Table 36> Viewing VLAN Configuration

Command	Description	Mode
show vlans	Shows the following information on VLAN. <ul style="list-style-type: none"> VLANid Member port 	Privileged

Switch# **show vlans**

VLAN MEMBER-LIST

```

-----
 1 vd1  vd2  vd3  vd4  vd5  vd6  vd7  vd8  vd9  vd10
   vd11 vd12 vd13 vd14 vd15 vd16 vd17 vd18 vd19 vd20
   vd21 vd22 vd23 vd24 gi1  gi2
-----

```

Total 1 VLANs listed 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 U3024B 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 lists IP address ranges, reserved addresses and available addresses.

<Table 37> 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 U3024B supports assigning several IP addresses to one interface. The U3024B 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 38> Command for Assigning an IP Address

Command	Description
ip address <i>ipaddress/prefixlen</i>	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 39> 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 40> Command for Setting a Default Gateway

Command	Description
ip default-gateway <i>gateway-ipaddress</i>	Registers a default gateway. gateway-ipaddress : IP address of gateway.

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

<Table 41> Displaying Default Gateway

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
Flags>> R: reachable D: delay P: permanent
-----
IP Address      MAC Address      Interface PORT      Flags
-----
192.10.25.1     00:07:70:9e:64:d2 eth0      eth0      D
-----
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

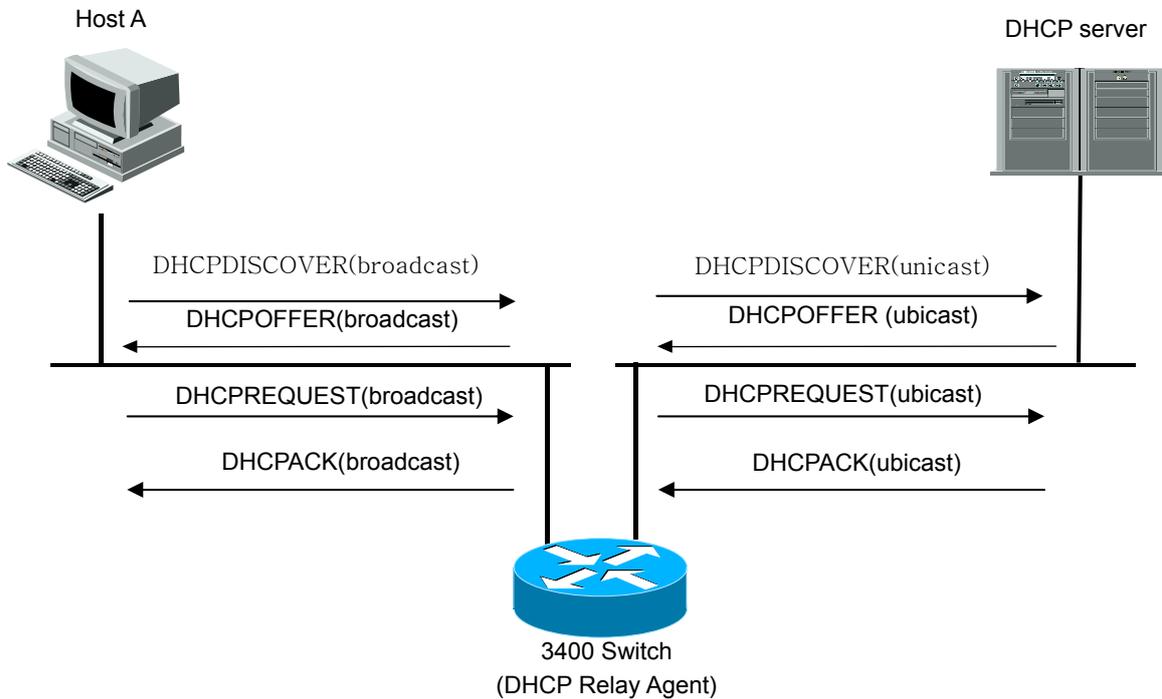
This chapter describes how to set DHCP Relay.

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 U3024B 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 42> 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

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

<Table 43> Setting DHCP server at DHCP relay agent

Command	Description
ip dhcp-server <i>address</i>	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

U3024B can have upto 20 helper-address as a DHCP relay Agent.

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

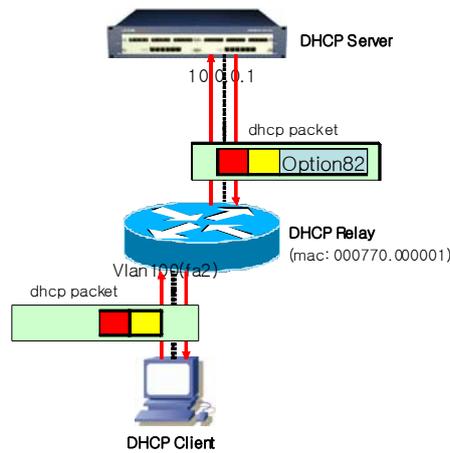
```
Switch# configure terminal
Switch(config)# ip dhcp helper-address 192.168.0.254
Switch(config)# exit
Switch#
Switch#
Switch# show ip dhcp relay

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 44> 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 U3024B 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 45> 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
    
```

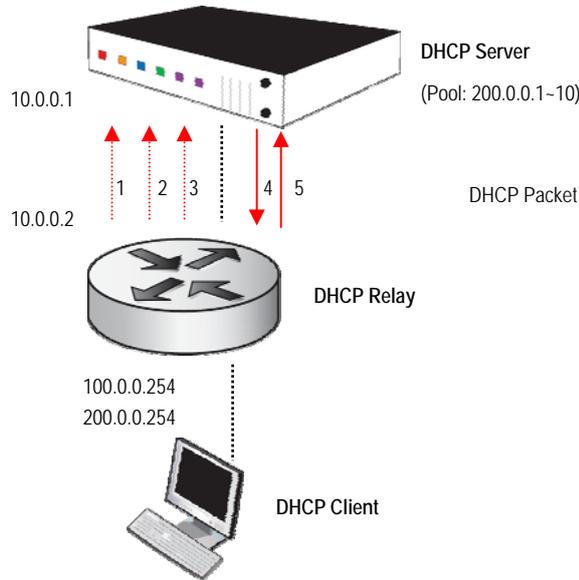
```

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 46> 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 47> 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 function is used.

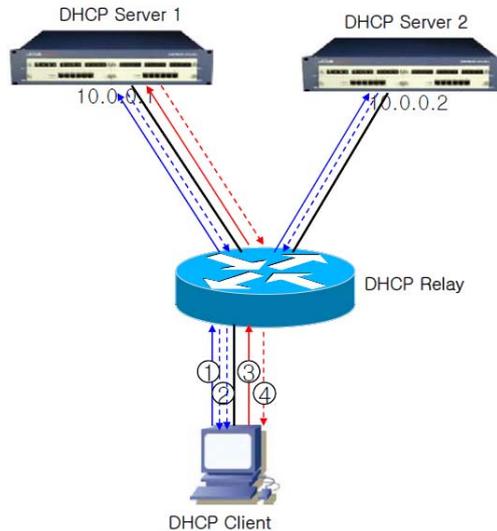
```
Switch# configure terminal
Switch(config)# no ip dhcp relay verify mac-address
Switch(config)# exit
Switch# show ip dhcp relay

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 48> 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
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 49> Commands for DHCP relay monitor and management

Command	Description
show ip dhcp relay	Display the DHCP Relay Configuration
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 50> Field Title

Field title	Meaning
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 create 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.

Configuring DHCP Snooping

When U3024B is enabled for DHCP Snooping, the switch will conduct Snooping with every DHCP packets that pass through it to create 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 51> 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 52> Configuring DHCP Snooping Vlan

Command	Description
ip dhcp snooping vlan <i>vlan_ID</i>	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 Vlan 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 53> Activation of DHCP snooping information option function

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 U3024B'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 54> IP DHCP snooping Information Policy

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

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 55> 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 'vd1' is set to be Trust Port.

```
Switch(config)# interface vd1
Switch(config-if-vd1)# ip dhcp snooping trust
Switch(config-if-vd1)# end
Switch# show ip dhcp snooping interface
```

Interface	Trust State	Max Entry
vd1	Trusted	2000
vd2	Untrusted	2000
vd3	Untrusted	2000
vd4	Untrusted	2000
vd5	Untrusted	2000
vd6	Untrusted	2000
vd7	Untrusted	2000
vd8	Untrusted	2000
vd9	Untrusted	2000
vd10	Untrusted	2000
vd11	Untrusted	2000
vd12	Untrusted	2000
vd13	Untrusted	2000
vd14	Untrusted	2000
vd15	Untrusted	2000
vd16	Untrusted	2000
vd17	Untrusted	2000
vd18	Untrusted	2000
vd19	Untrusted	2000
vd20	Untrusted	2000
vd21	Untrusted	2000
vd22	Untrusted	2000
vd23	Untrusted	2000
vd24	Untrusted	2000
gi1	Untrusted	2000
gi2	Untrusted	2000

Configuring DHCP snooping max-entry

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

<Table 56> 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 'vd1' is set to be '100'.

```
Switch# configure terminal
Switch(config)# interface vd1
Switch(config-if-vd1)# ip dhcp snooping max-entry 100
Switch(config-if-vd1)# end
Switch# show ip dhcp snooping interface
```

Interface	Trust State	Max Entry
vd1	Trusted	100
vd2	Untrusted	2000
vd3	Untrusted	2000
vd4	Untrusted	2000
vd5	Untrusted	2000
vd6	Untrusted	2000
vd7	Untrusted	2000
vd8	Untrusted	2000
vd9	Untrusted	2000
vd10	Untrusted	2000
vd11	Untrusted	2000
vd12	Untrusted	2000
vd13	Untrusted	2000
vd14	Untrusted	2000
vd15	Untrusted	2000
vd16	Untrusted	2000
vd17	Untrusted	2000
vd18	Untrusted	2000
vd19	Untrusted	2000
vd20	Untrusted	2000
vd21	Untrusted	2000
vd22	Untrusted	2000
vd23	Untrusted	2000
vd24	Untrusted	2000
gi1	Untrusted	2000
gi2	Untrusted	2000

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 57> 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 58> 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 59> 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 60> DHCP Snooping Manual Binding configuration

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

In the following example, a user whose MAC address is 1111.2222.3333 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

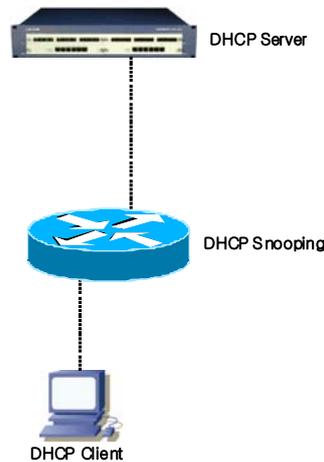
Commands for monitoring and managing DHCP Snooping

<Table 61> 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 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.



```
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         vd1/8
```

Chapter 6. IGMP Snooping

This chapter describes IGMP snooping in the U3024B switch.

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 VLAN, 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 62> 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 63> 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 vd1
Switch (config-if-vd1)# igmp-trap
Switch (config-if-vd1)# end
Switch # show running-configure
...
!
interface vd1
  igmp-trap
```

Enable IGMP Snooping on a VLAN

You should enable/disable IGMP snooping for an individual VLAN in the U3024B switch.

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

<Table 64> 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 : vd1 vd2 vd3 vd4
```

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 65> 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 # **show ip igmp snooping**

Global IGMP Snooping configuration:

- Aging Interval : 300 sec
- Last Member Join Interval : 300 sec
- TCN Query Solicit : DISABLED
- IGMP Report Suppression : **ENABLED**

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 : vd1 vd2 vd3 vd4

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 66> 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 vd1
Switch (config)# ip igmp snooping vlan 1 fast-leave vd2
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 ENABLED on vd1 vd2
    IGMP snooping mr-learn is DISABLED on this interface
    Vlan Members : vd1 vd2 vd3 vd4
Switch #
```

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 67> 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 vd1**

Switch # **show ip igmp snooping mrouter**

```
VLAN      MULTICAST-ROUTER-PORT
0001      vd1
```

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

<Table 68> Setting Mrouter 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 # 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 ENABLED on this interface
    Vlan Members : vd1 vd2 vd3 vd4
```

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 69> 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 # show ip igmp snooping
Global IGMP Snooping configuration:
- Aging Interval : 250 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 : vd1 vd2 vd3
```

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 70> 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 # show ip igmp snooping
Global IGMP Snooping configuration:
- Aging Interval : 300 sec
- Last Member Join Interval : 5 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 : vd1 vd2 vd3
```

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 71> 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 # show ip igmp snooping
Global IGMP Snooping configuration:
- Aging Interval           : 300 sec
- Last Member Join Interval : 300 sec
- TCN Query Solicit       : ENABLED
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 vd1 vd2 vd3
```

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 72> 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 # **show ip igmp snooping profile**

IGMP Profile 1

deny

range : 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

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

<Table 73> Applying IGMP Fitering

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 vd1
Switch (config-if-vd1)# ip igmp snoop-filter 1
Switch # show running-configure
...
!
interface vd1
ip igmp snoop-filter 1
...
Switch #
```

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 74> 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 vd1 10
Switch # show running-configure
...
ip igmp snooping
ip igmp snooping max-group-count vd1 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 75> Setting IGMP Max-Reporter-Count

Command	Description
ip igmp snooping max-reporter-count vlan <i><vlan-id> <count></i>	Applies max-reporter-count for a VLAN interface.
no ip igmp snooping max-reporter-count vlan <i><vlan-id></i>	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 #
```

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 76> Configuring drop-igmp-ttl-over

Command	Description
ip igmp snooping drop-igmp-ttl-over <i><1-255></i>	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 77> 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 78> 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)#
Switch # show ip igmp snooping proxy-reporting interface
IGMP Proxy Interface
IGMP Gateway is DISABLED on ALL interface.
```

```
total : 0
Switch #
Switch #
```

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 79> 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 proxy-reporting interface**

IGMP Proxy Interface

vlan1

IGMP Proxy is ENABLED on this interface

IGMP Query-Interval is 60 seconds.

IGMP Leave-Timeout is 10 seconds.

IGMP Query-Max-Response-Time is 10 seconds.

Multicast Router Port : NOT CONFIGURED!

VLAN Members :

vd1 vd2 vd3

total : 1

Switch #

Configure IGMP Proxy-Reporting Functionality

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

Setting Static Multicast Router Port

You can set a static multicast router port to interwork with a higher multicast router for IGMP membership information managed by IGMP proxy-reporting. In case static multicast router port is not specified, the port that dynamically receives IGMP Query message will be acknowledged as a multicast router port.

The IGMP proxy-reporting switch does not act as an IGMP Querier until a multicast router port is acknowledged and initiates to act as an IGMP Querier to manage subscriber's IGMP membership after a multicast router port has been acknowledged statically or dynamically.

<Table 80> Setting Static Multicast Router Port

Command	Description
ip igmp snooping proxy-reporting vlan <1-4096> mrouter-port IFNAME	Sets a multicast router port for IGMP proxy-reporting for a specific VLAN.
no ip igmp snooping proxy-reporting vlan <1-4096> mrouter-port IFNAME	Deletes the multicast router port for IGMP proxy-reporting specified for a VLAN.

```
Switch # configure terminal
Switch (config)# ip igmp snooping proxy-reporting vlan 1 mrouter-port vd1
Switch (config)#
Switch # show ip igmp snooping proxy-reporting interface
IGMP Proxy Interface
vlan1
    IGMP Proxy is ENABLED on this interface
    IGMP Query-Interval is 60 seconds.
    IGMP Leave-Timeout is 10 seconds.
    IGMP Query-Max-Response-Time is 10 seconds.
Multicast Router Port : vd1
VLAN Members:
vd1 vd2 vd3
total: 1
Switch #
```

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 81> 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 # **show ip igmp snooping proxy-reporting group**

VLAN	GROUP	LAST-REPORTER	EXPIRE-TIME
0080	224.1.1.1	0.0.0.0	00:04:03 STATIC-GROUP

total : 1

Switch #

Display System and Network Statistics

<Table 82> 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 suppression-forwarder	Shows the information on forwarder of the suppressed multicast group.

<Table 83> Commands for Monitoring IGMP Proxy-Reporting

Command	Description
show ip igmp snooping proxy-reporting interface	Shows the IGMP proxy-reporting status of all VLANs.
show ip igmp snooping proxy-reporting group	Shows the information on IGMP membership management.
show ip igmp snooping proxy-reporting querier	Shows the information on all IGMP Queriers acknowledged.

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 U3024B 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 84> 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

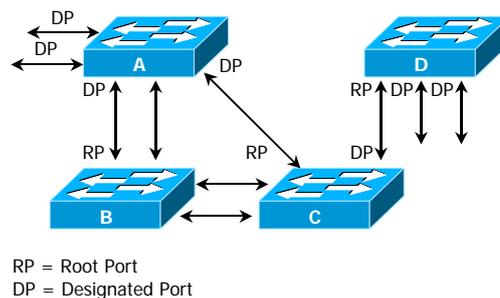
The table below describes the timers affecting performance of a spanning-tree.

<Table 85> 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 15> 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.

