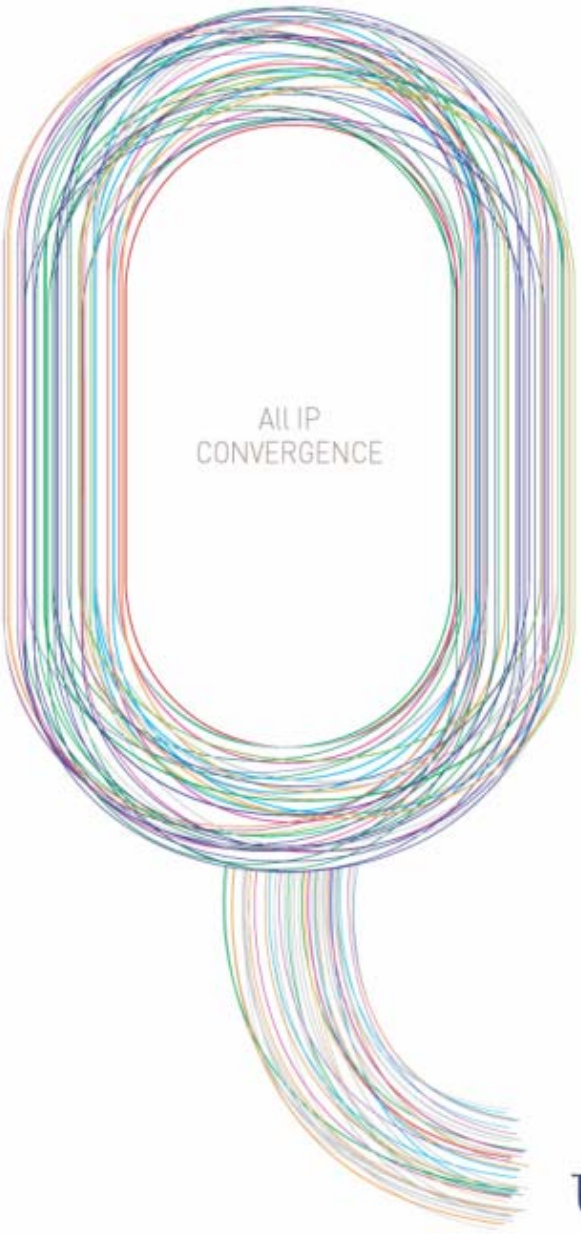
L3
SWITCH

P8824XG

■ User Guide



ubiQuoss

L3
SWITCH

P8824XG

■ User Guide

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

Preface

This preface provides the overview of P8824XG user guide, which describes guide conventions, and lists other publications that may be useful.

Introduction

This guide provides the information required for configuring and operating the network environment after the installation of P8824XG switch hardware.

The target readers of this guide are Ethernet-based network administrators and related engineers who are responsible for installing and setting network equipment. This guide will help them configure optimum networks and operate & manage them more effectively. This guide also provides the information on how to solve problems that may occur during the network operation. Therefore, this guide assumes that the readers have basic working knowledge of:

- Local Area Networks (LAN) and Metro Area Network (MAN)
- Ethernet, Fast Ethernet, and Gigabit Ethernet concepts
- Ethernet switching and bridging concepts
- Routing concepts
- TCP/IP (Transmission Control Protocol/Internet Protocol) concepts
- Routing Information Protocol (RIP) and Open Shortest Path First (OSPF)
- Simple Network Management Protocol (SNMP)

Notice For more information on the installation and the initial configuration of P8824XG switch hardware, please refer to the hardware installation guide of each system.

Conventions

The following <Table 1> and <Table 2> list conventions and icons used throughout this guide.

Table 1. Text Conventions

Convention	Description
Screen displays	■ The information displayed on the OAM terminal screen as a result of command execution ■ This typeface indicates command syntax
Screen displays bold	■ This typeface indicates how you would type a particular command
[Key] names	■ To indicate pressing a key of the keyboard, a square bracket is used with the key, for example, [Enter] or [Ctrl]. ■ When two or more keys are pressed at the same time, the two keys are connected with '+', for example, [Ctrl] + [z]
Words in *italicized* type	■ Used to emphasize a point or denote new terms where they are defined in the text. ■ Parameters that users enter in the system command syntax

Table 2. Notice Icons

Icon	Notice Type	Description
	Notice	■ Important features, characteristics, commands or tips
	Warning	■ Danger that can cause bodily injury, data loss, or system damage

Related Documents

P8824XG switch manual set includes as follows:

Manual	Contents
Hardware Installation Guide	■ Switch hardware installation ■ Initial operating environment configuration
User Guide	■ Operating configuration for services ■ System operation, administration and maintenance ■ Trouble Shooting

Notice You can download or request the latest documents and information on the products of Ubiquoss Inc. including P8824XG from the website (http://www.ubiquoss.com).
This document is the manual for the P8824XG.

Organization

The chapters of this manual are organized as follows:

Chapter 1.Starting P8824XG

This chapter provides the following information required for the system administrator to set up the configuration and to start up P8824XG switch.

Chapter 2.Interface Configuration

This chapter describes the Interface of the system.

Chapter 3.VLAN

This chapter describes the VLAN of system.

Chapter 4.IP Configuration

This chapter explains how to set IP address.

Chapter 5.DHCP

This chapter describes the DHCP configuration of system.

Chapter 6.NAT

This chapter explains NAT setting of P8824XG switch.

Chapter 7.IGMP Snooping

This chapter introduces the IGMP Snooping functionality of P8824XG.

Chapter 8.Multicast Routing

This chapter describes IP multicast routing elements and IP multicast routing setting of P8824XG switch.

Chapter 9.Routing Protocol

This chapter describes the IP unicast routing protocols available in P8824XG. This chapter assumes that the users are familiar with IP unicast routing.

Chapter 10.LACP

This chapter descirbes how to configure IEEE 802.3ad Link Aggregation Control Protocol (LACP) on the switch.

Chapter 11.Statistics Monitoring and QoS

This chapter describes how to view the current operating status of P8824XG switch, how to display information in the log, and how to take advantage of available Remote Monitoring (RMON) capabilities.

Chapter 12.STP and SLD

This chapter explains how to configure the Spanning Tree Protocol (STP) and Rapid Spanning Tree Protocol (RSTP) on the switch.

Chapter 13.Configuration saving & Software Upgrade

This chapter describes the procedure for upgrading the system software image. This chapter also discusses how to save booting image and configuration file on P8824XG switch.

Chapter 14.IP Account and Snoop Device

This chapter describes the IP Account functions of 8700 Series switch and the snoop devices.

Chapter 15.CPU-FILTER & IP-OPTION

This chapter describes how to set CPU-Filter and IP-OPTION

Chapter 16.VRRP

This chapter describes the VRRP configuration of system.