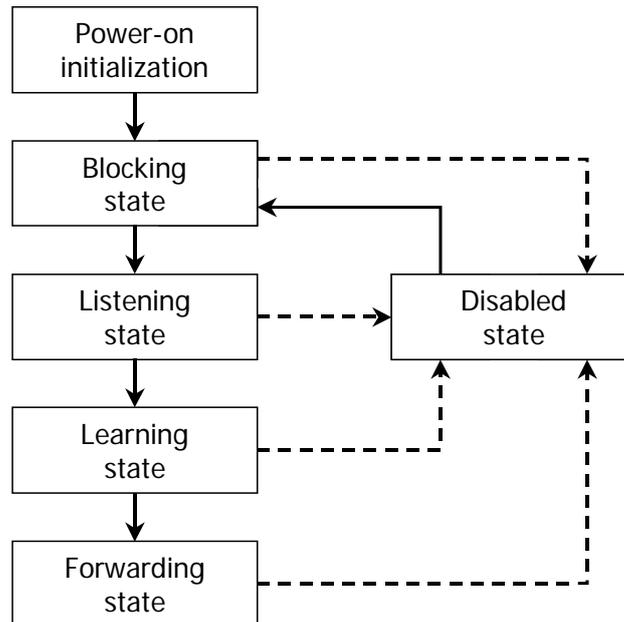
A Layer 2 interface of the switch with spanning tree enabled is one of the following states:

- 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 16> 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

<p>Listening State</p>	<p>Listening state comes after the blocking state. If an interface decides to forward the frames, it goes into listening state.</p> <p>An interface acts as following in listening state:</p> <ul style="list-style-type: none"> • Drops the frames received through the port • Drops the frames switched from other interfaces • Does not perform address learning • Receives BPDUs
<p>Learning State</p>	<p>In learning state, a Layer 2 interface is ready to forward frames. The interface goes from listening state to learning state.</p> <p>In learning state, an interface acts as follows:</p> <ul style="list-style-type: none"> • Drops the frames received through the port • Drops the frames switched from other interfaces • Performs address learning • Receives BPDUs
<p>Forwarding State</p>	<p>In forwarding state, a Layer 2 interface forwards frames. The interface goes from learning state to forwarding state.</p> <p>In forwarding state, an interface acts as follows:</p> <ul style="list-style-type: none"> • Forwards the frames received through the port • Forwards the frames switched from other interfaces • Performs address learning • Receives BPDUs
<p>Disable State</p>	<p>In disabled state, a Layer 2 interface does not participate in frame forwarding or spanning tree.</p> <p>A disabled interface acts as follows:</p> <ul style="list-style-type: none"> • 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 86> Port State Comparison

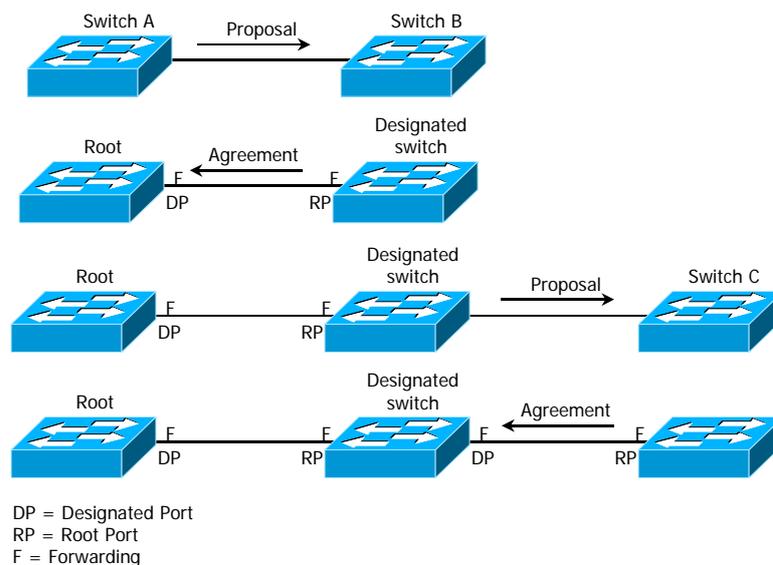
Operational Status	STP Port State	RSTP Port State	Is Port Included in the Active Topology?
Enabled	Blocking	Discarding	No
Enabled	Listening	Discarding	No
Enabled	Learning	Learning	Yes
Enabled	Forwarding	Forwarding	Yes
Disabled	Disabled	Discarding	No

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 26> 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 87> 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 88> 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 U3024B supports IEEE 802.1w RSTP. As 802.1D STP is internally included in 802.1w, the U3024B 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 89> Enabling STP

	Command	Purpose
Step1	configure terminal	Enters global configuration mode.
Step2	spanning-tree vlan <i>vlan-id</i>	Enables STP by VLAN. VLAN ranges from 1 to 4094.
Step3	End	Changes to privileged EXEC mode.
Step4	show spanning-tree vlan <i>vlan-id</i>	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***.

Disable per VLAN STP

The U3024B 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 90> 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**.

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 91> Configuring the Port Priority

	Command	Purpose
Step1	configure terminal	Enters the global configuration mode.
Step2	interface <i>interface-id</i>	Specifies an interface and enters interface configuration mode. Effective interfaces include physical interfaces and port groups.
Step3	spanning-tree vlan <i>vlan-id</i> port-priority <i>priority</i>	Sets a VLAN port priority of the interface. <ul style="list-style-type: none"> • <i>vlan-id</i> ranges from 1 to 4094. • <i>priority</i> 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 <i>interface-id</i> or show spanning-tree vlan <i>vlan-id</i>	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**.

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 92> Configuring the Path Cost

	Command	Purpose
Step1	configure terminal	Enters global configuration mode.
Step2	interface <i>interface-id</i>	Specifies an interface and enters interface configuration mode. Effective interfaces include physical interfaces and port groups.
Step3	spanning-tree vlan <i>vlan-id</i> cost <i>cost</i>	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. <ul style="list-style-type: none"> ● <i>vlan-id</i> ranges from 1 to 4094. ● <i>cost</i> 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 <i>interface-id</i> or show spanning-tree vlan <i>vlan-id</i>	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**.

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 93> Configuring the Switch Priority of a VLAN

	Command	Purpose
Step1	configure terminal	Enters global configuration mode.
Step2	spanning-tree vlan <i>vlan-id</i> priority <i>priority</i>	Sets a switch priority for VLAN. <ul style="list-style-type: none"> • <i>vlan-id</i> ranges from 1 to 4094. • <i>priority</i> 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 <i>vlan-id</i>	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**.

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 94> Configuring the Hello Time

	Command	Purpose
Step1	configure terminal	Enters global configuration mode.
Step2	spanning-tree vlan <i>vlan-id</i> hello-time <i>seconds</i>	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. <ul style="list-style-type: none">• <i>vlan-id</i> ranges from 1 to 4094.• <i>seconds</i> ranges from 1 to 10. The default setting is 2.
Step3	End	Changes to privileged EXEC mode.
Step4	show spanning-tree vlan <i>vlan-id</i>	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**.

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 95> Configuring the Forwarding-Delay Time for a VLAN

	Command	Purpose
Step1	configure terminal	Enters global configuration mode.
Step2	spanning-tree vlan <i>vlan-id</i> forward-time <i>seconds</i>	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. <ul style="list-style-type: none"> • <i>vlan-id</i> ranges from 1 to 4094. • <i>seconds</i> ranges from 4 to 30. The default setting is 15.
Step3	End	Changes to privileged EXEC mode.
Step4	show spanning-tree vlan <i>vlan-id</i>	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**.

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 96> Configuring the Maximum-Aging Time for a VLAN

	Command	Purpose
Step1	configure terminal	Enters global configuration mode.
Step2	spanning-tree vlan <i>vlan-id</i> max-age <i>seconds</i>	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. <ul style="list-style-type: none"> ● <i>vlan-id</i> ranges from 1 to 4094. ● <i>seconds</i> ranges from 6 to 40. The default setting is 20.
Step3	End	Changes to privileged EXEC mode.
Step4	show spanning-tree vlan <i>vlan-id</i>	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**.

Configuring the Port as Edge Port

To enable STP in the U3024B, 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 97> Configuring the Port as Edge Port

	Command	Purpose
Step1	configure terminal	Enters global configuration mode.
Step2	Interface <i>interface-id</i>	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**.

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 98> Configuring the RSTP Mode

	Command	Purpose
Step1	configure terminal	Enters global configuration mode.
Step2	spanning-tree vlan <i>vlan-id</i> force-version rstp	Sets protocol mode to RSTP mode for an RSTP instance of a specific VLAN. <i>vlan-id</i> 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**.

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 99> Specifying the Link Type to Ensure Rapid Transitions

	Command	Purpose
Step1	configure terminal	Enters global configuration mode.
Step2	interface <i>interface-id</i>	Sets an interface and enters interface configuration mode.
Step3	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**.

Displaying the Spanning-Tree Status

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

<Table 100> Displaying the Spanning-Tree Status

Command	Purpose
show spanning-tree active	Shows the spanning-tree information on active interfaces only.
show spanning-tree interface <i>interface-id</i>	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.

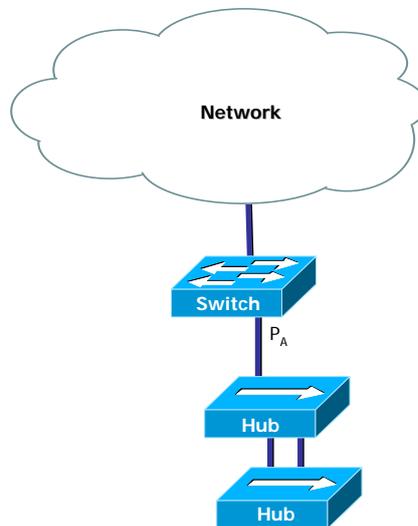
Self-loop Detection

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 18> 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).

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.

When 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 101> Enabling Self-loop Detection

	Command	Purpose
Step1	Configure terminal	Enters global configuration mode.
Step2	interface <i>interface-name</i>	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 vd1 with the default limit time:

```
Switch# configure terminal
Switch(config)# interface vd1
Switch(config-if-vd1)# self-loop-detection
Switch(config-if-vd1)# end
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 102> Changing the Service Status of Port

	Command	Purpose
Step1	Configure terminal	Enters global configuration mode.
Step2	interface <i>interface-name</i>	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 103> Disabling Self-loop Detection

	Command	Purpose
Step1	Configure terminal	Enters global configuration mode.
Step2	interface <i>interface-name</i>	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 vd1:

```
Switch# configure terminal
Switch(config)# interface vd1
Switch(config-if-vd1)# no self-loop-detection
Switch(config-if-vd1)# end
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 vd5
  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
vd1	.	down	.	.	.	0	.
vd2	.	up	.	.	.	0	.
vd3	.	down	.	.	.	0	.
vd4	.	down	.	.	.	0	.
vd5	set	up	set	5 min	.	1	May 29 04:48:39 2006
vd6	.	down	.	.	.	0	.
vd7	.	down	.	.	.	0	.
vd8	.	down	.	.	.	0	.

```
Switch#
```

Chapter 8. Stacking

This chapter describes the stacking function to manage several switches with one IP address.

This chapter is organized into the following sections:

- Stacking Overview
- Configuring Stacking Features
- Displaying the Stacking Status

Stacking Overview

The U3024B can manage several switches with one IP address. The switch with a master IP address is called *Master switch*, and the other switches in the switch group managed by the master switch are called *Slave switches*.

The U3024B can be stacked regardless of network topology only if the master switch and slave switches are linked through a common VLAN. The VLAN connecting the master switch with slave switches are called *Stack VLAN*.

Configuring Stacking Feature

This section describes how to configure the stacking feature:

- Configuring the Stack VLAN
- Configuring the Stack Member
- Enabling the Stack
- Connecting to Slave Switch

Configuring the Stack VLAN

For stacking, a common VLAN, Stack VLAN, should be configured for communication between master switch and slave switches.



Note

It is recommended to isolate VLAN to isolate general traffic from stacking traffic. In other words, create a separate trunk VLAN and define it as a stack VLAN.

You can define a stack VLAN in privileged EXEC mode as follows:

<Table 104> Configuring the Stack VLAN

	Command	Purpose
Step1	configure terminal	Enters Global configuration mode.
Step2	stack vlan <i>vlan-id</i>	Defines a stack VLAN. <i>vlan-id</i> ranges from 1 to 4094. The default setting is VLAN 1.
Step3	End	Changes to privileged EXEC mode.
Step4	show running-config	Views the settings.
Step5	copy running-config startup-config	Saves the (option) settings in the configuration file.

The global configuration command **no stack vlan** is used to restore the default setting of the stack VLAN.

Configuring the Stack Member

You should register the slave switches to be managed in the master switch.



Note

This command is meaningful only in the master switch and does not affect operation when defined in a slave switch. The registered switches should be included in the same VLAN (Stack VLAN) as the master switch.

You can register a slave switch in privileged EXEC mode as follows:

<Table 105> Configuring the Stack Member

	Command	Purpose
Step1	configure terminal	Enters Global configuration mode.
Step2	stack member <i>node-id mac-address</i>	Registers a slave switch. <ul style="list-style-type: none"> • <i>node-id</i> ranges from 2 to 5. • <i>mac-address</i> is given in the format AABB.CCDD.EEFF.
Step3	End	Changes to privileged EXEC mode.

Step4	show running-config	Views the settings.
Step5	copy running-config startup-config	Saves the (option) settings in the configuration file.

To delete a registered switch, use the global configuration command **no stack member**.

Enabling the Stack

The stacking feature of a switch is enabled as a master switch or a slave switch.

You can enable the stack of a switch in privileged EXEC mode as follows:

<Table 106> Enabling the Stack

	Command	Purpose
Step1	configure terminal	Enters Global configuration mode.
Step2	stack role {master slave}	Enables the stack of switch. <ul style="list-style-type: none"> ● master – Acts as a master switch. ● slave – Acts as a slave switch.
Step3	End	Changes to privileged EXEC mode.
Step4	show running-config	Views the settings.
Step5	copy running-config startup-config	Saves the (option) settings in the configuration file.

To disable the stack, use the global configuration command **no stack role**.

Connecting to Slave Switch

If stacking of the master switch and slave switches is carried out successfully, it is possible to access a slave switch through the master switch. The U3024B provides a means to use the shell of slave switch.



Note This command is effective in the master switch only.

You can enable the stack of a switch in privileged EXEC mode as follows:

<Table 107> Connecting to Slave Switch

	Command	Purpose
Step1	rcommand <i>node-id</i>	Connects the master switch with a slave switch. <i>node-id</i> ranges from 2 to 5.

Displaying the Stacking Status

You can view the stacking status using the privileged EXEC command given below:

<Table 108> Displaying the Stacking Status

Command	Purpose
show stack	Shows the stacking status information.

The following shows the execution result of the **show stack** command in the master switch:

```
Switch# show stack
```

```
Node  Mac address   Status   Platform  VLAN
1      0007.7000.100a  active  P3324G    10
2      0007.7000.100c  active  P3324G    10
```

The following shows the execution result of the **show stack** command in a slave switch:

```
Switch# show stack
```

```
Stacking VLAN : 10
```

```
Node ID       : 2
```

```
Master switch : P3324G(0007.7000.100a) on VLAN 10
```

Chapter 9. Static Monitoring & Qos

This chapter describes the administration and management function through RMON (Remote Monitoring) to monitor the current status of the U3024B and to display the log information on the screen.

The statistics information provided by the U3024B 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 U3024B provides various types of status information on the user terminal using subcommands of the 'show' command.

<Table 109> 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 U3024B 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 U3024B 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.

```
U3024# show interface vd1
```

```
vd1 is link up.  
type VDSL-100-100  
line-profile is test  
alarm-profile (co) is defval  
alarm-profile (remote) is  
up speed set 100M by line-profile  
down speed set 100M by line-profile  
current speed is 100M/100M  
cpu-mac-filter disable  
  
Last clearing of counters 436:15:33  
1 minutes input rate 0 bytes/sec, 0 packets/sec  
1 minutes output rate 31 bytes/sec, 0 packets/sec  
0 packets input, 0 bytes  
Received 0 broadcasts, 0 multicasts  
0 CRC, 0 oversize, 0 dropped
```

784,985 packets output, 50,239,040 bytes
Sent 784,985 broadcasts, 0 multicasts
U3024#

<Table 110> 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 statistics IFNAME	Shows Rx/Tx bit/s, bytes/s and pkts/s of the specified interface by 5sec, 1 min and 5 min.	Config

The following shows an example of showing the counters of packets for all ports and the statistics data of a specific interface(vd1/1) 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
vd1	0	0	0	0	0	615,085
vd2	0	0	0	149	0	0
vd3	0	0	0	0	0	0
vd4	0	0	0	0	0	0
vd5	0	0	0	0	0	0
vd6	0	0	0	0	0	0
vd7	0	0	0	0	0	0
vd8	0	0	0	0	0	0
vd9	0	0	0	0	0	0
vd10	0	0	0	0	0	0
vd11	0	0	0	0	0	0
vd12	0	0	0	0	0	0
vd13	0	0	0	0	0	0
vd14	0	0	0	0	0	0
vd15	0	0	0	0	0	0
vd16	0	0	0	0	0	0
vd17	0	0	0	0	0	0
vd18	0	0	0	0	0	0
vd19	0	0	0	0	0	0
vd20	0	0	0	0	0	0
vd21	0	0	0	0	0	0
vd22	0	0	0	0	0	0
vd23	0	0	0	0	0	0
vd24	0	0	0	0	0	0
gi1	0	0	0	0	0	0
gi2	0	0	0	0	0	0

Switch#

Switch#

Switch# **show port statistics vd24**

Last clearing of counters 17:31:45

RX			TX		
bits/s	bytes/s	pkts/s	bits/s	bytes/s	pkts/s

5sec :	222656	27832	23	0	0	0
1min :	223912	27989	23	40	5	0
5min :	222840	27855	23	80	10	0
Switch#						

Using the following commands, you can change the statistics items to be displayed using 'show interface' or log High/Low thresholds for a given interface during the specified period.

<Table 111> > Commands for Viewing Port Statistics

Command	Description	Mode
load interval <5-100>	Sets an interval of mean value to be displayed with Show interface.	interface
no load interval	Clears the interval of mean value to be displayed with Show interface to the default value (60 sec)	interface
input-load-monitor <5-100> <1-1000> <1-1000>	Sets low/high thresholds for an interface during the specified period and reports them through syslog, snmp trap.	interface
no input-load-monitor	Disables Input-load-monitor.	interface

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

<Table 112> Commands for Clearing Port Statistics

Command	Description	Mode
clear counters	Clears the counters of all interfaces of the system.	privileged
clear counters IFNAME	Clears the counters for statistics on a specific interface.	privileged
clear counters snmp	Clears the snmp counters of all interfaces of the system.	privileged

CPU Traffic Statistics

U3024B, 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 1 minute 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 113> Addition of packet type

	Command	Purpose
Step1	Configure terminal	To get in Global configuration mode.
Step2a	cpu-packet-counter ethertype <i>ETHERTYPE</i>	To add new ethertype
Step2b	cpu-packet-counter ip_protocol <i>IP_PROTO</i>	To add new IP protocol
Step2c	cpu-packet-counter tcp_port <i>PORT_NUM</i>	To add new TCP port
Step2d	cpu-packet-counter udp_port <i>PORT_NUM</i>	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 is “unsigned short”, IP protoco is “unsigned char”, TCP/UDP port is “unsigned short”.

<Table 114> Removal of packet type

	Command	Purpose
Step1	Configure terminal	To get in Global configuration mode.
Step2a	no cpu-packet-counter ethertype <i>ETHERTYPE</i>	To remove the ethertype which user has added
Step2b	no cpu-packet-counter ip_protocol <i>IP_PROTO</i>	To remove the IP protocol which user has added
Step2c	no cpu-packet-counter tcp_port <i>PORT_NUM</i>	To remove the TCP port which user has added
Step2d	no cpu-packet-counter udp_port <i>PORT_NUM</i>	To remove the UDP port which user has added
Step3	end	To get back to 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.

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 115> 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 <i>IFNAME</i>	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 <i>IFNAME</i>	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 <i>IFNAME</i>	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 <i>IFNAME</i>	To display all the packet counts which come up to CPU from the specified interface according to ethertype.
show cpu-packet-counter ip_protocol <i>IFNAME</i>	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 <i>IFNAME</i>	To display all the packet counts which come up to CPU from the specified interface according to TCP port.
show cpu-packet-counter udp_port <i>IFNAME</i>	To display all the packet counts which come up to CPU from the specified interface according to UDP port.
show cpu-packet-counter type-list	To display all the types of packet that are referred in counting packets.
clear cpu-packet-counter	To clear all the stored cpu packet count.

The U3024B shows the statistics on CPU packets.

<Table 116> Command to Clear the Statistics on CPU Traffic

Command	Description	Mode
show cpu-packet-counter (all ip_icmp tcp udp)	Shows the statistics on Cpu incoming packets.	privileged

Example

```

Switch# show cpu-packet-counter all
Ip:
  15368 total packets received
  0 forwarded
  0 incoming packets discarded
  15181 incoming packets delivered
  15103 requests sent out
Icmp:
  3 ICMP messages received
  0 input ICMP message failed.
  ICMP input histogram:
    echo requests: 3
  3 ICMP messages sent
  0 ICMP messages failed
  ICMP output histogram:
    echo replies: 3
Tcp:
  0 active connections openings
  1 passive connection openings
  0 failed connection attempts
  0 connection resets received
  1 connections established
  2158 segments received
  2075 segments send out
  10 segments retransmitted
  0 bad segments received.
  1 resets sent
Udp:
  13012 packets received
  0 packets to unknown port received.
  0 packet receive errors
  13025 packets sent
TcpExt:
  1 invalid SYN cookies received
  ArpFilter: 0
  2 delayed acks sent
  1 packets directly queued to recvmsg prequeue.
  3 packets directly received from prequeue
  19 packets header predicted
  1 packets header predicted and directly queued to user
  TCPPureAcks: 4
  TCPHPAcks: 2047
  
```

TCPRenoRecovery: 0
TCPSackRecovery: 0
TCPSACKReneging: 0
TCPFACKReorder: 0
TCPSACKReorder: 0
TCPRenoReorder: 0
TCPTSReorder: 0
TCPFullUndo: 0
TCPPartialUndo: 0
TCPDSACKUndo: 0
TCPLossUndo: 0
TCPLoss: 0
TCPLostRetransmit: 0
TCPRenoFailures: 0
TCPSackFailures: 0
TCPLossFailures: 0
TCPFastRetrans: 0
TCPForwardRetrans: 0
TCPSlowStartRetrans: 0
TCPTimeouts: 2
TCPRenoRecoveryFail: 0
TCPSackRecoveryFail: 0
TCPSchedulerFailed: 0
TCPRcvCollapsed: 0
TCPDSACKOldSent: 0
TCPDSACKOfoSent: 0
TCPDSACKRecv: 2
TCPDSACKOfoRecv: 0
TCPAbortOnSyn: 0
TCPAbortOnData: 0
TCPAbortOnClose: 0
TCPAbortOnMemory: 0

Logging

The U3024B 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 U3024B stores logs in the debug level in the internal buffer and on the system console. Users 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 U3024B supports severity levels 0-7.

<Table 117> Log Levels of U3024B

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 U3024B provides the following information:

Timestamp

Timestamp logs the month, date, year and time of an event in the following format: 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 Ins
May 6 11:54:01	[5] IFM-NOTICE: Rate limit ra creation
May 7 02:10:24	[5] %REMOTE-CONNECT: login from console as Ins
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 Ins
May 7 05:23:10	[5] IFM-NOTICE: Service pa add interface vd1

Default Logging Settings

<Table 118> 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 119> Commands for Setting up System Message Logging Environment

Command	Description
logging console { <i>enable disable level</i> }	To configure the displaying the logging message into console and environment.
logging facility { <i>auth cron daemon kernel local0 local1 local2 local3 local4 local5 local6 local7 lpr mail news syslog user uucp</i> }	To configure the Facility parameter
logging flash { <i>enable disable level size</i> }	To configure whether to store the syslog message into flash.
logging server <i>A.B.C.D</i>	To configure whether to send the syslog message to external syslog server
logging session { <i>enable disable level</i> }	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.

<Table 120> Displaying Log

Command	Description
logging console {enable/disable}	Enables/disables logging on the console.
logging facility {auth cron daemon kernel local0 local1 local2 local3 local4 local5 local6 local7 pr mail news syslog user uucp}	Sets facility parameters to send syslog messages.
logging flash {enable/disable level size}	Sets environment to save syslog messages in the flash memory.
logging server A.B.C.D	Sets transmission of syslog messages to an external syslog server
logging session {enable/disable level }	Enables/disables logging on the current session.
logging source-ip A.B.C.D	Sets source ip of syslog packet
logging trap {<0-7> alert crit debug emerg err info notice warn}	Sets a logging level of syslog server
show log {<0-7> back flash }	Views the logging buffer and logging settings.
logging console {enable/disable}	Enables/disables logging on the console.

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 U3024B switch.

The following sections describe the concept of RMON and the RMON service provided by the U3024B switch.

RMON Overview

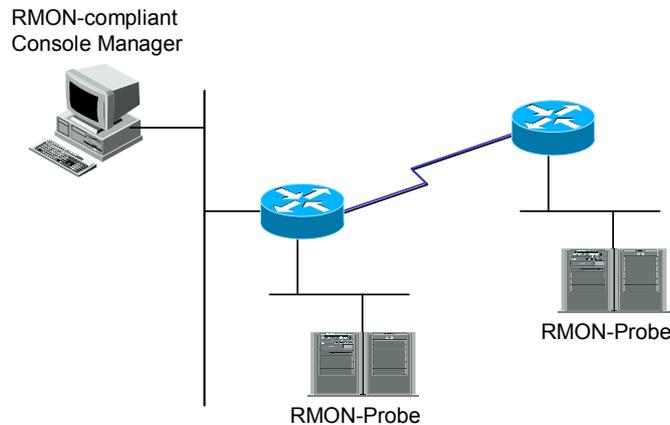
RMON enables the system operator to remotely manage the network in accordance with the international specifications defined in RFC 1271 and RFC 1757 of IETF (Internet Engineering Task Force). Typically, RMON consists of the two elements below:

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 19> 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 U3024B 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
<pre>rmon alarm <i>index</i> ifEntry <i>variable</i> ifIndex <i>interval</i> {delta absolute} rising- threshold <i>value</i> [<i>event-number</i>] falling- threshold <i>value</i> [<i>event-number</i>] [<i>owner string</i>]</pre>	<p>Adds an alarm to the alarm table of RMON</p> <p>Index : An integer from 1 to 65535.</p> <p>Variable: MIB object</p> <p>'interval' indicates a time period specified in seconds to monitor the alarm variable</p> <p>'delta' indicates monitoring a difference between samples of MIB variable and 'absolute' indicates monitoring the absolute value of MIB variable.</p> <p>Sets a rising-threshold and a falling-threshold respectively.</p> <p>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.</p> <p>Alarm owner can be defined.</p>	Config
<pre>rmon event <i>index</i> [log] [trap community <i>string</i>] [<i>owner string</i>] [<i>description string</i>]</pre>	<p>Adds an event to the RMON event table.</p> <p>'log' specifies whether or not to create a RMON log when an event occurs. 'Trap' specifies trap transmission when an event occurs.</p>	Config
<pre>no rmon alarm <i>alarm-index</i></pre>	<p>Deletes an alarm from the RMON alarm table.</p>	Config
<pre>no rmon event <i>event-index</i></pre>	<p>Deletes an event from the RMON event table.</p>	Config
<pre>show rmon alarm</pre>	<p>Shows the RMON alarm table.</p>	Privileged
<pre>show rmon event</pre>	<p>Shows the RMON event table.</p>	Privileged
<pre>show rmon log</pre>	<p>Shows the RMON log table.</p>	Privileged

```
Switch# configure terminal
Switch(config)# rmon alarm 10 ifEntry inErrors 1 20 delta rising-threshold 15 1 falling-threshold 0 owner mijiok
Switch(config)# rmon event 1 log trap community rmonTrap owner mijiok 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          : vd1
The type of Sample     : deltaValue
alarmValue              : 0
The status of starting: RISING_FALLING_ALARM
alarmRisingThreshold   : 15
alarmFallingThreshold  : 0
alarmRisingEventIndex  : 1
alarmFallingEventIndex: 1
alarmOwner              : mijiok
Switch# show rmon event
```

Event Configurations

```
The Index of event : 1
eventDescription   : "Noti:TooMuchInErrors"
eventType          : log and trap
Community          : rmonTrap
eventOwner         : mijiok
Switch#
```

<Table 123> Commands for Setting RMON Statistics and History

Command	Description	Mode
rmon history <i>index</i> ifEntry <i>ifIndex</i> [buckets <i>bucket-number</i>] [interval seconds] [owner <i>string</i>]	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 <i>index</i> ifEntry <i>ifindex</i>	Disables collecting history data.	Config
show rmon history	Shows RMON history table.	Privileged
show rmon statistics	Shows RMON statistics table.	Privileged

Switch# **show rmon statistics**

SHOW STATISTICS

```
The Index of stats : 1
Interface          : vd1
Drop Events        : 0
Total Octets       : 0
Total Packets      : 0
Broadcst Packets   : 0
Multicast Packets  : 0
CRC errors         : 0
Under Size Packets : 0
Over Size Packets  : 0
Fragments          : 0
Jabbers           : 0
Collisions         : 0
Pkts 64 Octets     : 0
Pkts 65 to 127 Oct : 0
Pkts 128 to 255 Oct : 0
Pkts 256 to 511 Oct : 0
Pkts 512 to 1023 Oct : 0
Pkts 1024 to 1518 Oct : 0
Owner              : locus
```

```
The Index of stats : 2
Interface          : fa2
Drop Events        : 0
Total Octets       : 0
Total Packets      : 0
```

.....
Switch#

Switch# **configure terminal**

Switch#(config)# **rmon history 1 ifEntry 1 buckets 20 interval 10 owner mijiok**

Switch#(config)# **exit**

Switch# **show rmon history**

SHOW HISTORY

```

===== vd1 =====
Control-index      : 1
ifindex           : 1
interval          : 10
buckets           : 20
owner             : hong
    
```

```

--- vd1 : bucket 1 ---
DropEvents        : 0
Octets            : 0
Pkts              : 0
BroadcastPkts     : 0
MulticastPkts     : 0
CRCAlignErrors    : 0
UndersizePkts     : 0
OversizePkts      : 0
Fragments         : 0
Jabbers           : 0
Collisions        : 0
Utilization       : 0
    
```

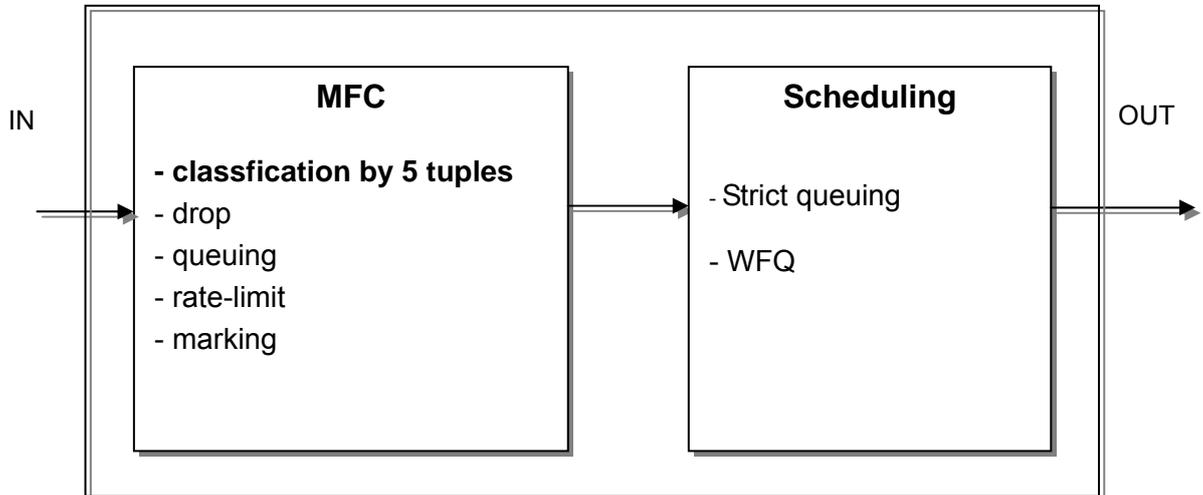
```

--- vd1 : bucket 2 ---
DropEvents        : 0
Octets            : 0
Pkts              : 0
BroadcastPkts     : 0
MulticastPkts     : 0
CRCAlignErrors    : 0
UndersizePkts     : 0
OversizePkts      : 0
Fragments         : 0
Jabbers           : 0
Collisions        : 0
Utilization       : 0
    
```

```

--- vd1 : bucket 3 ---
DropEvents        : 0
Octets            : 0
Pkts              : 0
BroadcastPkts     : 0
MulticastPkts     : 0
CRCAlignErrors    : 0
    
```

Qos and Packet Filtering



The U3024B 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.

WFQ (Weighted Fair Queuing Method)

This algorithm supplements SPQ by processing data by the weighted fair queuing defined according to the user environment.

MFC (Multi-Field Classifier)

Creating/Deleting a Flow-Rule and Setting a Mode

It is necessary to define rules to establish a policy for packet handling. For this purpose, you should first create a flow-rule and set a profile-mode properly. Classification is carried out using Mac/vlan/cos/ethertype/ipaddr/protocol in L2 mode and using Ipaddr /protocol /dscp /tos /l4port/tcp-control in L3 mode. In address mode, mac / ip addr / l4 port / protocol is used for classification.

<Table 124> Command for Creating/Deleting a Flow-Rule and Setting a Mode

Command	Description	Mode
flow-rule <i>NAME</i>	Creates a flow-rule	Config
no flow-rule <i>NAME</i>	Deletes a flow-rule	Config
flow-rule <i>NAME</i> profile-mode I2	Applies I2 profile for Mac/vlan/cos/ethertype/ipaddr/protocol	Config
flow-rule <i>NAME</i> profile-mode I3	Applies I3 profile for Ipaddr/protocol/dscp/tos/l4port/tcp-control (default)	Config
flow-rule <i>NAME</i> profile-mode address	Applies address mode for Mac / ip / l4 port / protocol.	Config

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 125> Commands for Flow-Rule Classification

Command	Description	Mode
flow-rule <i>NAME</i> classify mac {H.H.H any} {H.H.H any}	Enables classification using Mac.	Config
flow-rule <i>NAME</i> classify mac mask H.H.H H.H.H mask H.H.H H.H.H	Enables classification using Mac mask.	Config
flow-rule <i>NAME</i> classify vlan <1-4094>	Enables classification using Vlan	Config
flow-rule <i>NAME</i> classify cos <0-7>	Enables classification using Cos.	Config
flow-rule <i>NAME</i> classify ethertype <i>WORD</i>	Enables classification using Ethertype.	Config
flow-rule <i>NAME</i> classify ipaddr {A.B.C.D/M any} {A.B.C.D/M any}	Enables classification using IP address.	Config
flow-rule <i>NAME</i> classify protocol {<0-255> icmp igmp ip ospf pim tcp udp}	Enables classification using Protocol.	Config
flow-rule <i>NAME</i> classify dscp <0-63>	Enables classification using DSCP.	Config
flow-rule <i>NAME</i> classify tos <0-7>	Enables classification using Tos.	Config
flow-rule <i>NAME</i> classify l4port {<0-	Enables classification using L4 port	Config

65535> any} {<0-65535> any}	number.	
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 control fla.	Config



Notice Classification not applicable to Profile-mode will be ignored.