Chapter 17.Utilities

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

Chapter 18.Dynamic ARP Inspection

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

Chapter 19.ARP Snoop

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

Table of Content

Preface II
Introduction II
Conventions II
Related Documents III
Organization IV
Table of Content VI
Figure and Table List XV

Chapter 1.Starting P8824XG 1

Command Line Edit and Help 2
Understanding the Command Syntax 2
Command Syntax Helper 2
Abbreviated Syntax 4
Symbols 4
Line Editing Keys 5
Switch Command Mode 7
P8824XG Switch Startup 9
User Interface 10
Connection through Console Port 10
Connection through Telnet 11
Connection through SNMP Network Manager 11
Account Management & Authentication 12
Add/Delete User 12
Password Setting 13
Privileged mode password setting 14
Password Encryption Setting 14
User Authentication 14
User Authentication Setting 15
Authentication Server Setting 15
Hostname Setting 17
SNMP (Simple Network Management Protocol) 18
SNMP Community Setting 19
SNMP Trap Setting 19
System Contact Setting 20
System Location Setting 20
ACL (Access Control List) 21
Rules for Access List Creation 21
Configuration of Standard IP Access List 21
Configuration of Extended IP Access List 22
Configuration of Access List for Telnet Connection 23
NTP Setting 24
NTP Introduction 24
NTP Commands 24
NTP Setting Example 24

Chapter 2.Interface Configuration 25

P8824XG Interface 26
Common Commands 27
Interface Name 27
Interface ID 27
Interface Mode Prompt 28
Description Command 28
Show Interface Information and Status 29
Show Interfaces Command 29
Show Port Status Command 29
Show Switchport Command 30
Physical Port Configuration 31
Shutdown 31
Speed and Duplex 32
Broadcast Suppression 33
Port Mirroring 34
Layer 2 Interface Configuration 35
VLAN Trunking 35
Layer 2 Interface 35
Layer 2 Interface Defaults 35
Layer 2 Interface Configuration/Cancel 35
Trunk Port Setting 36
Access Port Setting 37
Port Group 38
Port Group Introduction 38
Port Group Configuration 38
MAC Filtering 39
MAC Filtering Introduction 39
MAC Filtering Configuration 39

Chapter 3.VLAN 40

VLAN Overview 41
Definition 41
Advantages of VLAN 41
VLAN Types 42
Port-Based VLAN (Port-Based VLANs) 42
Connecting Switches with a Port-based VLAN 42
Tagged VLANs 44
Uses of Tagged VLANs 44
Assigning a VLAN Tag 44
Mixing Port-based VLAN and Tagged VLAN 45
VLAN Names 46
VLAN ID 46
Default VLAN 46
Native VLAN 46
Configuring VLAN on the Switch 48
Commands for VLAN configuration 48
Examples of VLAN Configuration 50
Displaying VLAN Settings 52
802.1QinQ 53

Private Edge VLAN 56
Abnormal MAC Drop 58

Chapter 4.IP Configuration 59

Assigning an IP address 60
ARP (Address Resolution Protocol) 62
Configuration of Static Routes 63
IP Configuration Examples 64

Chapter 5.DHCP 67

DHCP Configuration 68
Overview of DHCP Server Functions 68
IP Address Allocation Mechanism of DHCP Server 68
P8824XG Switch as a DHCP Server 69
P8824XG Switch as DHCP Relay Agent 70
Advantages of DHCP Server 71
DHCP Address Pool Setting 71
DHCP Address Pool Setting 71
Setting DHCP Network Pool Name and Entering DHCP Configuration Mode 72
Configuration of DHCP Server Boot File 72
Setting Default Router for Client 72
Setting DNS IP Server for Client 72
Setting the Domain Name for Client 72
Setting Group for Network Pool 73
Setting the Address Lease Time 73
Setting DHCP Subnet and Network Mask 73
Setting the NetBios WINS IP Server for Client 74
Setting NetBIOS Node Type for Client 74
Setting IP Address Range to Be Assigned in Network Pool 74
DHCP Host Pool Setting 75
Setting DHCP Host Pool Name and Entering DHCP Configuration Mode 75
Setting client for Client DHCP Manual Binding 76
Other Global Command 77
DHCP Server Enabling 77
Registering DHCP Relay Agent 77
Server Configuration in DHCP Relay Agent 77
DHCP relay information option (OPTION82) Configuration 78
Enabling DHCP Relay Function 78
DHCP Server Monitoring and Management 79
Displaying DHCP Server Pool Information 79
Displaying DHCP Server Binding 79
DHCP Server Statistics Inquiry 79
DHCP Server Conflict Inquiry 79
DHCP Server Variable Initialization Command 80
DHCP Relay Monitoring and Management 81
Example of DHCP Configuration 82
Example of DHCP Network Pool Configuration 82
Example of DHCP Host Pool Configuration 83
Example of DHCP Server Monitoring and Management 83

Example of DHCP Relay Agent Configuration 86

Chapter 6.NAT 87

NAT Introduction 88
NAT Configuration 89
Static NAT Configuration 89
Dynamic NAT Configuration 89
Setting Local NAT 91
Enabling NAT 92
NAT Configuration 93
Static NAT Setting Information Inquiry 93
Dynamic NAT Configuration Information Inquriy 93
Local NAT Configuraion Information Inquiry 93

Chapter 7.IGMP Snooping 94

IGMP Snooping Introduction 95
IGMP Snooping Configuration 96
Enable Global IGMP Snooping 96
Enable IGMP-TRAP on an Interface 96
Enable IGMP snooping on a VLAN 97
Configure IGMP Snooping Functionality 97
IGMP Proxy-Reporting Overview 104
IGMP Proxy-Reporting Setup 105
Enable IGMP Proxy-Reporting 105
Enable IGMP Proxy-Reporting on a VLAN 105
Configure IGMP Proxy-Reporting Functionality 106
Specifying Multicast Router Port 106
Display System and Network Statistics 108

Chapter 8.Multicast Routing 109

IP Multicast Routing Overview 110
IGMP Overview 110
PIM-SM Overview 110
IP Multicast Routing Setting 111
Enable IP Multicast Routing 111
Enable IGMP-TRAP on an interface 111
Enable PIM on an interface 111
Enable IGMP on an interface 111
Configure IGMP Functionality 112
Configure PIM-SM Functionality 115
IP Multicast Routing Monitoring Commands 121

Chapter 9.Routing Protocol 122

Routing Protocol Overview 123
RIP vs OSPF 123
RIP overview 124
Routing Table 124
Route Advertisement of VLANs 124
RIP Version 1 vs. RIP Version 2 124

OSPF overview 125
Link-state Database 126
Areas 126
AREA 0 126
Stub areas 127
Virtual links 127
Route Redistribution 127
Border Gateway Protocol (BGP) 128
BGP Overview 128
RIP Configuration 130
Commands 130
RIP Configuration 133
Distance Configuration 134
Distribute-list Configuration 135
Offset-List Configuration 137
Passive-Interface Configuration 138
OSPF Configuration 139
Command 139
area 140
Configuration of Example OSPF Network 144
Route Re-Distribution 146
Passive-Interface Configuration 147
BGP Configuration 148
Enabling BGP Protocol 148
Neighbor Configuration 148
BGP Filtering 148
Route Filtering 149
Community Filtering 151
BGP Attribute Configuration 154
As_path Attribute 154
Origin Attribute 154
BGP Nexthop Attribute 156
BGP Nexthop (Multiaccess Networks) 158
BGP Nexthop (NBMA) 158
Nexthopself 158
Local Preference Attribute 159
Metric Attribute 161
Community Attribute 163
Weight Attribute 163
Routing Policy Modification 165
Miscellaneous Functions 167
Use of Set as-path Prepend Command 167
BGP Peer Groups 167
BGP backdoor 168
Route Flap Dampening 170

Chapter 10.LACP 171

Understanding Link Aggregation Control Protocol 172
LACP Modes 172
LACP Parameters 172

Configuring 802.3ad Link Aggregation Control Protocol 174
Specifying the System Priority 174
Specifying the Port Priority 175
Specifying an Administrative Key Value 176
Specifying the Timeout Value 177
Changing the LACP Mode 178
Clearing LACP Statistics 179
Displaying 802.3ad Statistics and Status 180

Chapter 11.Statistics Monitoring and QoS 181

Status Monitoring 182
Port Statistics 183
Logging 186
System Log Message Context 187
Default Logging Value 188
RMON (Remote MONitoring) 189
RMON Overview 189
RMON Alarm and Event Group Setting 191
QoS and Packet Filtering 195
MFC (Multi-Field Classifier) 196
TC (Traffic Conditioner) 201
TC Creat/Cancel 202
TC Inquiry with statistics 203
QoS Parameter 205
Qos-related Parameter Modification 206
Scheduling 207
Extra Filtering 209
sFlow 210
sFlow Agent 210
sFlow Collector 212
sFlow Network Configuariton 214