Notice Creating a flow-rule without classification defined indicates 'all packets'.



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 126> 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 <i>NAME</i> 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 <i>NAME</i> match mirror	Copies the packets matching with the rule to the specified mirror port.	Config
flow-rule <i>NAME</i> match replace-vlan <1-4094>	Marks the vlan of a packet matching with the rule with the specified value.	Config
flow-rule <i>NAME</i> match redirect {all unicast not-unicast} <i>INTERFACE</i> { tag untag }	Redirects the packets matching with the rule to the specified INTERFACE.	Config
flow-rule <i>NAME</i> match trap-cpu	Traps the packets matching with the rule to the CPU.	Config
flow-rule <i>NAME</i> 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 <i>NAME</i> match drop-precedence	Assigns drop-precedence to the packets matching with the rule.	Config
flow-rule <i>NAME</i> match metering	Counts the packets matching with the rule.	Config
flow-rule <i>NAME</i> match rate-limit <64-1048576>	Applies rate-limit to the packets matching with the rule.	Config
no flow-rule <i>NAME</i> match drop	Permits the packets matching with the rule.	Config
no flow-rule <i>NAME</i> match queuing	Clears queuing of the packets matching with the rule.	Config
no flow-rule <i>NAME</i> match marking cos	Clears marking of the packets matching with the rule.	Config
no flow-rule <i>NAME</i> match marking dscp	Clears marking of the packets matching with the rule.	Config
no flow-rule <i>NAME</i> match marking tos	Clears marking of the packets matching with the rule.	Config
no flow-rule <i>NAME</i> match cos-to-tos	Clears marking of the packets matching with the rule.	Config
no flow-rule <i>NAME</i> match tos-to-cos	Clears marking of the packets matching with the rule.	Config
no flow-rule <i>NAME</i> match mirror	Clears mirroring of the packets matching with the rule.	Config
no flow-rule <i>NAME</i> match replace-vlan	Clears replace-vlan of the packets matching with the rule.	Config
no flow-rule <i>NAME</i> match redirect	Clears redirection of the packets matching with the rule.	Config
no flow-rule <i>NAME</i> match trap-cpu	Clears trap-cpu of the packets matching with the rule.	Config
no flow-rule <i>NAME</i> match control-cpu-trap	Clears trap-cpu of the packets matching with the rule.	Config
no flow-rule <i>NAME</i> match drop-precedence	Clears drop-precedence of the packets matching with the rule.	Config
no flow-rule <i>NAME</i> match metering	Clears metering of the packets matching with the rule.	Config
no flow-rule <i>NAME</i> 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 Icmp snooping.

Mask-Calculator

The command 'mask-calculator' facilitates calculation of hexadecimal mask required to run the command **flow-rule NAME classify l4port mask**. If a start and an end of L4port are given, the number of the needed masks and the mask values required will be displayed.

<Table 127> Mask-Calculator Commands

Command	Description	Mode
mask-calculator <0-65535> <0-65535>	Shows the mask values for the given start and end values.	Privileged

To help your understanding, an example to meet the following condition is given below.

e.g. 1) Mask calculation to classify 100 ports of port number 4000~4100

```
Switch# mask-calculator 4000 4100
```

```
mask 0fa0 ffe0 : 4000 ~ 4031 ( 6)
mask 0fc0 ffc0 : 4032 ~ 4095 ( 7)
mask 1000 fffc : 4096 ~ 4099 ( 3)
mask 1004 ffff : 4100 ~ 4100 ( 1)
```

Required number of mask = 4

Switch#

Classification rule can be applied using the four masks above.

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 128> Command for Creating and Adding a Policy-Map

Command	Description	Mode
policy-map <i>PNAME</i> flow-rule <i>FNAME</i>	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 129> Commands for Deleting the Policy-Map or a Specific Flow-Rule

Command	Description	Mode
No policy-map <i>PNAME</i>	Deletes the policy-map PNAME.	Config
No policy-map <i>PNAME</i> flow-rule <i>FNAME</i>	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 130> Commands for Enabling/Disabling Policy-Map

Command	Description	Mode
service-policy <i>IFNAME</i> {ingress egress} <i>PNAME</i>	Enables the policy-map PNAME in the specified direction of a specific port interface.	Config
no service-policy <i>IFNAME</i>	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 131> 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 vd1.
 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
Switch(config)# flow-rule f1 classify protocol tcp
Switch(config)# flow-rule f1 classify l4port 6000 any
Switch(config)# flow-rule f1 match drop
Switch(config)# flow-rule f2
Switch(config)# flow-rule f2 classify ipaddr 10.1.1.0/24 any
Switch(config)# flow-rule f2 match queuing 3
Switch(config)# flow-rule f3
Switch(config)# flow-rule f3 classify protocol tcp
Switch(config)# flow-rule f3 classify l4port 23 any
Switch(config)# flow-rule f3 match queuing 3
Switch(config)# flow-rule f3 match marking cos 3
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 vd1
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
Switch(config)# flow-rule f4 classify protocol tcp
Switch(config)# flow-rule f4 classify l4port 4010 any
Switch(config)# flow-rule f4 match rate-limit 10000
Switch(config)# flow-rule f5
Switch(config)# flow-rule f5 classify protocol tcp
Switch(config)# flow-rule f5 classify l4port 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 U3024B 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 132> 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

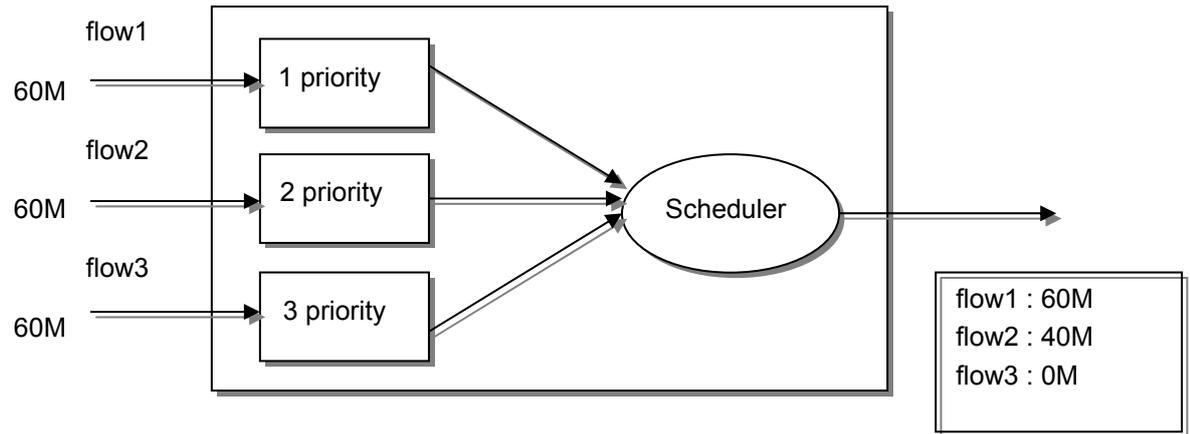
<Table 133> Commands for Viewing Qos Related Marking/Remarking Table

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

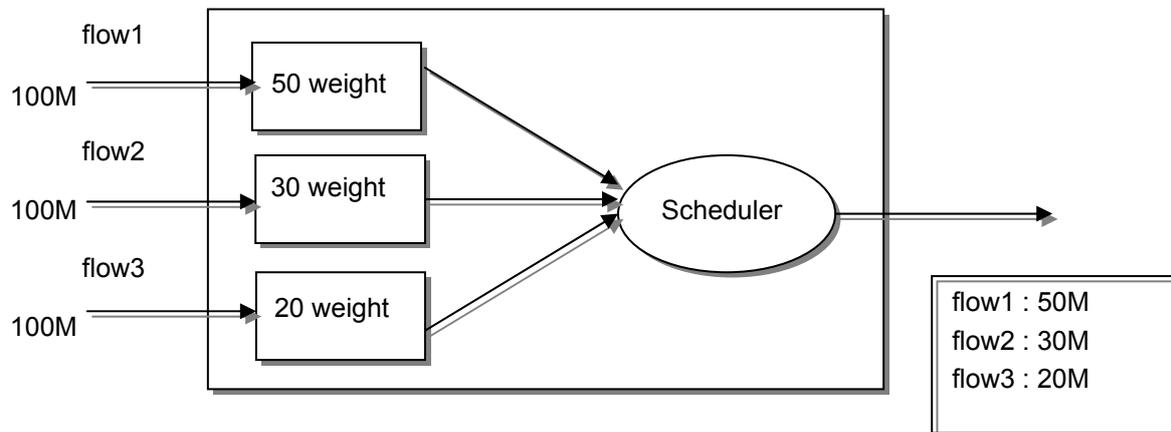
The U3024B provides SPQ (Strict Priority Queue), WRR (Weighted Round Robin) and WFQ(Weighted Fair Queuing) methods for scheduling. The default setting is SPQ.

The figure below illustrates differences between SPQ and WFQ.



<Figure 21> 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 22> 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 U3024B provides 8 queues for scheduling. The following commands are used to define queue-mode for a specific interface.

<Table 134> 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.



Notice Queuing-mode can be set for an individual FX / Giga port but TX ports can be defined by 8 ports only. The mode defined for the first one of the 8 ports equally applies to all of the 8 ports. For example, if a mode is set to vd1, vd1 ~ vd8 are to be set to the same mode.

The following commands are used to change weight in the queues in WRR / WFQ mode.

<Table 135> 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 136> 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 U3024B preferentially discards packets with a higher drop priority marked by the flow classifier or traffic conditioner. In the U3024B, 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 137> 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

Chapter 10. System File Management

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.

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 U3024B 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 138> Commands for File Management

Command	Description	Mode
show flash	<ul style="list-style-type: none">• Shows the status of flash files.	Privileged
erase <i>filename</i>	<ul style="list-style-type: none">• Deletes a configuration file stored in the flash memory.	Privileged

The following shows an example of running the show flash command. The U3024B 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 U3024B 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 139> 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
(skipped)
```

Download/Upload over TFTP

The table below describes the commands for downloading/uploading files over TFTP.

<Table 140> Commands for Downloading/Uploading over TFTP

Command	Description	Mode
copy tftp flash	<ul style="list-style-type: none"> Copies an OS image file from the TFTP server to the flash memory. 	Privileged
copy flash tftp	<ul style="list-style-type: none"> Copies an OS image file from the flash memory to the TFTP server. 	
copy tftp config-file	<ul style="list-style-type: none"> Copies a configuration file from the TFTP server to the flash memory. 	Privileged
copy tftp running-config	<ul style="list-style-type: none"> Applies a configuration file in the TFTP server as the current running-config. 	Privileged
copy running-config tftp	<ul style="list-style-type: none"> 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
(skipped)

```

Configuration File Management

Environment settings are a set of various parameters defined by the system operator while operating the U3024B switch. The configuration of U3024B 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 141> Commands for Configuration Management

Command	Description	Mode
show startup-config	• Shows the environment settings of the booting configuration 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
 ... <skipped > ....
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 U3024B 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 flash System1.cfg  
Warning: System1.cfg is booting config file  
Do you want to erase it [yes/no]? y  
Switch# reload
```

Boot Mode Setting and System Restarting

You can configure the OS image and configuration files required for operation of the U3024B 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 142> Commands for Setting Boot Mode and Restarting the System

Command	Description	Mode
boot flash <i>filename</i>	• Sets an OS image to be applied to rebooting.	Privileged
boot config <i>filename</i>	• 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 U3024B switch, care should be taken on the following points. The command 'boot flash' should be applied only to the OS image file applicable to the U3024B switch. In addition, the command 'boot config' should be applied to the configuration file applicable to the U3024B switch. 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 U3024B 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.CPU-FILTER & SYSCTL

This chapter describes how to set CPU-Filter and SYSCTL.

CPU Filtering

The Ubiquoss U3024B 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 143> Enabling/Disabling CPU-Filtering Rule

Command	Description
<code>cpu-filter rule NAME ip { srcIP srcIP/M any } { dstIP dstIP/M any } match { permit deny }</code>	CPU-filter for IP protocol Applies CPU-filter by source address and destination address Permits/denies packets using the match command
<code>cpu-filter rule NAME tcp { srcIP srcIP/M any } { dstIP dstIP/M any } { srcPort any } { dstPort any } match { permit deny }</code>	CPU-filter for TCP protocol CPU-filter by source/destination address and source/ destination port number Permits/denies packets using the match command
<code>cpu-filter rule NAME udp { srcIP srcIP/M any } { dstIP dstIP/M any } { srcPort any } { dstPort any } match { permit deny }</code>	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 144> Disabling the CPU-filter rule

Command	Description
<code>no cpu-filter rule NAME</code>	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 145> Adding/Deleting an INPUT Group

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

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

<Table 146> Disabling All Rule

Command	Description
cpu-filter group input delete <i>NAME</i>	<i>NAME</i> : 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 147> Add/Delete Forward Group

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

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 148> 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 2 group-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

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

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

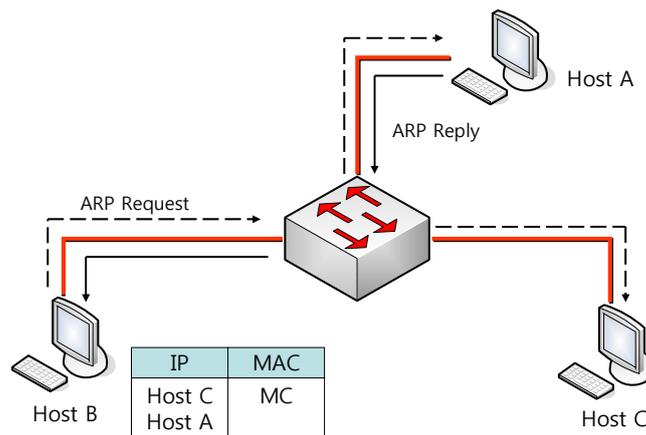
Understanding DAI

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.

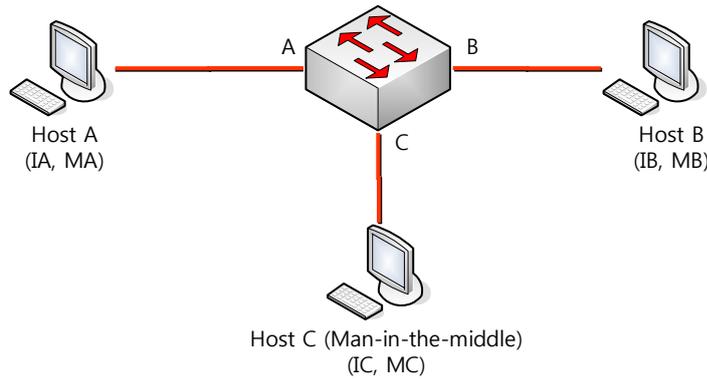


In order for host B to find out the MAC address for host A's IP address, host B sends out broadcast message (ARP request) to all the hosts in the broadcast domain. Then all the hosts in the broadcast domain shall receive the ARP request which was sent by host B and host A will reply to host B with its MAC address.

Understanding ARP Spoofing Attacks

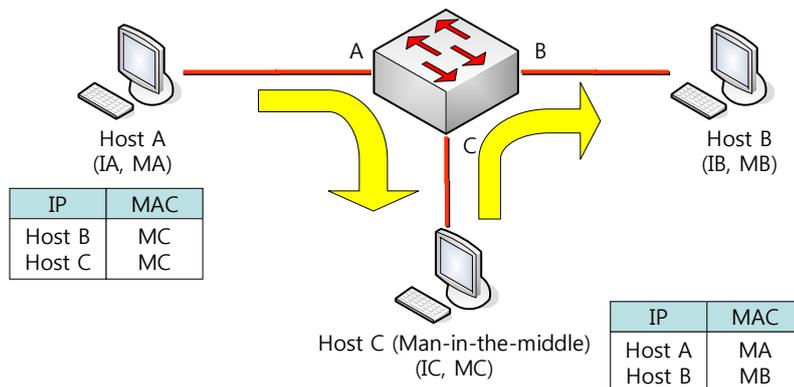
ARP unintentionally gets to have ARP table changed by the gratuitous reply which is sent by a host who has not received ARP request. Due to this defect, the ARP spoofing attack or ARP cache poisoning might happen. After this attack, the traffic of the victimized switch shall be transferred to other routers, 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.

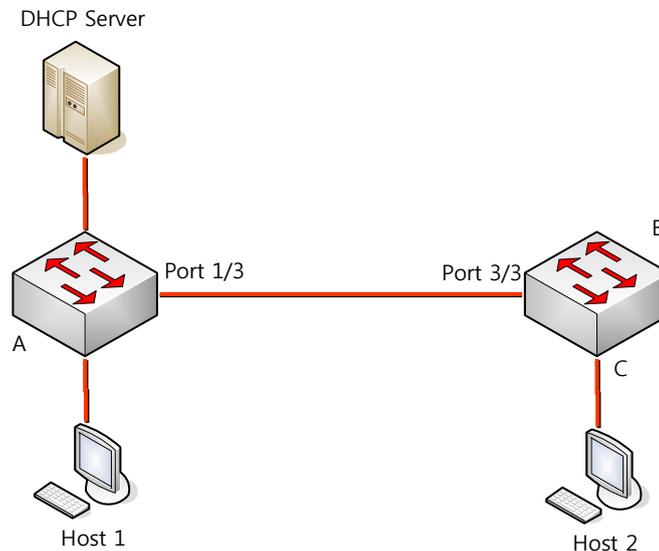
In a typical network formation, the switch ports which are connected to a host are to be configured as 'untrusted' and the switch ports to another switch are to be configured as 'trusted'. In this configuration, all the coming ARP packets into the switch will be inspected. And no more validity inspections 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 3000 series support 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 logging**' you can specify the type of packets to log.

Default DAI Configuration

The following table shows the default DAI configuration.

<Table 150> 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-disabled switch. As the man-in-the-middle attack is confined to a single Layer 2 broadcast domain, you ought to separate 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 151> Enabling DAI on VLANs

Command	Purpose
Switch# configure terminal	To get in global configuration mode.
Switch(config)# ip arp inspection vlan <i>vlan-id</i>	To enable DAI on a VLAN.
Switch(config)# no ip arp inspection vlan <i>vlan-id</i>	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 152> 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-vd1/1)# ip arp inspection trust	To configure the interface to be trusted. (default: untrusted)
Switch(config-if-vd1/1)# no ip arp inspection trust	To configure the interface to be untrusted.
Switch(config-if-vd1/1)# 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 153> Applying ARP ACLs for DAI Filtering

Command	Purpose
Switch# configure terminal	To get in global configuration mode.
Switch(config)# ip arp inspection filter <i>arp_acl_name</i> vlan <i>vlan-id</i> [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 154> 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-vd1/1)# ip arp inspection limit {rate pps [burst interval seconds] none}	(Optional) To set the rate limit upon ARP packet.
Switch(config-if-vd1/1)# no ip arp inspection limit	To get back to default configuration.
Switch(config-if-vd1/1)# ip arp inspection limit enable	To enable the ARP rate limit of an interface.
Switch(config-if-vd1/1)# no ip arp inspection limit enable	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 fa2/1
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
fa2/1	Untrusted	20	2	Disabled
fa2/2	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 155> 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- <i>vd1/1</i>)# ip arp inspection limit auto-recovery seconds	(Optional) To enable the automatic recovery function.
Switch(config)# no ip arp inspection limit auto-recovery	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 156> 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}	(Optional) To enable additive validity check. (default: none)
Switch(config)# no ip arp inspection validate {dst-mac ip src-mac}	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          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 157> 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 <i>number</i>	To set the size of DAI log buffer (range: 0 ~ 1024).
Switch(config)# no ip arp inspection log-buffer entries	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 158> 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 <i>number_of_messages</i> interval <i>length_in_seconds</i>	To configure the DAI log buffer.
Switch(config)# no ip arp inspection log-buffer logs	To return to default value.
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_messages*', 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 159> Configuring the DAI Log Filtering

Command	Purpose
Switch# configure terminal	To get in global configuration mode.
Switch(config)# ip arp inspection vlan <i>vlan-id</i> { 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 160> 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 [<i>vlan-id</i>]	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:

<Table 161> Initializing and Displaying the DAI Statistics

Command	Description
clear ip arp inspection statistics	To initialize DAI statistics.
show ip arp inspection statistics [<i>vlan</i> <i>vlan-id</i>]	To display the DAI statistics about ARP packets.

To display or initialize the DAI logging information, use the following commands:

<Table 162> Initializing and Displaying the DAI log buffer

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.

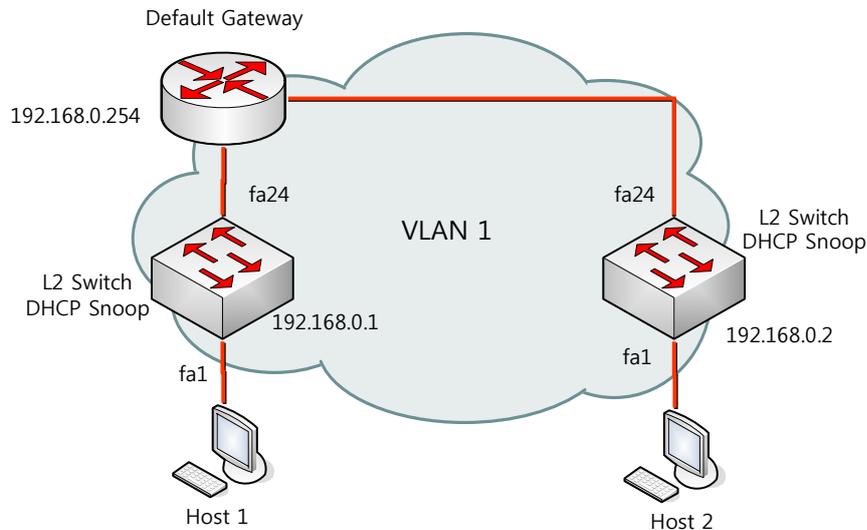
DAI Configuration Samples

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 163> Steps of Using DAL Function

Step	Description
Step 1	Activate DHCP snooping within VLAN 1 to build up the IP-to-MAC binding information of a host.

	<pre>Switch# configure terminal Switch(config)# ip dhcp snooping vlan 1 Switch(config)# ip dhcp snooping</pre>
Step 2	<p>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.</p> <pre>Switch# configure terminal Switch(config)# interface fa24 Switch(config-if-fa24)# ip arp inspection trust</pre>
Step 3	<p>Activate DAI upon VLAN 1.</p> <pre>Switch# configure terminal Switch(config)# ip arp inspection vlan 1 Switch(config)# end</pre> <p>To identify that the configuration has been set correctly.</p> <pre>Switch# show ip arp inspection vlan 1</pre>
Step 4	<p>Create flow rule and policy map to block ARP packets.</p> <pre>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</pre>
Step 5	<p>Apply the flow rule to the port that is connected to host.</p> <pre>Switch# configure terminal Switch(config)# service-policy vd1 ingress arp-trap Switch(config)# end</pre>

Chapter 13. ARP Snooping

This chapter is to explain how to configure ARP snoop function that is used to build Ethernet address information on specific IP address range.

**Note**

For detailed information on the grammar and usage of the commands used in this chapter, please refer to the commands reference.

This chapter consists of the following sections:

- Understanding ARP Snoop
- Default ARP Snoop Configuration
- Configuring ARP Snoop
- ARP Snoop Configuration Samples

Understanding ARP Snoop

This section is to explain about ARP snoop function.

Understanding ARP Snoop

Generally an ARP cache is generated in the following cases:

When a host transmits an ARP Request

When a host receives an ARP Request about the IP address the host has

The ARP cache, once generated, is continuously updated by ARP packets and deleted if it is not updated for specified time period.

The following table shows types of ARP packet that updates ARP cache:

<Table 164> Types of ARP that updates ARP cache

ARP op	Target address	Sender address	ARP cache
Request	To me	!= 0	Generates an ARP cache if there is no existing one
Reply	To me	!= 0	Updates the existing ARP cache
Request	Any	!= 0	Updates the existing ARP cache
Reply	Any	!= 0	Updates the existing ARP cache

If there is an ARP cache for the sender address of ARP packet, any ARP packet will change the ARP cache of the host.

The basic concept of the ARP snoop function is to provide information about the ARP sender to prevent the ARP cache from being updated by ARP packets not requested by the host. To achieve this purpose, the ARP snoop manages the (IP address, Ethernet address) information called ARP snoop binding.

If the host ARP snoop function activated receives an unsolicited ARP, it generates ARP snoop binding and sends an ARP Request to the host specified in the ARP packet. Later, if the sender information in the received ARP Reply is consistent with the information in ARP Request, this ARP snoop binding information is considered to be reliable.

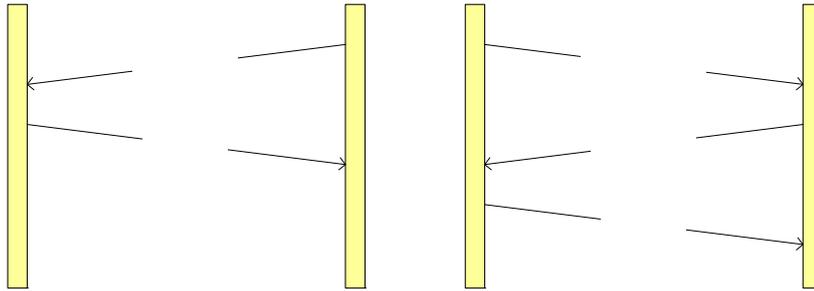


Figure 23 ARP snoop (3-way handshake)

Because the ARP packet does not have any security protection by itself, it can't determine which is valid when it receives several ARP Replies at the same time. So this method can't block ARP spoofing attacks completely. But if some reliable information can be generated before any attack starts, it can decrease the attacks' damage.



Caution To block ARP cache from being updated based on ARP snoop binding information, DAI and ARP ACL should be used together. ARP snoop provides ARP binding information only.

Update

ARP Snoop Entry States

ARP snoop keeps the status of ARP snoop binding information as follows:

<Table 165> ARP Snoop Entry States

State	Description
INIT	Initial state in which ARP snoop entry is generated
INCOMPLETE	The state after transmitting the ARP request in INIT state or UNSOLICITED state (probe)
REACHABLE	State verified through 3 Way handshake procedures
STALE	State in which age-time has passed in REACHABLE state
3WAY	State of waiting ARP reply after transmitting ARP request
UNSOLICITED	State in which no ARP reply has been received in 3WAY state

The reliable part of the ARP snoop is the ARP snoop binding in REACHABLE state.

ARP Snoop Ageing Time

ARP snoop considers that ARP snoop binding in REACHABLE state is valid only for ageing-time (default 80 seconds) period. The ARP snoop binding that has passed aging-time without any update by ARP Reply is deleted through STALE state.

To keep ARP snoop binding that has once turned to REACHABLE state, it's recommended not to use ageing-time.



Caution For the ARP snoop binding generated in error, it's recommended to use ageing-time since it can be kept.

ARP Snoop Binding Health Check

ARP snoop provides Health-check function, a function to determine the validity of the ARP snoop binding periodically. Even if the ARP snoop binding is in REACHABLE state, its value is not enough to be relied. The health-check function can be used usefully in the following cases:

- When the equipment does not exist in the network anymore
- When the host that has been attacking maliciously is disappeared

The purpose of Health-check is to check the validity of ARP snoop binding periodically and to keep it once it is turned out to be valid.

ARP Snoop Probe

The probe function of ARP snoop is similar to the health check function. The probe function of the ARP snoop is carried out only for the ARP snoop binding in INIT and UNSOLICITED state.

INIT state and UNSOLICITED state means the case when there is a host that has sent ARP Request, but no ARP Reply to the ARP Request that the ARP snoop received. The ARP snoop carries out probe operation periodically for the IP address that has been used more than once.

**Note**

If the probe is carried out for all the IP ranges, the number of packets of the ARP request may get increased. In order to decrease the number of ARP request packets that the ARP snoop sends, carry out the probe for the IP address which was in INIT state or UNSOLICITED state.

ARP snoop deletes unnecessary ARP snoop binding in INIT or UNSOLICITED state once per 60 seconds, so the probe hardly occurs repeatedly.

Understanding DAI and ARP Snoop

DAI is a security function to check ARP packet. DAI carry out logging of ARP packets with invalid IP-to-MAC address binding, and drop them. This function protects the network from main-in-the-middle attacks.

For the IP addresses without DHCP binding, DAI requires the following settings:

- Static ARP – The operator sets the IP address and its corresponding Ethernet address by himself
- ARP ACLs – Set the IP address and Ethernet address to allow or to drop based on ACL

The method of preventing ARP spoofing of the static IP address that does not use DHCP is to create 1:1 mapping for the IP address and Ethernet address using static ARP or ARP ACL. If 1:1 mapping is used for the IP address and Ethernet address, the protection of ARP spoofing may be perfect, but if the number of hosts that uses static IP addresses increases or if the equipments are replaced, the configuration should also be changed.

Though not recommended, in order not to change the settings for any addition or replace of equipments, the wildcard function of ARP ACL may be used in the following ways:

- Allow all the equipments for the IP address ranging from 192.168.0.10 to 192.168.0.20 – permit ip range 192.168.0.10 192.168.0.20 mac any
- Use specific vendor's equipments for specific IP address – permit ip range 192.168.0.10 192.168.0.20 mac 0007.7000.0000 0000.00ff.ffff



Caution If the ARP ACL is not used in 1:1 mapping, the ARP cache can't be protected from the ARP spoofing attack that uses the same ARP packet as in the permit configuration.

If there is an ARP snoop binding information with ARP snoop activated, DAI compares the ARP packet allowed by ARP ACL with the ARP snoop binding information once again.



Note Even if both ARP snoop and DAI are used together, it's still vulnerable to the ARP spoofing attack, since ARP snoop binding information is also not 100% reliable. The reliable solution to protect ARP spoofing attacks on static IP is to set 1:1 mapping between the IP address and the Ethernet address.

Relative Priority of ARP ACLs and ARP Snoop Entries

DAI uses ARP snoop binding even to check IP-to-MAC address mapping.

When both ARP ACL and ARP snoop are set, ARP snoop binding is used for checking earlier than ARP ACLs. The switch checks ARP packet with ARP snoop binding. ARP packets in discord with ARP snoop binding information will be discarded.

Even the ARP packets allowed by ARP snoop binding is discarded when not allowed by ARP ACLs. In other words, DAI uses ARP snoop binding only for checking the condition for discard.

Default ARP Snoop Configuration

The following table shows the default ARP snoop configuration.

<Table 166> Default ARP Snoop Configuration

Feature	Default Setting
ARP snoop	Disable.
ARP snoop ip	No IP address set.
Ageing Time	80 seconds
Health check	Enable.
Probe	Enable.
Probe interval	60 seconds
Wait time	2 seconds
Gratuitous ARP update	Updates ARP snoop binding without checking Gratuitous ARP.

Configuring ARP Snoop

This section is to explain how to configure ARP Snoop:

- Enabling ARP Snoop (Mandatory)
- Configuring ARP Snoop Ageing-time
- Disabling Gratuitous ARP update without validation (Optional)
- Disabling Health-check (Optional)
- Displaying ARP Snoop Information

Enabling ARP Snoop

If ARP snoop is enabled in the switch, the switch manages ARP snoop binding for the preset IP address range.

To enable ARP snoop in the switch, please use the following commands:

<Table 167> Enabling ARP Snoop

Command	Purpose
Switch# configure terminal	To enter into the global configuration mode.
Switch(config)# arp snoop ip <i>ip-address</i> [<i>ip-address</i>]	To set the IP address range.
Switch(config)# arp snoop	To enabled ARP snoop.
Switch(config)# no arp snoop	To disable ARP snoop.
Switch# show arp snoop	To check the settings.

The following example shows how to enable ARP snoop for the IP address range of 192.168.0.10 ~ 192.168.0.20:

```
Switch# configure terminal
Switch(config)# arp snoop ip 192.168.0.10 192.168.0.20
Switch(config)# arp snoop
```

The following example shows how to check the configuration:

```
Switch# show arp snoop

ARP Snoop           : Enabled
Gratuitous ARP update : Enabled
Health Check        : Disabled
Wait Time           : 2 sec
Probe Interval       : 60 sec
```

Configuring ARP Snoop Ageing-time

ARP snoop keeps the ARP snoop binding in REACHABLE state for ageing-time period. Default ageing-time is 80 seconds.

To change the ageing-time of the ARP snoop binding, please use the following commands:

<Table 168> Configuring ARP Snoop Ageing-time

Command	Purpose
Switch# configure terminal	To enter into the global setup mode.
Switch(config)# arp snoop ip <i>ip-address</i> [<i>ip-address</i>] [aging-time <i>aging-time</i>]	To set the range of IP address and change the ageing-time.
Switch(config)# arp snoop	To enable ARP snoop.
Switch(config)# no arp snoop	To disable ARP snoop.
Switch# show arp snoop	To check the settings.

The following example shows how to enable ARP snoop for the IP address range of 192.168.0.10 ~ 192.168.0.20 and to set ageing-time to 300 seconds:

```
Switch# configure terminal
Switch(config)# arp snoop ip 192.168.0.10 192.168.0.20 ageing-time 300
Switch(config)# arp snoop
```



Caution If the value of Ageing-timer is set to 0, the state check and change for the ARP snoop binding in REACHABLE state does not occur. In other words, it continues to use wrong-mapped ARP snoop binding. If not a correctly-mapped ARP snoop binding, do not set the ageing-time to 0.

Disabling Gratuitous ARP Update without Validation

By Default, the ARP snoop does not transmit the ARP request but just update ARP snoop binding when it receives a gratuitous ARP.

To allow the ARP snoop to update ARP snoop binding after sending the ARP request even for the gratuitous ARP packet, please use the following commands.

<Table 169> Disabling Gratuitous ARP Update without Validation

Command	Purpose
Switch# configure terminal	To enter into global configuration mode.
Switch(config)# arp snoop ip <i>ip-address</i> [<i>ip-address</i>]	To set the range of IP address.
Switch(config)# arp snoop	To enable ARP snoop.
Switch(config)# no arp snoop	To disable ARP snoop.
Switch(config)# no arp snoop gratuitous-arp-update	Not to update the ARP snoop binding immediately when it receives a Gratuitous ARP.
Switch# show ip arp inspection	To check the configuration.

The following example shows how to enable ARP snoop for the IP address range of 192.168.0.10 ~ 192.168.0.20 and to set to send ARP request even for gratuitous ARPs:

```
Switch# configure terminal
Switch(config)# arp snoop ip 192.168.0.10 192.168.0.20
Switch(config)# arp snoop
Switch(config)# no arp snoop gratuitous-arp-update
Switch(config)# end
```

Disabling Health-check

ARP snoop sends ARP Request for ARP snoop binding in REACHABLE state periodically, and updates the state of ARP snoop binding by the received ARP Replies.

In order not to use health-check function of ARP snoop, use the following commands.

<Table 170> Disabling Health-check

Command	Purpose
Switch# configure terminal	To enter into the global setup mode.
Switch(config)# arp snoop ip <i>ip-address</i> [<i>ip-address</i>]	To set IP address range.
Switch(config)# arp snoop	To enable ARP snoop.
Switch(config)# no arp snoop	To disable ARP snoop.
Switch(config)# no arp snoop health-check	To disable Health-check function.
Switch# show ip arp inspection	To check the settings.

The following example shows how to enable ARP snoop for the IP address range of 192.168.0.10 ~ 192.168.0.20 without using health-check function:

```
Switch# configure terminal
Switch(config)# arp snoop ip 192.168.0.10 192.168.0.20
Switch(config)# arp snoop
Switch(config)# no arp snoop health-check
Switch(config)# end
```

Displaying ARP Snoop Information

To view the information of ARP snoop, please use the following commands:

<Table 171> Displaying ARP Snoop Information

Command	Description
show arp snoop	To view the setup information of ARP snoop.
show arp snoop binding	To view ARP snoop binding information.
show arp snoop interface	To view transmission rate of ARP packet that the ARP snoop sends.

To check or initialize the statistical information of ARP snoop, use the following commands:

Command	Description
clear arp snoop statistics	Initialize the statistical information of ARP snoop.
show arp snoop statistics	Print the statistical information on ARP packet that the ARP snoop sent or received.

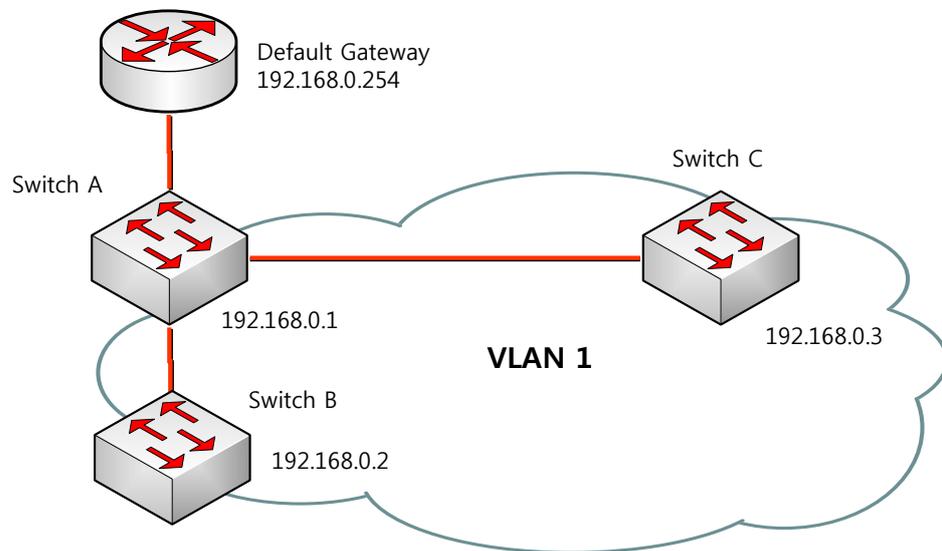
ARP Snoop Configuration Samples

This section includes the following samples:

- Sample One: ARP spoofing detection
- Sample Two: Interoperate with DAI on DHCP Relay

Sample One: ARP spoofing detection

This sample is to explain how to detect ARP spoofing for specific IP address range using ARP snoop function. Let's consider that the network is configured as seen in the following figure:



To activate ARP snoop function to obtain IP-to-MAC binding information for the IP address range used by other Default gateway or other switches in the switch A, please set as follows:

<Table 172> ARP Snoop Configuration

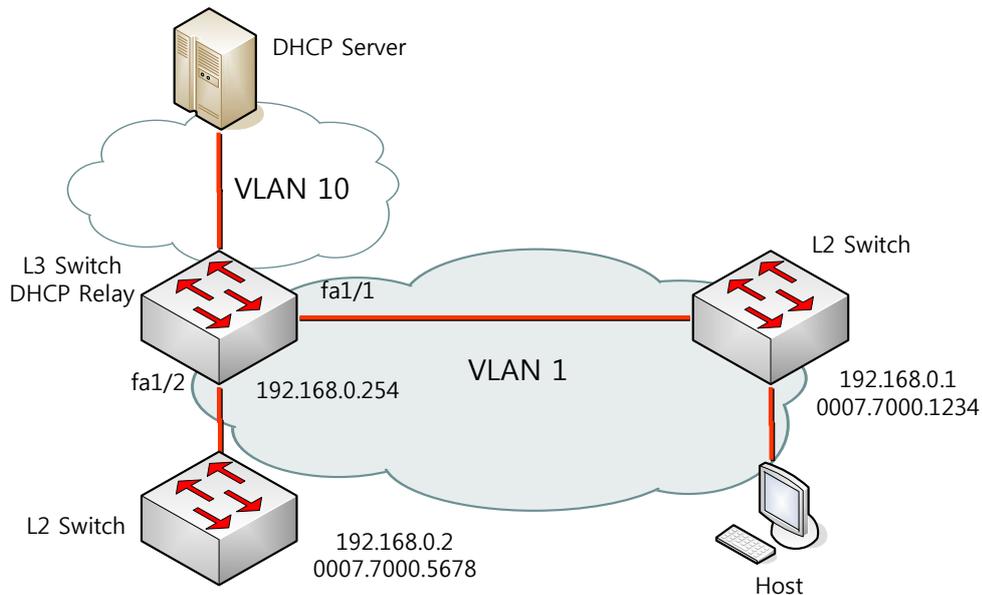
	<p>Activate the ARP snoop to create IP-to-MAC binding information for specific IP address range,.</p>
Step 1	<pre>Switch# configure terminal Switch(config)# arp snoop 192.168.0.1 192.168.0.10 Switch(config)# arp snoop 192.168.0.254 Switch(config)# arp snoop</pre> <p>Check if the settings are correct. Switch# show arp snoop</p>



Note Because the ARP snoop creates IP-to-MAC binding information only, it's impossible to protect the ARP table. It's possible to detect ARP spoofing by comparing the results of "show arp snoop binding" command and "show arp" command.

Sample Two: Interoperate with DAI on DHCP Relay

This example is to explain how to block ARP packet using IP-to-MAC binding information of ARP snoop in DHCP relay that uses DAI function. Consider that the network is configured as seen in the following picture:



L3 switch relays DHCP message to the DHCP server through VLAN 10, and is connected to host or L2 switch. The L2 switch connected to the L3 switch uses a static IP address. The hosts are assigned IP addresses through DHCP. And all the switches and hosts are located in the VLAN 1.



Note In the above configuration, DAI relies fully on DHCP snooping binding information for IP-to-MAC binding information. For DHCP snooping configuration, please refer to the DHCP snooping manual.

To use DAI function in the switch used as a DHCP relay, please set as below:

<Table 173> DAI on DHCP Relay

	Activate the DHCP relay function.
Step 1	Switch# configure terminal Switch(config)# ip dhcp helper-address 10.1.1.1 Switch(config)# service dhcp relay

<p>Step 2</p>	<p>Activate DHCP snooping on the interface VLAN 10 used for communication with the DHCP server and the interface VLAN 1 to which the host is connected, to create IP-to-MAC binding information of hosts in which IP address is assigned by DHCP.</p> <pre>Switch# configure terminal Switch(config)# ip dhcp snooping vlan 1 Switch(config)# ip dhcp snooping vlan 10 Switch(config)# ip dhcp snooping</pre>
<p>Step 3</p>	<p>Activate ARP snoop to create IP-to-MAC binding information for IP address ranges that use Static IP.</p> <pre>Switch# configure terminal Switch(config)# arp snoop ip 192.168.0.1 192.168.0.10 Switch(config)# arp snoop</pre>
<p>Step 4</p>	<p>Set ARP ACL to allow ARP packets of switches that use static IP.</p> <pre>Switch# configure terminal Switch(config)# arp access-list permit-switch Switch(config-arp-nacl)# permit ip range 192.168.0.1 192.168.0.10 mac any Switch(config-arp-nacl)# exit Switch(config)# ip arp inspection filter permit-switch vlan 1 Switch(config)# end</pre> <p>Check if the settings are correct. Switch# show ip arp inspection vlan 1</p>
<p>Step 5</p>	<p>Activate DAI in the VLAN 1 to which the host is connected.</p> <pre>Switch# configure terminal Switch(config)# ip arp inspection vlan 1 Switch(config)# end</pre> <p>Check if the settings are correct. Switch# show ip arp inspection vlan 1</p>

The result of L3 switch settings are as follows.

```
!
arp snoop ip 192.168.0.1 192.168.0.10
arp snoop
!
arp access-list permit-switch
```