Chapter 12.STP and SLD 216

Understanding Spanning-Tree Features 217
STP Overview 217
Bridge Protocol Data Units 217
Election of Root Switch 218
Bridge ID, Switch Priority, and Extended System ID 218
Spanning-Tree Timers 219
Creating the Spanning-Tree Topology 219
Spanning-Tree Interface States 220
Understanding RSTP 223
RSTP Overview 223
Port Roles and the Active Topology 223
Rapid Convergence 224
Bridge Protocol Data Unit Format and Processing 225
Configuring Spanning-Tree Features 227
Default STP Configuration 227
STP Configuration Guidelines 227

Enabling STP 227
Disable per VLAN STP 228
Configuring the Port Priority 228
Configuring the Path Cost 229
Configuring the Switch Priority of a VLAN 230
Configuring the Hello Time 230
Configuring the Forwarding-Delay Time for a VLAN 231
Configuring the Maximum-Aging Time for a VLAN 231
Configuring the Port as Edge Port 231
Configuring the RSTP Mode 232
Specifying the Link Type to Ensure Rapid Transitions 233
Restarting the Protocol Migration Process 233
Displaying the Spanning-Tree Status 234
Self-loop Detection 235
Understanding Self-loop Detection 235
Configuring Self-loop Detection 235
Displaying Self-loop Status 237

Chapter 13.Configuration saving & Software Upgrade 239

Flash File System 240
Configuration Saving 241
Deleting Configuration File 241
Configuration Backup 242
Configuration Download 243
Image Upgrade 244
Image/Configuration File Backup 246
System Restart 247

Chapter 14.IP Account and Snoop Device 248

Overview of IP account 249
Commands for IP account 250
Show ip account 250
Installing and executing NTOP 250
Downloading ntop.conf 250
Registering service key 251
Executing NTOP 251
Creating protocol list 252
Snoop device 254

Chapter 15.CPU-FILTER & IP-OPTION 255

CPU Filtering 256
Establishing/unestablishing CPU-filtering rule 256
Establishing CPU-FILTER group 256
Example of establishing CPU-FILTER 258
Overview of IP Option 260
IP option commands 260

Chapter 16.VRRP 262

Information about VRRP 263

VRRP Operation 263
VRRP Benefits 265
Multiple Virtual Router Support 266
VRRP Router Priority and Preemption 266
VRRP Advetisements 266
VRRP Object Tracking 266
How to Configure VRRP 268
Enabling VRRP 268
Disabling VRRP on an Interface 269
Configuring VRRP Object Tracking 269
Configuration Examples for VRRP 271
Configuring VRRP: Example 271
VRRP Object Tracking: Example 272
VRRP Object Tracking Verification: Example 272
Disabling a VRRP Group on an Interface: Example 272

Chapter 17.Utilities 273

Status dump command 274
Command 274
Command history 277
Output Post Processing 278
Overview of output post processing 278
Example of output post processing 278
DDM (Digital Diagnostic Monitoring) 280
DDM Monitoring enable/disable (No command) 280
GBIC status check 280
Setting DDM monitoring threshold 281

Chapter 18.Dynamic ARP Inspection 283

Understanding DAI 284
Understanding ARP 284
Understanding ARP Spoofing Attacks 284
Understanding DAI and ARP Spoofing Attacks 285
Interface Trust States and Network Security 286
Rate Limiting of ARP Packets 287
Relative Priority of ARP ACLs and DHCP Snooping Entries 288
Logging of Dropped Packets 288
Default DAI Configuration 289
DAI Configuration Guidelines and Restrictions 290
Configuring DAI 291
Enabling DAI on VLANs 291
Configuring the DAI Interface Trust State 292
Applying ARP ACLs for DAI Filtering 292
Configuring ARP Packet Rate Limiting 293
Enabling DAI Error-Disabled Recovery 294
Enabling Additional Validation 295
Configuring DAI Logging 297
DAI Logging Overview 297
Configuring the DAI Logging Buffer Size 298
Configuring the DAI Logging System Messages 298

Configuring the DAI Log Filtering 299
Displaying DAI Information 300
DAI Configuration Samples 301
Sample: Interoperate with DHCP Relay 301

Chapter 19.ARP Snoop 306

Understanding ARP Snoop 307
Understanding ARP Snoop 307
ARP Snoop Entry Status 308
ARP Snoop Ageing Time 308
ARP Snoop Binding Health Check 309
ARP Snoop Probe 309
Understanding DAI and ARP Snoop 309
Relative Priority of ARP ACLs and ARP Snoop Entries 310
Default ARP Snoop Configuration 311
Configuring ARP Snoop 312
Enabling ARP Snoop 312
Configuring ARP Snoop Ageing-time 312
Disabling Gratuitous ARP Update without Validation 313
Disabling Health-check 313
Displaying ARP Snoop Information 314
ARP Snoop Configuration Samples 315
Sample One: ARP spoofing detection 315
Sample Two: Interoperate with DAI on DHCP Relay 316

Figure and Table List

Table 1. Text Conventions II
Table 2. Notice Icons III
Table 3. Command Syntax Symbol 4
Table 4. Basic Command Line Editing Command and Help 5
Table 5 Switch Command Mode 7
Table 6. Change of Switch Command Modes 7
Figure 1. Connection of P8824XG Switch and OAM Terminal 10
Table 7. Add/Delete Command 12
Table 8 Commands for Switch Password Setting 13
Table 9 User Authentication Setting Command 14
Table 10. RADIUS Server Setting Command 15
Table 11 TACACS+ Server Setting Command 16
Table 12 Commands for Hostname Setting 17
Table 13. SNMP Configuration Command 18
Table 14. ACL Configuration Command 21
Table 15. Interfaces Supported by P8824XG Switch 26
Table 16. P8824XG Switch Port Commands 27
Table 17. Interface Name 27
Table 18. Interface ID and range 27
Table 19. Commands Related to Interface Information and Status 29
Table 20. Physical Port Configuration Command 31
Table 21. Broadcast Suppression Command 33
Table 22. Port Mirroring Command 34
Table 23. Layer 2 Interface Modes 35
Table 24. Layer 2 Interface Defaults 35
Table 25. Layer 2 Interface Setting/Clear Command 35
Table 26. Commands for Trunk Port Configuration 36
Table 27. Trunk Port Configuration Command 36
Table 28. Command for Access Port Configuration 37
Table 29. Command for Port Group Configuration 38
Table 30. Command for Layer 3 Interface Configuration 39
Figure 2. Example of a Port-based VLAN (8000 Switch) 42
Figure 3. Single Port-based VLANs Connecting 2 Switches 43
Figure 4. Two Port-based VLANs Connecting 2 Switches 43
Figure 5. Physical Diagram of Tagged and Untagged frame 45
Figure 6. Logical Diagram of Tagged Frame and Untagged frame 45
Figure 7. Native VLAN 47
Table 31. Commands for VLAN Configuration 48
Figure 8. VLAN Configuration Example – Tagged and Untagged VLAN 50
Table 32. 802.1QinQ Command Set 53
Table 33. Private Edge VLAN Setting table 56
Table 34. Abnormal MAC Drop commands 58
Table 35. Available IP Address 60