```
    permit ip range 192.168.0.1 192.168.0.10 mac any
!
ip arp inspection vlan 1
ip arp inspection filter permit-switch vlan 1
!
ip dhcp helper-address 10.1.1.1
service dhcp relay
!
ip dhcp snooping vlan 1
ip dhcp snooping vlan 10
ip dhcp snooping
!
```

Chapter 14. VDSL Configuration

In this chapter is the explanation upon how to set-up the VDSL2 configuration for U3000 switch. The main content includes as below:

- Overview of Profile
- Setting up the Line Profile
- CPE firmware upgrade
- Displaying VDSL Status

**Note**

The detail usage of the CLI commands which are shown in this chapter can be found in command reference.

Overview of Profile

The upstream and downstream of the VDSL link can be controlled by setting up the profile with regard to U3024Bes. According to the profile, VDSL link can be set to any value of bandwidth between 64Kbps and 100 Mbps in terms of uplink and downlink.

U3024B is having predefined profile (DEFVAL profile) and able to redefine a new profile. A profile can be configured with respect to individual port. Typically every VDSL ports in U3024B are under the effect of DEFVAL profile.

**Note**

The configuration of DEFVAL profile may be different according to the released version of Operating System. User is encouraged to setup his own profile referring to the DEFVAL profile.

Setting up Line Profile

This section tells how to setup a profile and apply it to VDSL ports.

Default configuration

- Toward every VDSL ports in U3024B, DEFVAL profile is basically assigned.

Assigning a Profile to a Specific VDSL Port

A port can be assigned any profile individually. Thus any one VDSL port can have either same or different profile comparing with others.

In order to assign a profile to any one port, the following commands are to be executed sequentially in privileged EXEC mode:

<Table 174> Assigning a Profile to a Specific VDSL Port

	Command	Effect
Step 1	configure terminal	To enter the global configuration mode.
Step 2	interface <i>interface-id</i>	To specify the interface and enter the interface configuration mode.
Step 3	service-line-profile <i>profile-name</i>	To specify the profile name.

To delete the assigned profile and consequently utilize the default profile, the interface configuration command, '**no service-line-profile**' is required to be used.

Configuring a New Line Profile

A new Line profile can be created. The new Line profile inherits the value of DEFVAL profile.

In order to create a profile, the following commands are to be executed sequentially in privileged EXEC mode:

<Table 175> Configuring a New Line Profile

	Command	Effect
Step 1	configure terminal	To enter the global configuration mode.
Step 2	line-profile <i>profile-name</i>	To specify the profile name and enter into profile configuration mode.
Step 3	end	To return to privileged EXEC mode.

The newly created profile has the similar configuration as the DEFVAL profile. By using the command of profile configuration, the configuration can be modified.

To delete the profile, the global configuration command, '**no line-profile** *profile-name*' is required to be used.

Reset VDSL Port with Updated Profile

When the content of a profile is changed, corresponding VDSL port(s) should be reset so that the modified profile can be reassigned to them again. U3024B has the function of resetting all the ports at once.

In order to apply the modified profile to VDSL ports, the following commands are to be executed sequentially in privileged EXEC mode:

<Table 176> Reset VDSL Port with Updated Profile

	Command	Effect
Step 1	configure terminal	To enter into global configuration mode.
Step 2	line-profile <i>profile-name</i>	To specify profile name and enter into profile configuration mode.
Step 3	apply associated-ports	To reset all the related VDSL ports which are using the profile.
Step 4	end	To return to privileged EXEC mode.

Setting up Line profile

<Table 177> Setting up Line profile

Command	Mode	Function
band-modifier	Line-profile	Band Modifier
downstream		Downstream
g-handshake		G.HS (Handshake)
ife-rx-filter		IFE RX filter
ife-tx-filter		IFE TX filter
line-type		VDSL line type
option-band-plan		Option Band Plan
pbo-config		PBO(Power Back Off) config
power-mode		Power Mode
rate-adaptation-mode		Rate adaptation mode
tcm		Determine whether to apply TCM (Trellis Code Modulation)
upstream		Upstream
downstream		Downstream

Setting up pbo-config

The distance between VDSL port and CPE are variant. Therefore if the feeding power is equally applied to ports regardless of the individual distance, it would induce some problem of interference. U3000 series has the feature of controlling the power level.

<Table 178> Setting up pbo-config

Command	Mode	Function
pbo-config enable	line-profile	Enable PBO function.
pbo-config disable		Disable PBO function.
pbo-config length {0,...,900}		Set the distance unit by 100m.

pbo-config k1[1] k1[2] k1[3] k1[4] k1[5] k1[6]		Adjust the value for PBO function in order to fit the system environment. However we recommend to use the default values.
pbo-config k2[1] k2[2] k2[3] k2[4] k2[5] k2[6]		

Setting up Optional band

U3000 series utilize 6band in case of short distance, and 3band in case of longer distance. In case of long distance, typically the bandwidth of upstream is narrower than that of downstream, however U3000 series can extend the upstream bandwidth to make sure reliable transmission. This augmented band is called Option band. To setup Option band, the following commands are to be used.

<Table 179> Setting up Optional band

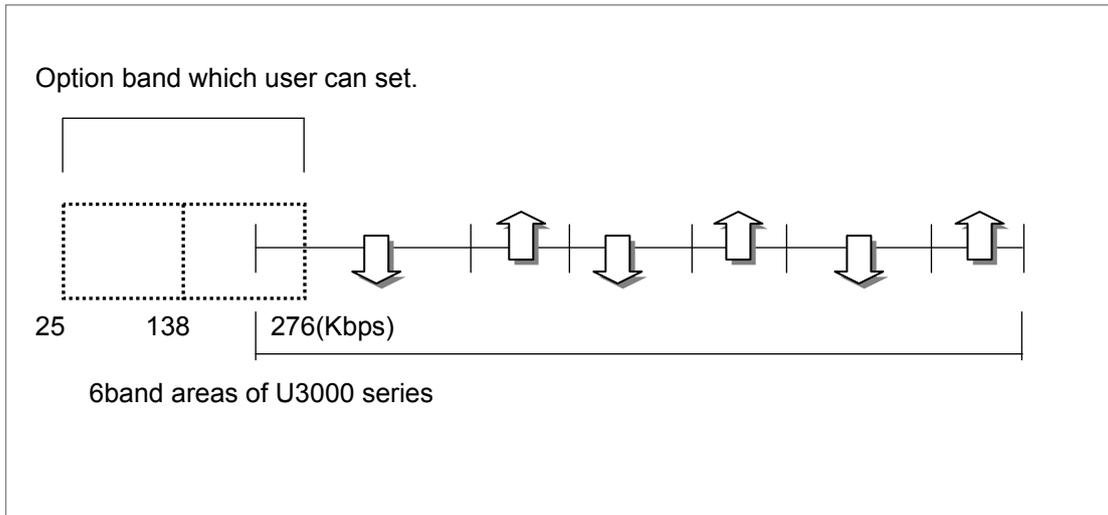
Command	Mode	Function
optional-band-plan annex-a-25-138	line-profile	Use the band of 25~138Kbps as an optional band.
optional-band-plan annex-b-138-276		Use the band of 138~276Kbps as an optional band.
optional-band-plan annex-m-25-276		Use the band of 25~276Kbps as an optional band, which is combined one of the two bands above.
exclude		Specify that there is No optional band used.



Note

Default setting is 'exclude'.

The explanation upon Option band is depicted below;



【 Option band and 6band 】

Setting up band-modifier

To hide from the interference of existing ADSL or ISDN, U3000 can filter out of some frequency range by this feature.

<Table 180> Setting up band-modifier

Command	Mode	Function
band-modifier rx disable-640k-below	line-profile	Disable ISDN band.
band-modifier rx disable-1.1m-below		Disable ISDN and ADSL band.
band-modifier rx disable-2.2m-below		Disable the band which is below than 2.2MHz.
band-modifier rx all-tones-on		Enable to use the band of ISDN and ADSL range.
band-modifier tx disable-640k-below		Disable ISDN band.
band-modifier tx disable-1.1m-below		Disable ISDN and ADSL band.
band-modifier tx disable-2.2m-below		Disable the band which is below than 2.2MHz.
band-modifier tx all-tones-on		Enable to use the band of ISDN and ADSL range.



Note

The default value is all-tone-on.

Setting up G.HS

VDSL equipment and user side CPE can set the optimized values by communicating each other based upon the distance, noise level, and band plan. This sequence is defined as G.HS. U3000 series support the method of A43, B43, I43 and V43 G.HS procedure.

<Table 181> Setting up G.HS

Command	Mode	Function
g-handshake a43 {on off}	line-profile	On or off of the Ikanos a43
g-handshake b43 {on off}		On or off of the Ikanos b43
g-handshake v43 {on off}		On or off of V43 specified in G.992 and G.993
g-handshake i43 {on off}		On or off of the Ikanos I43



Note Default is V43, B43.

Setting up ife-tx-filter and ife-rx-filter

While using 5band or 6band, no external filter is required. But in case of using 100/100 band plan or VLR, external filter is required. To set up the Extern filter, the following commands are to be used.

<Table 182> Setting up ife-tx-filter and ife-rx-filter

Command	Mode	Function
ife-tx-filter internal	line-profile	Set not to use external filter.
ife-tx-filter k1_external		Use K1 filter.
ife-tx-filter u1_external		Use U1 filter.
ife-tx-filter h1_external		Use H1 filter
ife-tx-filter ttc_external		Use TTC filter



Note Default is internal for both of tx, rx.

Setting up line type

U3000 series support various profiles according to geographic characterist, distance, and bandwidth. To set the Line-type, the following commands are to be used.

<Table 183> Setting up line type

Command	Mode	Function
<code>line-type auto-detect all-xdsl</code>	line-profile	Apply all the profiles of ADSL 1/2/2+ and VDSL 1/2 .
<code>line-type auto-detect vdsl2-itu</code>		Apply the profiles of 8A/8B/8C/8D/12A/12B/17A.
<code>line-type auto-detect vdsl2-all</code>		Apply the profiles of 8A/8B/8C/8D/12A/12B/17A and 30A

<Table 184> Setting up line type manually

Command	Mode	Function
<code>line-type manual-set adsl-annex-a {on off}</code>	line-profile	Set up the ADSL DMT Annex A
<code>line-type manual-set adsl-annex-b {on off}</code>		Set up the ADSL DMT Annex B
<code>line-type manual-set adsl-annex-c {on off}</code>		Set up the ADSL DMT Annex C
<code>line-type manual-set adsl2-annex-a {on off}</code>		Set up the ADSL2 DMT Annex A
<code>line-type manual-set adsl2-annex-b {on off}</code>		Set up the ADSL2 DMT Annex B
<code>line-type manual-set adsl2+-annex-a {on off}</code>		Set up the ADSL2+ DMT Annex A
<code>line-type manual-set adsl2+-annex-b {on off}</code>		Set up the ADSL2+ DMT Annex B
<code>line-type manual-set adsl2+-annex-m {on off}</code>		Set up the ADSL2+ DMT Annex M
<code>line-type manual-set adsl2+-annex-l {on off}</code>		Set up the ADSL2+ DMT Annex L
<code>line-type manual-set vdsl-ansi {on off}</code>		Set up the VDSL ANSI
<code>line-type manual-set vdsl-etsi {on off}</code>		Set up the VDSL ETSI
<code>line-type manual-set vdsl-itu-993-1 {on off}</code>		Set up the VDSL ITU 993 1
<code>line-type manual-set vdsl-ieee-802-ah {on off}</code>		Set up the VDSL IEEE 802 AH
<code>line-type manual-set vdsl2-itu-g993-2-8a {on off}</code>		Set up the VDSL2 ITU G993 2 8A
<code>line-type manual-set vdsl2-itu-g993-2-8b {on off}</code>		Set up the VDSL2 ITU G993 2 8B
<code>line-type manual-set vdsl2-itu-g993-2-8c {on off}</code>		Set up the VDSL2 ITU G993 2 8C
<code>line-type manual-set vdsl2-itu-g993-2-8d {on off}</code>		Set up the VDSL2 ITU G993 2 8D
<code>line-type manual-set vdsl2-itu-g993-2-12a {on off}</code>		Set up the VDSL2 ITU G993 2 12A
<code>line-type manual-set vdsl2-itu-g993-2-12b {on off}</code>		Set up the VDSL2 ITU G993 2 12B
<code>line-type manual-set vdsl2-itu-g993-2-17a {on off}</code>		Set up the VDSL2 ITU G993 2 17A
<code>line-type manual-set vdsl2-itu-g993-2-30a {on off}</code>	Set up the VDSL2 ITU G993 2 30A	



Note

U3000 series has auto switching function. For example, while being et as 8A, 12A, 30A and if the distance is 3Km, 8A is automatically applied. However if the distance would be shorten to 100m, then the profile in use is automatically converted to 30A.

Setting up power-mode

U3000 series can set the power level as below.

<Table 185> Setting up power-mode

Command	Mode	Function
power-mode 0	line-profile	Set the power level to 8.5 dBm
power-mode 1		Set the power level to 11.5 dBm
power-mode 2		Set the power level to 14.5 dBm
power-mode 3		Set the power level to 17.5 dBm
power-mode 4		Set the power level to 20.5 dBm



Note Default is (4) 20.5 dBm

Setting up rate-adaptation-mode

U3000 series system can set the speed either automatic adjustment or fixed rate based upon the distance and line condition. If the system is set to fixed mode, it will train at the maximum data rate. In this case, even though Synchronization would fail, the system will continue to train in the fixed rate mode. Consequently it might not be possible to stay in communication. Contrarily in startup mode, it will try to get synchronized at the value between Max rate and min rate according to distance and line condition. To set rate-adaptation-mode the following commands are to be used.

<Table 186> Setting up rate-adaptation-mode

Command	Mode	Function
rate-adaptation-mode fixed	line-profile	Set to Fixed mode.
rate-adaptation-mode startup		Set to Startup mode



Note Default is startup mode.

Setting up upstream / downstream

U3000 series can adjust the value of rate limit and snr margin with respect to upstream and downstream individually.

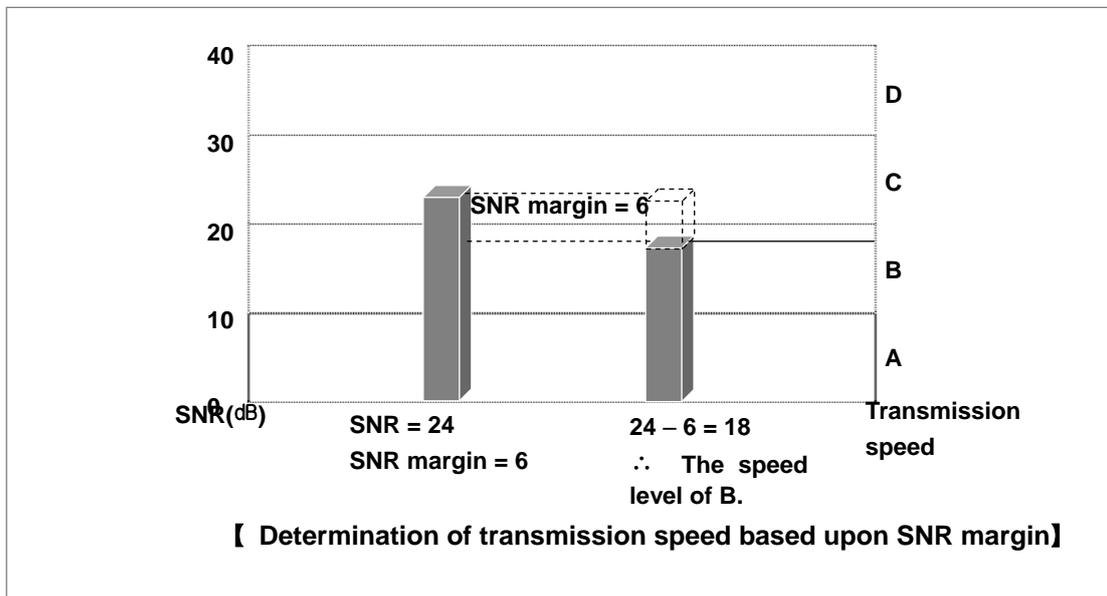
Setting up max-margin, min-noise-margin, target-noise-margin

In the communication system, SNR(Signal to Noise Ratio) represents the ratio of signal to noise. Its calculation formula is 「 $SNR(dB) = 20 \log_{10}(Vs/Vn)$ 」 where Vs represents signal strength and Vn represents noise strength. If signal strength is weaker than noise strength, no reliable communication is guaranteed. Thus in order to keep the communication lines reliable, SNR shouldn't be negative or "0" If it would be the case, the signal level should be increased or noise level should be decreased.

The line speed of VDSL depends on SNR. However the line environment cannot be kept in constant stability. Thus line speed ought to be determined considering the possibility of changing line environment. By predetermining the SNR value based upon SNR, there would be no problem even when noise level would be suddenly increased.

U3000 series can set the SNR range based upon forecast, and determine the transmission speed by subtracting the width of SNR range from current SNR value. The width of SNR range is called 「**SNR margin**」

In other words, when the SNR margin is set to "6" then the determined transmission speed will be the value of "current SNR minus SNR margin" as depicted below.



When noise variation is expected to be severe then SNR margin would better be set large. However if SNR value is set large, it will have the handicap of slowed speed while guaranteeing reliable communication.

To set snr margin the following commands are to be used.

<Table 187> Setting up max-margin, min-noise-margin, target-noise-margin

Command	Mode	Function
upstream max-margin	line-	To set maximum value of snr margin

upstream min-noise-margin	profile	To set minimum value of snr margin.
upstream target-noise-margin		To set target value of snr margin.
downstream max-margin		To set maximum value of snr margin
downstream min-noise-margin		To set minimum value of snr margin.
downstream target-noise-margin		To set target value of snr margin.



Note

Default values are as follows: max-margin is 31 dB, min-noise-margin is 5dB, and target-noise-margin is 6dB.

Setting up VDSL port transmission speed

VDSL port transmission speed can be adjusted like Ethernet port can be done so. This function gives VDSL user differentiated service.

Line Rate is the speed between VDSL system and modem while Payload Rate is actual data rate which has been set. The preset Line Rate is adjusted according to noise margin and line type. Each Rate will have minimum and maximum values and if the Payload Rate of the line is not inbetween these values, the line will automatically be released. To set the bandwidth of the port, the following commands are to be used.

<Table 188> Setting up VDSL port transmission speed

Command	Mode	Function
upstream slow-max-rate <0-200000>	line-profile	To set the maximum value of upstream speed by unit of 64Kbps.
upstream slow-min-rate <0-200000>		To set the minimum value of upstream speed by unit of 64Kbps.
downstream slow-max-rate <0-200000>		To set the maximum value of downstream speed by unit of 64Kbps.
downstream slow-min-rate <0-200000>		To set the minimum value of downstream speed by unit of 64Kbps.



Note

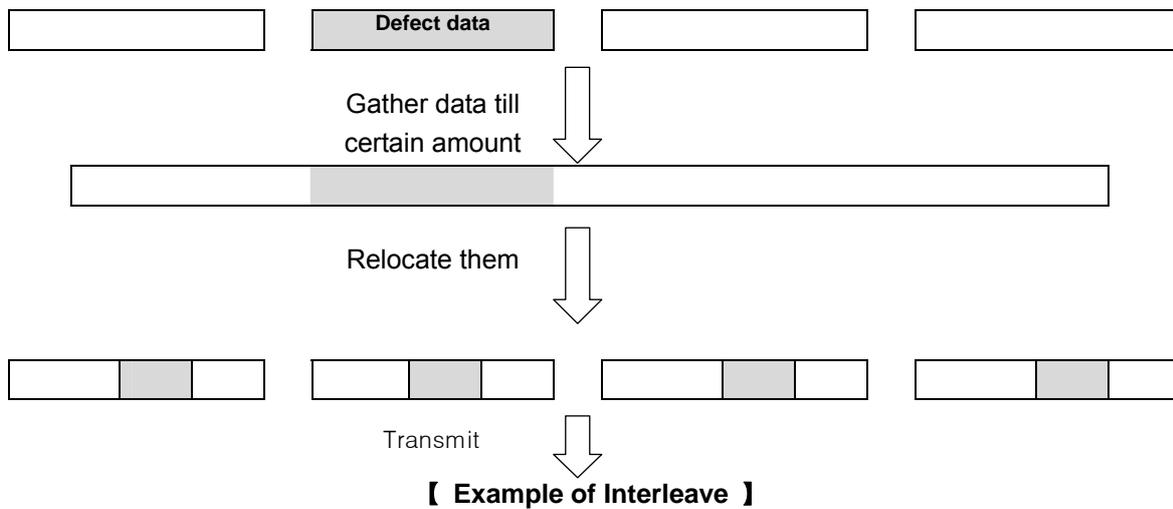
Default values is 125Mbps for up and down links individually

Setting up Interleave

Before the digital data is modulated into analog signal, in order to recover the signal from error there is a procedure of Interleave.

In the procedure of Interleave, when a certain size of data block is gathered, the U3000 system relocates the data, and divide thme into predetermined size of data blocks and transmit.

As you see in the figure below, the data block which has errors is relocated by Interleave so as to scatter the errors throughout the whole data blocks. By distributing the errors the recovery process can be executed more effectively.



By way of Interleave procedure, error can be adjusted more effectively, however there is a disadvantage for the system to wait until the data will be collected to be a certain size for transmission. Contrarily if the Interleave procedure is omitted, the data transmission speed will be faster but the effectiveness of error recovery is worsen.

U3000 which has chosen DMT modulation is using only slow channel mode.

The system can set the time interval between data transmissions when the system is in the operation of Interleave procedure. This time interval is called Interleave-delay. When Interleave-delay is selected and set, the further delay of data transmission can be prevented. To change the value of Interleave delay, the following commands are to be used.

<Table 189> Setting up Interleave

Command	Mode	Function
upstream slow-max-interdelay <0-200>	line-profile	To set the value of interleave delay for uplink in the unit of 0.5 ms
downstream slow-max-interdelay		To set the value of interleave delay for downlink in the unit of 0.5 ms



Note

Default values of interleaved delay for both links are set to 1.0ms

Setting up min-ohm-rate

OHM(Over Head Message) is a way to get relevant information for the purpose of maintenance from the CPE which resides in customer's site. OHM utilizes subscriber data rather than its own dedicated one. Thus it might affect the usage of subscriber channel. In order to minimize the negative influence on the data channel, there needs to be a way to set the range of the OHM bandwidth. Min-ohm-rate is the command for this need. To set Min-ohm-rate the following commands are to be used.

<Table 190> Setting up min-ohm-rate

Command	Mode	Function
upstream min-ohm-rate <1-256>	line-profile	Adjust the upstream bandwidth for OHM by unit of Kbps.
downstream min-ohm-rate <1-256>		Adjust the downstream bandwidth for OHM by unit of Kbps.



Note Default value of min-ohm-rate is 5Kbps each for uplink and downlink.

Setting up Alarm profile

Alarm profile is used when making out a policy upon alarm and applying the policy to service ports. By way of alarm profile, the system is able to inform user of the system fault through SNMP Trap. This feature enables users to set the checkup standard for faults which is variant according to service characteristics.

Alarm profile consists of the Threshold values of individual errors which would be set by users. Every 15 minutes the system checks up each error items, and if any one item would be over the adjusted threshold, it would issue SNMP Trap.

The followings are the method to make and set Alarm profile. In order to get in the mode for setting Alarm profile, in Global setup mode, type in the following commands.

<Table 191> Setting up Alarm profile

Command	Mode	Function
alarm-profile <i>profile-name</i>	Global	Get in the mode for setting Alarm profile

<Table 192> Adjusting the Threshold Value

Command	Mode	Function
thresh-15min-crc <0-900>	Alarm-profile	Adjust the threshold value for CRC error duration by unit of second.
thresh-15min-ess <0-900>		Adjust the threshold value for ESs error duration by unit of second.
thresh-15min-fecs <0-900>		Adjust the threshold value for RECs error duration by unit of second.
thresh-15min-lofs <0-900>		Adjust the threshold value for LOFS error duration by unit of second.

thresh-15min-lols <0-900>		Adjust the threshold value for LOLS error duration by unit of second.
thresh-15min-loss <0-900>		Adjust the threshold value for LOSS error duration by unit of second.
thresh-15min-lprs <0-900>		Adjust the threshold value for LPRs error duration by unit of second.
thresh-15min-sess <0-900>		Adjust the threshold value for SES error duration by unit of second.
thresh-15min-uass <0-900>		Adjust the threshold value for UAS error duration by unit of second.
Command	Mode	Function
set alarm-profile <i>profile-name</i> add <i>port-number</i>	Interface	Apply the content of Profile to the specified port.

Setting up System profile

Meanwhile Line profile is applied to individual port, system profile is applied to the whole system. Thus the items specified in System-profile shall be applied to every ports in the system.

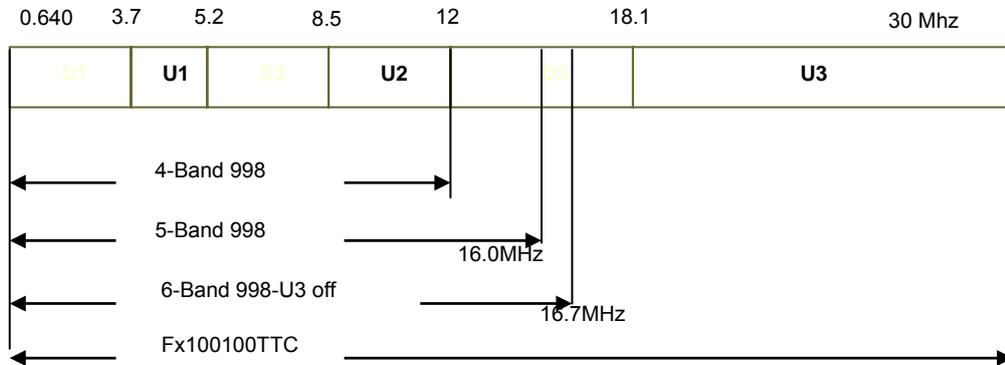
The followings are the commands to set the Profile.

<Table 193> Setting up System profile

Command	Mode	Function
adsl-safe-mode	System-profile	ADSL safe mode
band-plan		Band Plan
bit-swap		Bit Swap
ham-band		HAM Band
psd-mask-level		PSD Mark Level
rfi-band		RFI Band
tlan-safe-mode		Decide whether to apply TLAN safe mode or not.

Setting up band-plan

U3000 series can support various Band without changing hardware so that they can provide different speed according to the service condition of operators.



The followings are the commands to set band plan.

<Table 194> Setting up band-plan

Command	Mode	Function
band-plan 0	system-profile	Band Plan 998 3 (BP1_998_3)
band-plan 1		Band Plan 998 3 (BP2_998_3 or BP998_3B_8_5M)
band-plan 2		Band Plan 998 4 (BP3_998_4 or BP998_4B_12M)
band-plan 3		Band Plan 997 3 (BP4_997_3 or BP997_3B_7_1M)
band-plan 4		Band Plan 997 3 (BP5_997_3)
band-plan 5		Band Plan 997 4 (BP6_997_4 or BP997_4B_7_1M)
band-plan 6		Band Plan Flex (BP7_MXU_3 or FLEX_3B_8_5M)
band-plan 7		Band Plan Flex (BP8_MXU_2)
band-plan 8		Band Plan 998 6 (BP998_6B_30A)
band-plan 9		Band Plan 998 2 (BP10_998_2 or BP998_2B_3_8M)
band-plan 10		Band Plan 998 2 (BP11_998_2)
band-plan 11		Band Plan 998 3 (BP998_3B_17000_4K)
band-plan 12		Band Plan Flex (BP13_MXU_3)
band-plan 13		Band Plan Flex (BP14_MXU_3)
band-plan 14		Band Plan 998 (BP15_998_138_32000)
band-plan 15		Band Plan 997 (BP16_997_4B_4P)
band-plan 16		Band Plan 998 138 4400 (BP17_998_138_4400)
band-plan 17		Band Plan 997 138 4400 (BP18_997_138_4000)
band-plan 18		Band Plan 997 32 4400 (BP19_997_32_4000)
band-plan 21		Band Plan 998 138 4400 Option Band
band-plan 22		Band Plan 997 138 4400 Option Band
band-plan 23		Band Plan 998 138 16000
band-plan 24		Band Plan 998 3B 8KHz
band-plan 25		Band Plan 998 138 17600
band-plan 26		Band Plan CH1 3
band-plan 27		Band Plan CH1 4

Setting up rfi-band

In order to reduce the influence of HAM band, the system can keep the corresponding bands out so as not to be used. The number of RFI Bands used is 13, and they can be selected in multiple. To set Rfi-band the following commands are to be used.

<Table 195> Setting up rfi-band

Command	Mode	Function
rfi-band 1 {on off}	System-profile	1.810 - 1.825 MHz: ANNEX F
rfi-band 2 {on off}		1.810 - 2.000 MHz: ETSI, T1E1
rfi-band 3 {on off}		1.9075 - 1.9125MHz: ANNEX F
rfi-band 4 {on off}		3.500 - 3.575 MHz: ANNEX F
rfi-band 5 {on off}		3.500 - 3.800 MHz: ETSI
rfi-band 6 {on off}		3.500 - 4.000 MHz: T1E1
rfi-band 7 {on off}		3.747 - 3.754 MHz: ANNEX F
rfi-band 8 {on off}		3.791 - 3.805 MHz: ANNEX F
rfi-band 9 {on off}		7.000 - 7.100 MHz: ANNEX F, ETSI
rfi-band 10 {on off}		7.000 - 7.300 MHz: T1E1
rfi-band 11 {on off}		10.100 - 10.150 MHz: ANNEX F, ETSI, T1E1
rfi-band 12 {on off}		14.000 - 14.350 MHz: ANNEX F, ETSI, T1E1
rfi-band 13 {on off}		18.068 - 18.168 MHz: ANNEX F, ETSI, T1E1
rfi-band 14 {on off}		1.800 - 1.825 MHz: HAM Band 1
rfi-band 15 {on off}		3.500 - 3.550 MHz: HAM Band 2
rfi-band 16 {on off}		3.790 - 3.800 MHz: HAM Band 3
rfi-band 17 {on off}		1.800 - 1.810 MHz: RFI Notch
rfi-band 18 {on off}		21.000 - 21.450 MHz: ANNEX F, ETSI, T1E1
rfi-band 19 {on off}		24.890 - 24.990 MHz: ANNEX F, ETSI, T1E1
rfi-band 20 {on off}		28.000 - 29.100 MHz: ANNEX F, ETSI, T1E1
rfi-band 21 {on off}		28.000 - 29.700 MHz: ANNEX F, ETSI, T1E1
rfi-band all {on off}	ALL Bands	

Setting up adsl-safe-mode, tlan-safe-mode

The command of adsl-safe-mode is used to minimize the interference with ADSL and tlan-safe-mode is for reducing the interference with TLAN. When these commands are typed in with the option of 'Enable' only the corresponding part of bands which would be interfered with ADSL/TLAN frequency shall be blocked leaving other part of bands in normal use.

The followings are the commands to set adsl-safe-mode, tlan-safe-mode.

<Table 196> Setting up adsl-safe-mode, tlan-safe-mode

Command	Mode	Function
adsl-safe-mode {enable disable}	System-profile	Set adsl-safe-mode to either Enable or Disable
tlan-safe-mode {enable disable}		Set tlan-safe-mode to either Enable or Disable



Note

When the adsl-safe-mode and tlan-safe-mode are set to enable, as it will block certain part of frequency bands which consequently reduce the data rate. Thus 'Disable' option is recommended as its default setting.

Setting up psd-mask-level

By controlling PSD (Power Spectrum Density) level, which is related to the signal, the system can communicate in the same frequency band without having interference each other. However the PSD is getting too big, then the system may perceive it as a noise. Consequently unwanted interference might be induced. To prevent this, the upper limit of PSD (MASK-Level) is recommended as a standard. U3000 series can adjust the PSD MASK Level of VDSL lines.

The followings are the commands to set PSD MASK Level.

<Table 197> Setting up psd-mask-level

Command	Mode	Function
psd-mask-level default-psd	System-profile	Default PSD
psd-mask-level etsi-m1-cab		Etsi M1 cab
psd-mask-level etsi-m2-cab		Etsi M2 cab
psd-mask-level itu-t-annex-f		ITU-T Annex F (Japan)
psd-mask-level ansi-m1-ex		Ansi M1 Ex
psd-mask-level ansi-m2-ex		Ansi M2 Ex
psd-mask-level etsi-m1-ex-p2		Atsi M1 Ex P1
psd-mask-level etsi-m2-ex-p2		Atsi M2 Ex P2
psd-mask-level ansi-m1-cab		Ansi M1 cab
psd-mask-level psd-china		Psd china
psd-mask-level etsi-m1-ex-p1		Etsi M1 Ex P1

Setting up Ham-band

In the frequency band that VDSL ports of U3000 series are using, the Ham band is included. However, due to the Ham band the VDSL lines might be interfered. To prevent the unwanted interference with Ham band, U3000 series can set the system kept out of using the band. To make the system not to use the Ham band, the following commands are to be used.

<Table 198> Setting up Ham-band

Command	Mode	Function
ham-band 1 {on off}	System-profile	1.800 - 2.000 MHz: Amateur Radio
ham-band 2 {on off}		2.173 - 2.191 MHz: GMDSS
ham-band 3 {on off}		2.850 - 3.155 MHz: Aeronautical Comm.
ham-band 4 {on off}		3.400 - 3.500 MHz: Aeronautical Comm.
ham-band 5 {on off}		3.500 - 3.800 MHz: Amateur Radio
ham-band 6 {on off}		3.800 - 4.000 MHz: Aeronautical/Broadcasting
ham-band 7 {on off}		4.200 - 4.215 MHz: GMDSS
ham-band 8 {on off}		4.650 - 4.850 MHz: Aeronautical Comm.
ham-band 9 {on off}		5.450 - 5.730 MHz: Aeronautical Comm.
ham-band 10 {on off}		5.900 - 6.200 MHz: DRM Radio
ham-band 11 {on off}		6.300 - 6.320 MHz: GMDSS
ham-band 12 {on off}		6.525 - 6.765 MHz: Aeronautical Comm.
ham-band 13 {on off}		7.000 - 7.200 MHz: Amateur Radio
ham-band 14 {on off}		7.200 - 7.450 MHz: DRM Radio
ham-band 15 {on off}		8.405 - 8.420 MHz: GMDSS
ham-band 16 {on off}		8.815 - 9.040 MHz: Aeronautical Comm.
ham-band 17 {on off}		9.400 - 9.900 MHz: DRM Radio
ham-band 18 {on off}		10.005 - 10.100 MHz: Aeronautical Comm.
ham-band 19 {on off}		10.100 - 10.150 MHz: Amateur Radio
ham-band 20 {on off}		11.175 - 11.400 MHz: Aeronautical Comm.
ham-band 21 {on off}		11.600 - 12.100 MHz: DRM Radio
ham-band 22 {on off}		12.570 - 12.585 MHz: GMDSS
ham-band 23 {on off}		13.200 - 13.360 MHz: Aeronautical Comm.
ham-band 24 {on off}		13.570 - 13.870 MHz: DRM Radio
ham-band 25 {on off}		14.000 - 14.350 MHz: Amateur Radio
ham-band 26 {on off}		15.010 - 15.100 MHz: Aeronautical Comm.

ham-band 27 {on off}		15.100 - 15.800 MHz: DRM Radio
ham-band 28 {on off}		16.795 - 16.810 MHz: GMDSS
ham-band 29 {on off}		17.480 - 17.900 MHz: DRM Radio
ham-band 30 {on off}		17.900 - 18.030 MHz: Aeronautical Comm.
ham-band 31 {on off}		18.068 - 18.168 MHz: Amateur Radio
ham-band 32 {on off}		21.000 - 21.450 MHz: Amateur Radio
ham-band 33 {on off}		24.890 - 24.990 MHz: Amateur Radio
ham-band 34 {on off}		26.965 - 27.405 MHz: CB Radio
ham-band 35 {on off}		28.000 - 29.700 MHz: Amateur Radio
all {on off}		Apply to all the 1~35 items.

Setting up Interface

This is how to modify settings for any particular interface regarding VDSL operation.

In order to handle this modification about Interface, you have to get in the interface adjustment mode.

<Table 199> Setting up Interface

Command	Mode	Function
interface IFNAME	Global	Get in the Interface adjustment mode.

While in Interface mode, VDSL related parameters can be modified. The following commands are to be used for modifying them.

<Table 200> VDSL Parameters

Command	Mode	Function
cpe	Line-profile	Manages the modem which is connected to the Interface.
service-alarm-profile		Modify the alarm-profile which will be applied to the Interface.
service-line-profile		Modify the line-profile which will be applied to the Interface.
vdsl-custom-set		Modify the value of stream that is related to a VDSL port. By this modification, the value which is set by this will be applied instead of the value set in line-profile.

Identification of the VDSL profiles

Identification of Alarm-profile

The configured alarm-profile can be identified by this command.

<Table 201> Identification of Alarm-profile

Command	Mode	Function
Show alarm-profile PROFILE_NAME	Enable / Alarm-profile	Identify the content of alarm-profile.

VDSL2#1# show alarm-profile

VDSL Alarm Profile

```

-----
Alarm Profile Name      : DEFVAL
Thresh 15min FECs      : 0
Thresh 15min ESs       : 0
Thresh 15min SESs      : 0
Thresh 15min LOFs      : 0
Thresh 15min LOSs      : 0
Thresh 15min LPRs      : 0
Thresh 15min LOLs      : 0
Thresh 15min LOMs      : 0
Thresh 15min UASs      : 0
Thresh 15min CRC Count : 0

```

```

-----
Alarm Profile Name      : vd-al
Thresh 15min FECs      : 0
Thresh 15min ESs       : 0
Thresh 15min SESs      : 0
Thresh 15min LOFs      : 0
Thresh 15min LOSs      : 0
Thresh 15min LPRs      : 0
Thresh 15min LOLs      : 0
Thresh 15min LOMs      : 0
Thresh 15min UASs      : 0
Thresh 15min CRC Count : 0
-----

```

Identification of line-profile

The configured line-profile can be identified by this command.

<Table 202> Identification of line-profile

Command	Mode	Function
Show line-profile PROFILE_NAME	Enable / line-profile	Identify the content of line-profile.

VDSL2#1# show line-profile

VDSL Line Profile

```

-----
Profile Name           : DEFVAL
Line Type              : Auto Detect All xDSL
Option Band Plan      : (0) Exclude Option(US0) Band
Band Modifier TX       : (1) All Tones On
Band Modifier RX       : (1) All Tones On
Rate Adaptation Mode  : StartUp
Up Slow Rate Ratio     : 0
Down Slow Rate Ratio   : 0
Up Slow Max Rate       : 200000 Kbps
Up Slow Min Rate       : 0 Kbps
Down Slow Max Rate     : 200000 Kbps
Down Slow Min Rate     : 0 Kbps
Up Slow Max Interdelay : 1.0 ms (milliseconds)
Down Slow Max Interdelay : 1.0 ms (milliseconds)
Up Maximum Margin      : 127.5 dB
Down Maximum Margin    : 127.5 dB
Up Min Noise Margin    : 5.0 dB
Up Target Noise Margin : 6.0 dB
Down Min Noise Margin  : 5.0 dB
Down Target Noise Margin : 6.0 dB
Up Max Power           : 63.75 dBm
Down Max Power         : 63.75 dBm
Up Slow Min Protection : 0.000 ms (milliseconds)
Down Slow Min Protection : 0.000 ms (milliseconds)
Power Mode             : (2) 14.5 dBm
IFE RX Filter          : (0) Internal Filter
IFE TX Filter          : (0) Internal Filter
TCM (Trellis Code Modul.) : disable
G.Handshake            : V43 A43
PBO Config             : disable
PBO Length             : 100 meters
-----

Profile Name           : 100M
Line Type              : Manual Customized
                       VDSL ANSI
                       VDSL2 ITU G993 2 8D
                       VDSL2 ITU G993 2 12A

```

VDSL2 ITU G993 2 17A
VDSL2 ITU G993 2 30A

Option Band Plan : (2) Annex M 25 KHz ~ 276 KHz (6-64)
 Band Modifier TX : (1) All Tones On
 Band Modifier RX : (1) All Tones On
 Rate Adaptation Mode : StartUp
 Up Slow Rate Ratio : 0
 Down Slow Rate Ratio : 0
 Up Slow Max Rate : 200000 Kbps
 Up Slow Min Rate : 0 Kbps
 Down Slow Max Rate : 200000 Kbps
 Down Slow Min Rate : 0 Kbps
 Up Slow Max Interdelay : 1.0 ms (milliseconds)
 Down Slow Max Interdelay : 1.0 ms (milliseconds)
 Up Maximum Margin : 127.5 dB
 Down Maximum Margin : 127.5 dB
 Up Min Noise Margin : 5.0 dB
 Up Target Noise Margin : 6.0 dB
 Down Min Noise Margin : 5.0 dB
 Down Target Noise Margin : 6.0 dB
 Up Max Power : 63.75 dBm
 Down Max Power : 63.75 dBm
 Up Slow Min Protection : 0.000 ms (milliseconds)
 Down Slow Min Protection : 0.000 ms (milliseconds)
 Power Mode : (2) 14.5 dBm
 IFE RX Filter : (2) U1 External Filter
 IFE TX Filter : (2) U1 External Filter
 TCM (Trellis Code Modul.) : disable
 G.Handshake : V43 B43
 PBO Config : disable
 PBO Length : 100 meters

Identification of system-profile

The configured system-profile can be identified by this command.

<Table 203> Identification of system-profile

Command	Mode	Function
Show system-profile PROFILE_NAME	Enable / system-profile	Identify the content of system-profile.

```
VDSL2#1# show system-profile
```

```
VDSL System Profile
```

```
-----
```

	Configured	Current Working
Band Plan	: (8) Band Plan 998 6 (BP998_6B)	(Same to left)
PSD Mask Level	: (11) PSD K (Korean M1 FTTCab)	(Same to left)
TLAN Safe Mode	: disable	(Same to left)
ADSL Safe Mode	: disable	(Same to left)
Bit Swap	: disable	(Same to left)
HAM Band	: All Bands Disable	(Same to left)
RFI Band	: All Bands Disable	(Same to left)

```
-----
```

Identification of Interface

With the commands in the table below, you can identify the content for any particular interface regarding VDSL operation.

<Table 204> Identification of Interface

Command	Mode	Function
show port alarm-profile	Enable	Shows the content of alarm-profile which is applied to the specified Port.
show port bit-loading		Shows the information of bit-loading which is applied to the specified Port.
show port cpe-status		Shows the status information of CPE which is connected to the specified Port.
show port cpe-version		Shows the version number and ID information of CPE which is connected to the specified Port.
show port line-ewl		Shows the estimated value of EWL(Eletronic Wire Length) which is related to the specified Port.
show port line-profile		Shows the information of line-profile which is applied to the specified Port.
show port line-rate		Shows the information of line-rate which is applied to the specified Port.
show port line-snr		Shows the information of SNR, Authentication, and Tx

		Power which is applied to the specified Port.
show port vdsl- chan-perf-count		Shows the statistics of VDSL CHAN PERF which is applied to the specified Port.
show port vdsl- major		Shows the statistics of VDSL PERF based upon major items of a port.
show port vdsl-perf- count		Shows the statistics of VDSL PERF of a port.
show port vdsl- perf-second		Shows the statistics of VDSL PERF of a port based upon time passing.
show port vdsl- ptmf		Shows the statistics of VDSL PTMP for a port.