Table 36. Command for IP Address Setting..... 61
Table 37. Commands for ARP Table Configuration 62
Table 38. Commands for Static Route Configuration 63
Table 39. Default Administrative Distances of Dynamic Routing Protocol 63
Figure 10. Example Network for IP Configuration – Secondary IP Configuration 64
Figure 11. Example Network for IP configuration – Static route 65
Figure 12. P8824XG Switch as a DHCP Server..... 69
Figure 13. P8824XG Switch as a DHCP Relay Agent..... 70
Table 40. Host Pool Configuration Command 75
Table 41. Manual Binding Command..... 76
Table 42. Global Command List 77
Table 43. Command for Registering DHCP Relay Agent 77
Table 44. DHCP Relay Monitoring and Management Command 81
Figure 14. Example Network for DHCP Relay Agent Configuration..... 86
Table 46. IGMP Snooping-related monitoring command..... 108
Figure 15. Multicasting to Transmit Traffic to Many Destinations 110
Table 47. Multicast Protocol..... 110
Table 48. LSA Type number..... 126
Figure 16. RIC Network Configuration..... 133
Table 49. RIP Network Configuration Example and Diagram..... 133
Table 50. Commands after Router ospf Command Execution 139
Table 51. Sub Commands 140
Figure 17. Virtual Link Network..... 142
Figure 18. OSPF Network Example 144
Table 52. Items for Route Dampening 170
Table 53. Status Monitoring Command..... 182
Table 54. Port Statistics Inquiry Command..... 184
Table 55. Port Statistics Inquiry Setting Command 185
Table 56. Port Statistics Initialization Command..... 185
Table 57. P8824XG Switch Log Level 186
Table 58. System Log Defaults..... 188
Table 59. Commands for System Message Logging Configuration 188
Figure 19. RMON Manager and RMON Probe 189
Table 60. RMON Items 191
Table 61. RMON Alarm and Event Setting Command..... 191
Table 62. Commands for RMON Statistics and History Setting..... 192
Table 63. Command for Flow-rule Classification 196
Table 64. Command for Flow-rule Policy..... 197
Table 65. Command for Flow-rule 198
Table 66. Command for Flow-rule Cancel 198
Table 67. Command for Policy-map Creat/Add 198
Table 68. Policy-map Create and Profile Modification..... 199
Table 69. Command for Policy-map Cancel and Specific Flow-rule Cancel ... 199
Table 70. Command for Policy-map Apply/Cancel 199
Table 71. Command for Flow-rule Inquriy..... 199

Table 72. Command for Traffic Conditioner Creat 202
Table 73. Command for Traffic Conditioner Cancel 202
Table 74. Command for Traffic Conditioner Table Inquriy 203
Table 75. Command for Traffic Conditioner Statistics Inquiry 203
Table 76. Command for QoS-related Marking/Remarking Table Inquiry 205
Table 77. Command for Qos-related Marking/Remarking Table Setting 206
Table 78. Command for Queue-method Modification 207
Table 79. Command for Wrr-method Queue Weight Modification 208
Table 80. Command for Queue-method of the Whole Interfaces and Wegith Inquriy 208
Table 81. Command for Other Filtering 209
Table 82. sFlow Command 211
Table 83. Switch Priority Value and Extended System ID 219
Table 84. Spanning-Tree Timers 219
Table 85. Port State Comparison 224
Table 86. RSTP BPDU Flags 225
Table 87. Default STP Configuration 227
Table 88. Command for the File Management 240
Table 89. Command for Configuration Saving 241
Table 90. Command for Configuration Backup 242
Table 91. Command for Configuration Download 243
Table 92. Command for Image Download 244
Table 93. Image Backup Command 246
Table 94. Show ip account 250
Table 95. ntop execution/stop commands 251
Table 96. Protocol list commands 252
Table 97. Snoop device commands 254
Table 98. CPU-filtering rule 256
Table 99. Unestablishing cpu-filter rule 256
Table 100. CPU filter group 257
Table 101. cpu-filter group 257
Table 102. cpu-filter group forward 257
Table 103. Service cpu-filter 258
Table 104. Example of cpu-filter 258
Table 105. How to disallow FTP traffic 258
Table 106. show cpu-filter group 258
Table 107. show cpu-filter 259
Table 108. IP option commands 260
Figure 24. Basic VRRP Topology 264
Figure 25. Load Sharing and Redundancy VRRP Topology 265
Table 109. show tech 274
Table 110. Command history view and setting commands 277
Table 111. output post processing 278
Table 112. output post processing 278
Table 113. show ip interface 279
Table 114. Digital Diagnostic Monitoring 280

Table 115. DDM Monitoring enable/disable 280
Table 116. show port status gbic..... 280
Table 117. DDM monitoring threshold 281
Table 118. DAI Configuration 301
Figure 26. ARP snoop (3-way handshake)..... 308

Chapter 1. Starting P8824XG

This chapter provides the following information required for the system administrator to set up the configuration and to start up P8824XG switch.

- Command line edit and help
- Switch command mode
- Switch startup
- P8824XG switch user interface
- Switch login and password setting
- SNMP configuration
- Viewing and saving the files and configuration of switch
- Access list
- Telnet Client

Command Line Edit and Help

This chapter provides the information on command line editor and help.

Understanding the Command Syntax

This section describes the steps to take when entering a command. Refer to the sections that follow for detailed information on using the command-line interface

To use the command-line interface, follow the following steps:

1) When entering a command at the prompt, ensure that you have the appropriate privilege level. Most configuration commands require the administrator privilege level.

2) Enter the command name. If the command does not include a parameter or values, skip to step 3. If the command requires more information, continue to step 2) a.
   a. If the command includes a parameter, enter the parameter name and values.
   b. The value part of the command specifies how you want the parameter to be set. Values include numerics, strings, or addresses, depending on the parameter.

3) After entering the complete command, press [Return].

Notice When entering a command, you may receive a message, "%Command incomplete.". This means that the command you entered was not executed. If you press Up arrow key, your last command will be displayed.

The following shows the command that is entered and not executed.

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

Command Syntax Helper

The CLI of P8824XG has built-in command syntax helper. Help may be requested at any point in a command by entering a question mark '?'.

Two styles of help are provided:

- Full help
  - Available when ready to enter a command argument (e.g. 'show ?'). Describes each possible argument. (Note: a space between command and question mark is required).

- Partial help
  - Provided when an abbreviated argument is entered and want to know what arguments match the input (e.g. 'show me?'.) There is no space between command and question mark.

The following below shows an example of full help style with show command. A question mark isn't

displayed on the terminal screen like [Return] key.

```
Switch# show ?
  arpDisplay ARP table entries
  authentication  Authentication configurations parameters
  clock  show current system's time
  config  Show config file information
  cpuCPU information
  debugging  Debugging functions
  flash  Show flash filesystem information
  flow-rule  flow-rule
  igmpsnoop  IGMPSNOOP Tree
  interface  Interface status and configuration
  ip IP information
  lacp  Port group information
  loggingShow 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
  ntpshow current ntp status
  port  Port status and configuration
  port-group  Port-group configuration
  private-edge-vlan  Private edge vlan configuration
  privilege  Display your current level of privilege
  processes  Active process statistics
  qosQos 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
  startup-config  Show startup config file information
  switchport  Switching port configuration
  system  Display the system information
  tc-table  traffic-conditioner-table
  temperature Temperature and Threshold information
  uptime  Display elapsed time since boot
  users  Display information about terminal lines
  versionDisplay the system version
  vlans  VLAN information
Switch# show_
```

Partial help function can be used with the show command Type '?'. After typing the show command as shown below, wait for the blink of the cursor.

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

Suppose that the operation manager is not familiar with the exact command for the status of the port. If the system administrator enters a ‘p’ and a question mark with no space, CLI helper provides a list of options for the remainder of command

```
Switch# show p?
  pdp     Global PDP configuration subcommands
  port    Display port configuration
  port-group        Port group information
Switch# show p_
```

Abbreviated Syntax

Abbreviated syntax is the shortest, most unambiguous, allowable abbreviation of a command or parameter. Typically, this is the first three letters of the command.

Notice When using abbreviated command syntax, you must enter enough characters to make the command unambiguous, and distinguishable to P8824XG switch. You may receive “%Ambiguous command.”, which means there are more than one commands with the same prefix that you have entered in the mode.

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

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

Symbols

You may see a variety of symbols shown as part of the command syntax. These symbols explain how to enter the command and parameters. The following <Table 3> summarizes the symbols applied to the system command syntax.

Table 3. Command Syntax Symbol

Symbol	Name	Description
<>:	Angle brackets	■ Enclose a variable or value in the command syntax. You must specify the variable or value. For example, in the syntax access-list <1-99> {deny|permit} *address* you must supply standard access control list number for <1-99> when entering the command
{}:	Braces	■ Enclose a required value or list of parameters in the

		command syntax. ■ The administrator must enter at least one necessary item among the parameter list. For example, in the syntax router {*rip*|*ospf*} you must enter one of the two parameter list for specifying routing protocol.
[]:	Square brackets	■ Enclose a required value or list of parameters in the command syntax. ■ The administrator can specify necessary items among the list selectively. There may be no need to specify an item. For example, in the syntax show interfaces [*ifname*] you can enter the interface name for ifname or not.
|:	Vertical bar	■ Separate mutually exclusive items in the list, one of which must be entered. For example, in the syntax switch port mode {access|trunk} you must specify either access or trunk mode of switch port in the command. Do not type the vertical bar.
A.B.C.D		■ IP address or subnet mask
A.B.C.D/M		■ IP prefix (e.g. 192.168.0.0/24)

Line Editing Keys

The CLI of P8824XG switch supports Emacs-like line editing commands. The following < Table 4> describes the line-editing keys available using the CLI.

Table 4. Basic Command Line Editing Command and Help

Command	Description
[Ctrl] + [A]	■ Move the cursor to the beginning of the line.
[Ctrl] + [E]	■ Move the cursor to the end of the line.
[Ctrl] + [B]	■ Move the cursor to the next word.
[Ctrl] + [F]	■ Move the cursor to the left character.
Backspace	■ Delete the character in front of the cursor.
[Ctrl] + [K]	■ Delete all the characters from the cursor to the end of the line
[Ctrl] + [U]	■ Delete all the letters from the cursor to the beginning of the line.
Tab	■ If you type a part of a command and press [tab], the commands with the same prefix on the prompt will be listed. ■ If there is only one command with the prefix, the rest part of the command is completed.
[Ctrl] + [P] or ↑	■ Display the history of the last 20 commands you have entered.
[Ctrl] + [N] or ↓	■ Display the next command.
?	■ Display the list of the available commands on the prompt and the description on the commands. ■ If you type '?' after a command, the parameters required after the

	command will be listed. ■ If you type '?" right after a part of a command, the commands with the same prefix will be listed.
Return or Spacebar or Q	■ If you press [Return] in -- More --, the next one line will be displayed. ■ When you press spacebar, the next page will be displayed. Press Q to exit from the program and switch to the prompt state.

Switch Command Mode

P8824XG switch provides the following various CLI (Command Line Interface) access modes, as shown in <Table 5>.

Table 5 Switch Command Mode

Access Mode	Prompt	Description
User mode	Switch>	■ Display common statistic information.
Privileged mode	Switch#	■ Use Show command
Config mode	Switch(config) #	■ Change the scope of switch configuration into global.
Interface mode	Switch(config-if-gi1)# Switch(config-if-vlan1)#	■ Change the configuration of switch interface.
Router mode	Switch(config-rip)# Switch(config-ospf)#	■ Change the configuration of routing protocols such as RIP or OSPF.
DHCP pool mode	Switch(config-dhcp)#	■ Configure the DHCP address pool.

Notice The command prompt will show the name of the switch as host name in front of the mode character(s). The prompt 'Switch' will be used as common host name throughout this guide

When the system administrator sets up the configuration of P8824XG switch, the operation manager will face various kinds of prompts. The prompt shows the path where you are in the configuration mode. To change the configuration of the switch, you have to check prompts. Commands used for changing command prompt mode are shown in <Table 6>.

Table 6. Change of Switch Command Modes

Command	Description
enable	■ Move from the User mode to the Privileged mode. ■ Need to enter the password of the Privileged mode.
disable	■ Move from the Privileged mode to the User mode.
configure terminal	■ Move from the Privileged mode to the Config mode.
interface [*ifname]*	■ Move from the Config mode to the Interface mode.
router {*rip*|*ospf*}	■ Move from the Config mode to the router mode.
exit	■ Move back to the former mode.
end	■ Move from any mode to Privileged mode. ■ Do not move from User mode.

	User
ip dhcp network-pool *name* ip dhcp host-pool *name*	■ Move from the Config mode to the DHCP pool mode

P8824XG Switch Startup

When starting the switch for the first time, P8824XG switch performs self test which loads OS image from the flash memory on its main memory, and starts the system. When the system is booted, the switch loads the previous configuration (startup-config) saved in the flash memory.

Notice For the purpose of system reliability, P8824XG switch manages two OS images including Primary and Secondary. Primary OS image would be loaded by default setting. System Administrator can change the configuration in a switch boot mode or privileged mode.

User Interface

Network administrators can access the switch for configuration setting, configuration verification, and switch status management and etc. The simplest way to access the switch is to access by local OAM terminal connected to the console port provided by P8824XG switch (Out-of-band management).

Another way to access the switch is to use a Telnet program from remote site. The switch does not support separate port for the Telnet connection from remote. Therefore, access must take place through the service port (In-band management).

The system administrator can use the followings to manage P8824XG switch.

- Access the CLI by connecting a local terminal to the switch console port
- Access the CLI over a TCP/IP network through a telnet connection.
- Use an SNMP network manager over a network running the IP protocol.

P8824XG switch can support up to multiple user sessions concurrently, as follows:

- One console session
- Up to tenTelnet sessions.

Connection through Console Port

The command-line interface built into the system is accessible by way of the RJ-45 type Ethernet port labeled console. OAM terminal (or workstation with terminal-emulation software) must support 9-pin, RS-232 DB9 port. Console port is located on the back of the P8824XG switch SGIM (Switching, Gigabit ethernet I/O & Management Module).

Connect the terminal to the console port provided by P8824XG switch, as shown in <Figure 1>. Once connection is established, you will see the switch prompt and you may log in.

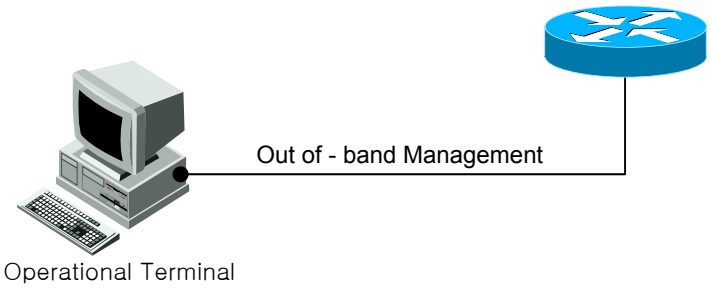


Figure 1. Connection of P8824XG Switch and OAM Terminal

Notice *For the information on the terminal configuration and console port pinouts, refer to the P8824XG switch Hardware Installation Guide.*

Connection through Telnet

Any workstation with a Telnet facility should be able to communicate with the P8824XG switch over a TCP/IP network. To use Telnet, the administrator must set up Telnet passwords and the switch must have at least one IP address.

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

When the telnet connection is successfully completed, a prompt for user password will be displayed. When you enter the Telnet user password, you will be in the User mode of the switch.
For security purpose, you can use the access list to restrict the Telnet connection. For more information, see ACL (Access Control List).

Connection through SNMP Network Manager

Any network manager running the Simple Network Management Protocol (SNMP) can manage the P8824XG switch.

Notice For more information on SNMP Network Manager, refer to SNMP section.

Account Management & Authentication

Add/Delete User

Administrator needs user registry to log in switch through console port or telnet. P8824XG can add/delete users and set up password, privilege, session timeout time, and access list for each user.

Notice For more information, see ACL (Access Control List) section.

Table 7. Add/Delete Command

Command	Description	Mode
username *userID* nopassword	■ UserID Creation ■ No password	Config
username *userID* password *password* username *userID* password 0 *password*	■ UserID Creation ■ Input password that is not yet encrypt	Config
username *userID* password 7 *password*	■ UserID Creation ■ Input encrypt password	Config
username *userID* privilege <0-15> nopassword	■ UserID Creation ■ No password ■ If privilege is 15, highest priority privilege (enable mode).	Config
username *userID* privilege <0-15> password *password* username *userID* privilege <0-15> password 0 *password*	■ UserID Creation ■ If privilege is 15, highest priority privilege (enable mode). ■ Input password that is not yet encrypt	Config
username *userID* privilege <0-15> password 7 *password*	■ UserID Creation ■ If privilege is 15, highest priority privilege (enable mode). ■ Input encrypt password	Config
username *userID* timeout <0-600>	■ Set session timeout per user (default 20 minutes)	Config
no username *userID* timeout	■ Delete session timeout per user ■ Return to the initial session timeout (20 minutes)	Config
username *userID* access-class *access-list-num*	■ Apply the access list to the user. ■ *access-list-num* : <1-99>, standard ip access list	Config
no username *userID* access-class	■ Clear the access list applied to the user.	Config
no username *userID*	■ UserID Delete	Config

	■ If userID is “root”, password is changed to default password.	

```
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)# user 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#
```

Password Setting

P8824XG switch uses two passwords for the system security.

- Enable password
  - Used for the security of the privileged mode.
- User password
  - Used by the user to access the switch through Telnet in the user mode.

The following table describes the commands related to password setting.

Table 8 Commands for Switch Password Setting

Command	Description	Mode
enable password *<password>*	■ Specify the password of the privileged mode.	Config
no enable password	■ Delete the password of the privileged mode.	Config
service password-encryption	■ Set up the password encryption mode.	Config
no service password-encryption	■ Delete the password encryption mode.	Config

Notice For more information, see < Add/Delete user >.

Privileged mode password setting

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

Password Encryption Setting

As in the examples above, anybody can see passwords with show running-config command after password setting. For security purposes, P8824XG switch supports encryption mode setting

```
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#
```

User Authentication

P8824XG can set up various types of user authentication. Normally, user authentication is given by user ID and password. But with RADIUS and TACACS+, the authorization to access to the subscriber database of each server is given.

Table 9 User Authentication Setting Command

Command	Description	Mode
authentication login enable (local | radius | tacacs)	■ Choose authentication system (local, radius, and tacacs). ■ Various authentications are possible.	Config
no authentication login enable (radius | tacacs)	■ Set usable authentication as not to use. ■ Always use local authentication	Config
authentication login primary (local | radius | tacacs)	■ Set up authentication system for primary authentication.	Config
no authentication login primary (local | radius | tacacs)	■ Clear authentication system for primary authentication.	Config
authentication login template-user *userID*	■ User authenticated by RADIUS or TACACS+ can not login without local account. User should set up account to	Config

	use.	
no authentication login template-user	■ Clear the account of users without account	Config
show authentication login primary	■ Show authentication system	Enable

User Authentication Setting

Three ways of user authentication are as following;

- Check access right with user ID and password
- Use RADIUS server
- Use TACACS+ server

When using more than one way, you authenticate based on the authentication priority. If authentication is succeeded, login through set account. If it is not, authenticate with the next priority.

```
Switch# configure terminal
Switch(config)# authentication login template-user lns
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 localenable

Switch#
```

Authentication Server Setting

Table 10. RADIUS Server Setting Command

Command	Description	Mode
radius-server host A.B.C.D	■ Set up radius-server	Config
no radius-server host A.B.C.D	■ Delete set radius-server	Config
radius-server host A.B.C.D key *encryption-key*	■ Set up radius –server ■ Set up encryption key to access to server.	Config
radius-server host A.B.C.D auth-port <0-65536>	■ Set up radius –server ■ Set up auth-port to access to server.	Config
no radius-server host A.B.C.D auth-port	■ Delete auth–port to access to server. Use default auth-port.	Config
radius-server host A.B.C.D auth-port <0-65536> key *encryption-key*	■ Set up radius –server ■ Set up auth-port to access to server ■ Set up encryption key to access to server.	Config
radius-server key *encryption-key*	■ Set up genera key to access to Radius-server. ■ Use general key if key is not set in server	Config

no radius-server key	■ Delete set general key.	Config
radius-server retransmit <1-5>	■ Set up retry counter when accessing to radius-server.	Config
no radius-server retransmit	■ Delete set retry counter (Default : 3)	Config
radius-server timeout <1-1000>	■ Set time to get response packet	Config
no radius-server timeout	■ Delete set timeout time.(Default : 5)	Config

You can set various RADIUS servers.
If first server is not authenticated, authentication attempt will be passed to the other servers.

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

Table 11 TACACS+ Server Setting Command

Command	Description	Mode
tacacs-server host A.B.C.D key *encryption-key*	■ Set up Tacacs -server setting ■ Set up encryption key to access the server	Config

You can set various TACACS+ servers.

If first server is not authenticated, authentication attempt will be passed to the other servers.

```
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#
```

Hostname Setting

Hostname can be used to identify systems during the operation, and the prompt of the console/Telnet screen consists of the combination of hostname and current command modes. In P8824XG switch, the system model name is the default hostname and the administrator can change the default hostname to a new hostname.

Table 12 Commands for Hostname Setting

Command	Description	Mode
hostname <*hostname*>	■ Change hostname.	Config
no hostname	■ Change hostname to default.	Config

The procedures to set and change the hostname are shown below.

```
Switch# configure terminal
Switch(config)# hostname P8000
P8000(config)# end
P8000#

P8000# configure terminal
P8000(config)# no hostname
Switch(config)# end
Switch#
```

SNMP (Simple Network Management Protocol)

SNMP network manager can manage the switch that provides Management Information Base (MIB). The network manager provides user interface for easy management purpose. You have to properly configure the environment of switch in order to use the SNMP manager to manage P8824XG switch.

To access SNMP agent, you need one or more IP addresses of the switch. For the information on IP address configuration, see the following table.

Table 13. SNMP Configuration Command

Command	Description	Mode
snmp-server contact *string*	■ Change the system contact information.	Config
snmp-server location string	■ Change the system location information.	Config
snmp-server community *community-string* [ro|rw] [*access-list number*]	■ Set up an SNMP community. ■ *access-list number* : Standard IP access-list <1-99> ■ *ro* : read only ■ *rw* : read write	Config
no snmp-server community *community-string*	■ Delete an SNMP community.	Config
snmp-server [enable|disable] traps	■ Set up whether to send or not to send SNMP Trap to Trap Host.	Config
snmp-server host *A.B.C.D trap-community-string*	■ Set up SNMP Trap Host.	Config
no snmp-server host *A.B.C.D*	■ Delete SNMP Trap Host.	Config
show snmp	■ Display SNMP statistics.	Privileged

Command	Description	Mode
snmp-server contact *string*	■ Change the system contact information	Config
snmp-server location *string*	■ Change the system location information.	Config
snmp-server community *string* [ro|rw] [host *A.B.C.D /mask*]	■ Set up an SNMP community ■ *ro* : read only ■ *rw* : read write ■ *A.B.C.D /mask* : IP address / prefix length	Config
no snmp-server community *string*	■ Delete an SNMP community.	Config
snmp-server enable traps	■ Set up whether to send SNMP Trap to Trap Host	Config
no snmp-server enable traps	■ Set up whether not to send SNMP Trap to Trap Host	Config
snmp-server trap-host *A.B.C.D* community *string*	■ Set up a Community to send SNMP Trap Host.	Config
no snmp-server trap-host *A.B.C.D*	■ Delete SNMP Trap Host.	Config

SNMP Community Setting

The community strings allow a simple method of authentication between the system and the remote network manager. There are two types of community strings on the P8824XG switch.

- Read community strings
  - Provide read-only access to the system.
  - The default read-only community string is *public*.

- Read-write community strings
  - Provide read and write access to the system.
  - The default read-write community string is *private*.

```
Switch# configure terminal
SWITCH(config)# snmp-server community public ro
SWITCH(config)# snmp-server community private rw
SWITCH(config)# snmp-server community lns ro host 192.168.0.0/24
SWITCH(config)# end
SWITCH# show running-config
!
snmp-server community public ro
snmp-server community private rw
snmp-server community lns ro host 192.168.0.0/24
!
SWITCH#
```

Notice When host is set, communicity can be only used within the SubNetwork range.

SNMP Trap Setting

An authorized trap receiver can be one or more network management station on your network. P8824XG switch sends 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
snmp-server trap-host 192.168.0.3 community private
!
SWITCH#
```

System Contact Setting

The system contact is a text field that enables to enter the name of the person(s) responsible for managing the system.

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

System Location Setting

```
Switch# configure terminal
Switch(config)# snmp-server location “Wonhyoro-3Ga, Yongsan-gu, Seoul.”
Switch(config)# end
Switch# show running-config
!
snmp-server location “Wonhyoro-3Ga, Yongsan-gu, Seoul.”
!
Switch#
```

ACL (Access Control List)

ACL enables the network manager to control the traffic delivered through the inter-network very closely. The manager can get the basic statistic data on the state of packet transmission and establish a security policy based on the data. In addition, the manager can protect the system from unauthorized accesses. ACL can be used to allow or reject the packets from the router, or can be used to access the router through Telnet (vty) or SNMP.
Access list is classified into the standard IP access list and the extended IP access list, each of which is assigned the numbers of <1-99> and <100-199> respectively.

Table 14. ACL Configuration Command

Command	Description	Mode
access-list <**1-99**> {**deny**|**permit**} *address*	■ Set up the standard IP access list. ■ Set up the source address/network only. ■ *address* ::= {any | A.B.C.D A.B.C.D | host A.B.C.D}	Config
access-list <100-199> {**deny**|**permit**} **ip** *address address*	■ Set up the extended access list for IP protocol. ■ Set up Source address/network and destination address/network.	Config
access-list <100-199> {**deny**|**permit**} {**tcp**|**udp**} *address* [*operator port* [*port*]] address [*operator port* [*port*]]	■ Set up the extended IP access list for TCP/UDP protocol among IP protocols. ■ Enter two port numbers to set the range of ports. ■ *Operator* ::= { lt | gt | eq | neq | range }	Config
no access-list <1-199>	■ Delete an access list.	Config

Rules for Access List Creation

- Declare the access list with smaller range first.
- Declare the access list that satisfies the condition more frequently first.
- If you don't specify 'permit any' at the end of an access-list, 'deny any' is set up as default.
- When you declare the conditions of an access list in many lines, you cannot delete or modify anything between lines, and the condition newly added will be added as the last line.

Configuration of Standard IP Access List

Permit any

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

Deny any

```
Switch# configure terminal
Switch(config)# access-list 1 deny any
```

```
Switch(config)# end
Switch# show running-config
!
access-list 1 deny any
!
```

Permit the Access from a Specific Host Only

```
Switch# configure terminal
Switch(config)# access-list 1 permit host 192.168.0.3
Switch(config)# end
Switch# show running-config
!
access-list 1 permit host 192.168.0.3
!
```

Permit the Access from a Specific Network Only

```
Switch# configure terminal
Switch(config)# access-list 1 permit 192.168.0.0 255.255.255.0
Switch(config)# end
Switch# show running-config
!
access-list 1 permit 192.168.0.0 255.255.255.0
!
```

Deny the Access from a Specific Network Only

```
Switch# configure terminal
Switch(config)# access-list 1 deny 192.168.0.1 255.255.255.0
Switch(config)# access-list 1 permit any
Switch(config)# end
Switch#    show running-config
!
access-list 1 deny 192.168.0.0 255.255.255.0
access-list 1 permit any
!
```

Configuration of Extended IP Access List

Deny the Access from a Specific Network to a Specific Network

```
Switch# configure terminal
Switch(config)# access-list 100 deny ip 192.168.0.0 255.255.255.0 192.168.4.0 255.255.255.0
Switch(config)# access-list 100 permit ip any any
Switch(config)# end
Switch# show running-config
!
access-list 100 deny ip 192.168.0.0 255.255.255.0 192.168.4.0 255.255.255.0
access-list 100 permit ip any any
!
```

Deny the FTP Access from a Specific Network to a Specific Network

```
Switch# configure terminal
Switch(config)# access-list 100 deny tcp 192.168.0.0 255.255.255.0 192.168.4.0
255.255.255.0 eq ftp
Switch(config)# access-list 100 permit ip any any
Switch(config)# end
Switch# show running-config
!
access-list 100 deny tcp 192.168.0.0 255.255.255.0 192.168.4.0 255.255.255.0 eq ftp
access-list 100 permit ip any any
!
```

Permit SNMP Access to a Specific Host Only

```
Switch# configure terminal
Switch(config)# access-list 100 permit udp any host 192.168.10.2 eq snmp
Switch(config)# end
Switch# show running-config
!
access-list 100 permit udp any host 192.168.10.2 eq snmp
!
```

Configuration of Access List for Telnet Connection

Access list is applied by user. The access list can be set to permit/limit from outside.
The commands shown are used to configure access list for Telnet connection.
An access list example allowing 192.168.0.0/24 and limiting the telnet access process is as follow;

```
Switch# configure terminal
Switch(config)# access-list 1 permit 192.168.0.0 255.255.255.0
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 192.168.0.0 255.255.255.0
!
Switch#
```

NTP Setting

NTP Introduction

NTP is the protocol synchronizes the system time. NTP runs above UDP (User Datagram Protocol) and uses Coordinated Universal Time (UTC) which is same as Greenwich Mean Time.

NTP Commands

Command	Description
ntp server *A.B.C.D*	■ Set up NTP server (Up to 8).
ntp poll-interval *<16-16284>*	■ Number of seconds between time requests to a server.
ntp rtc [disable|enable]	■ Set up RTC(Real Time Clock) using ntp.
ntp [disable|enable]	■ Enable or disable the ntp functions of the switch.
show ntp	■ Show the details on NTP.

NTP Setting Example

```
Switch#
Switch# configure terminal
Switch(config)#
Switch(config)# ntp server 10.1.1.1
Switch(config)# ntp server 10.2.3.4
Switch(config)# ntp poll-interval 100
Switch# show ntp
P7000# sh ntp
-----------------------------------------
Current time: Mon Jul 26 04:00:39 2004
-----------------------------------------
Poll interval       : 100
NTP Status    : Active
NTP RTC_SET : Inactive
-----------------------------------------
The list of NTP Server is below.
-----------------------------------------
[1] 10.1.1.1
[2] 10.1.2.3
-----------------------------------------
Switch#
```

Chapter 2. Interface Configuration

This chapter describes the Interface of the system.

P8824XG Interface

The interfaces supported by P8824XG are as in the following table.

Table 15. Interfaces Supported by P8824XG Switch

Interface	Types
Physical Interfaces	10/100/1000 Base-T (Auto Negotiation) Gigabit Ethernet Optic (1000 Base-X)
Port-group Interfaces	Port-group

To configure the interface environment, the following processes shall be performed in advance.

1) Enter the config mode from the privileged mode with “configure terminal” command.

2) Enter the interface mode with “interface” command.

3) Use the configuration commands for a particular interface.

Common Commands

The following table shows the commands for P8824XG switch interface configuration.

Table 16. P8824XG Switch Port Commands

Command	Description
interface *ifname*	Enter the interface mode. *ifname*: The name of the interface to configure.
description *string*	Interface comment *string*: Comment on interface, a string of 80 or less characters

Interface Name

P8824XG uses interface name in all interface configurations. Interface name consists of interface type identifier and interface ID as shown below.

Table 17. Interface Name

Classification	Interface Type	Interface Name	Example
Physical Interface	Gigabit Ethernet	"gi" + port_id	gi1, gi2
Port-group Interface	Port group	"po" + port-group id	po1
VLAN Interface	VLAN	"vlan" + vlan id	vlan10
Loopback Interface	Loopback	"lo" + id	lo0
Management Interface	Fast Ethernet	"eth" + id	eth0

Interface ID

Interface name consists of interface type and id, and each P8824XG switch model has a different naming method for interface ID. The following table shows how to name the interface ID of each model and the supportable range.

Table 18. Interface ID and range

Model	Interface Type	ID Composition	ID Range	Name (Example)
P808	Fast Ethernet	slot id /port id	FE-TX slot id: 1 port id: 1-6	fa1/1, fa1/6
	Gigabit Ethernet	slot id /port id	slot id : 2-3 port id : 1	gi2/1, gi3/1
	Port group	port-group id	1 – 30	po1, po30
	VLAN	vlan id	1 – 4094	vlan1, vlan4094
	Loopback	interface id	0 – 3	lo0, lo3
	management	interface id	0	eth0

VP5208A	Fast Ethernet Gigabit Ethernet Port group VLAN Loopback management	slot id /port id slot id /port id port-group id vlan id - -	port id: 1-8 port id: 1-2 1 – 8 1 – 4092 - -	fa1, fa8 gi1 po1, po8 vlan1, vlan4092 - -
P8124	Fast ethernet Gigabit ethernet Port group VLAN Loopback management	slot id /port id slot id/port id port-group id vlan id interface id interface id	slot id: 2-4 port id: 1-8 slotid: 1 port id: 1-2 1 – 30 1 – 4094 0 – 3 0	gi1 fa4/8 gi1/1, gi1/2 po1, po30 vlan1, vlan4094 lo0, lo3 eth0
P8524	Gigabit ethernet Port group VLAN Loopback management	slot id /port id port-group id vlan id interface id interface id	slot id: 1-3 port id: 1-8 1 – 30 1 – 4094 0 – 3 0	gi1/1 gi3/8 po1, po30 vlan1, vlan4094 lo0, lo3 eth0
P8824	Gigabit ethernet 10Gigabit Ethernet Port group VLAN Loopback management	port id port id port-group id vlan id interface id interface id	port id: 1-24 port id: 25-26 1-30 1 – 4094 0 – 3 0	gi1 gi24 gi25,gi26 po1, po30 vlan1, vlan4094 lo0, lo3 eth0
P8724	Gigabit ethernet Port group VLAN Loopback management	port id port-group id vlan id interface id interface id	port id: 1-24 1-30 1 – 4094 0 – 3 0	gi1 gi24 po1, po30 vlan1, vlan4094 lo0, lo3 eth0

Interface Mode Prompt

When you enter the interface mode with interface command, the following prompt will be displayed on the screen. You can configure and change interface environment in the interface mode.

```
Switch(config)# interface gi1
Switch(config-if-gi1)#
```

Description Command

The description command is used to add description on each interface. The description is the comment used to help the administrator remind of something and you can see the result with “show interfaces” command.

Show Interface Information and Status

The commands below are used to view the interface configuration information, the status information, and the statistic data.

Table 19. Commands Related to Interface Information and Status

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

Show Interfaces Command

This command is used to view the interface configuration information, the link status, and the interface-related statistics. Show interfaces command without any additional parameters shows the information on all the interfaced defined.

```
Switch# show interfaces
gi1 is up
type GBIC,SC
no auto-negotiation
speed set 1G, current 1G
duplex set full, current full

Last clearing of counters 26:03:20
0 seconds input rate 55495 bytes/sec, 53 packets/sec
0 seconds output rate 6006 bytes/sec, 50 packets/sec
   38548078 packets input, 4007497659 bytes
   Received 0 broadcasts, 0 multicasts
   0 CRC, 0 oversize, 0 dropped
   33191196 packets output, 1784705803 bytes
   Sent 7141 broadcasts, 0 multicasts
```

Show Port Status Command

This command is used to show the link, shutdown status, auto negotiation mode, speed/duplex mode, flow control, and interface type of all the physical interfaces.

```
Switch# show port status
--------------------------------------------------------------------------
 ifname   type  shutdown link  nego   set-speed   cur-speed  flow-control
--------------------------------------------------------------------------
 gi1 GE   . up   manual   1G /full    1G /full
 gi2 GE   .down  manual   1G /full .
 gi3 GE   .down  manual  1G /full .
 gi4 GE   .down  manual  1G /full .
```

Notice As for the below examples, See Interface ID <Tabel 18> about other model. The description is based on P8624XG.

Show Switchport Command

Switchport refers to a port or a port-group running in Layer 2 switching mode. Show switchport command shows the switchport information of physical ports and port-groups. Switchport information includes the access mode, the native and tagged vlan list.

```
Switch# show switchport

IFNAME    SWMODE N-VLAN TAGGED-VLAN-LIST
-------------------------------------------
  gi1     access 1
  gi2     access 1
  gi3     access 1
  gi4     access 1
```

Physical Port Configuration

The commands shown in the following table are used to configure a physical port.

Table 20. Physical Port Configuration Command

Command	Description	Mode
shutdown **no shutdown**	Enable/Disable physical port.	Interface
auto-negotiation **no auto-negotiation**	Enable/Disable speed auto-negotiation.	Interface
speed (10|100|1000) **speed auto**	Set speed	Interface
duplex (full-duplex|half-duplex) **duplex auto**	Set duplex mode	interface
flow-control (on|off)	Set/Clear Flow control	Interface

Shutdown

This command is used to disable a physical port. To check the shutdown status of a physical port, use show interface command.

```
Switch# configure terminal
Switch(config)#
Switch(config)# interface gi1
Switch(config-if-gi1)# shutdown <- disable port
Switch(config-if-gi1)# no shutdown    <- enable port
```

Speed and Duplex

The speed of each interface of P8824XG is as follow:

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

For configuring speed, duplex, close attentions to the following are necessary;

- If the interface type is 100Base-FX, there is no speed configuration.
- For 1000Base-X case, speed setting is not necessary but only auto-negotiation ON/OFF setting is available. In case of auto-negotiation ON, link down from both side of optical cable is monitored even though only one side of optical cable is blocked (Remote fault is monitored).
- If both ends of the line support auto-negotiation, we highly recommend the default setting of auto-negotiation.
- If one interface supports auto-negotiation and the other end does not, configure duplex and speed on both interfaces; do not use the auto setting on the supported side.

Broadcast Suppression

Broadcast suppression refers to a function that limits broadcast traffic from flowing in the system in order to prevent the system overload caused by the broadcast storm. A broadcast storm refers to a phenomenon where a broadcast/multicast packet is flooded in the subnet and too much traffic deteriorates the network performance. Errors in protocol stack implementation or in network configuration can cause the broadcast storm.

Broadcast suppression measures the rate of the broadcast traffic on the subnet, compares the value with the threshold, and discards the broadcast traffic over the threshold.

Table 21. Broadcast Suppression Command

Command	Description	Mode
broadcast suppression multicast **no broadcast suppression multicast**	Include Multicast packet in case of suppression Default : No multicast packet	config
broadcast suppression *rate* **no broadcast suppression**	Set up broadcast suppression rate	interface

Port Mirroring

Port mirroring copies all the I/O traffic of a particular port (source port) to the destination port (target port) that the administrator has set and monitors all the packets of any port.

P8824XG monitors RX/TX traffic from different source ports with one port.

Table 22. Port Mirroring Command

Command	Description	Mode
mirroring rx-target *ifname*	Set target port to monitor input packet	config
mirroring tx-target *ifname*	Set target port to monitor output packet	config
mirroring rx-traffic	Set input packet to monitor	interface
mirroring tx-traffic	Set output packet to monitor	interface

Layer 2 Interface Configuration

Layer 2 interface operates in the Layer 2 switching mode (IEEE 802.3 Bridged VLAN). In P8824XG switch, the physical port and the port-group interface operate in this mode.
This chapter describes the Layer 2 interface and the commands to set the physical port and the port-group as Layer 2 interface with the examples.

VLAN Trunking

Trunk refers to the point-to-point link between Ethernet switch and other network equipment (router, switch). Trunk can transmit multiple VLAN traffic to a link and you can extend VLAN to the entire network with trunks.

P8824XG switch supports 802.1Q trunking encapsulation for all Ethernet interfaces and you can set up trunks in the single Ethernet interface or the port-trunk interface

Layer 2 Interface

Layer 2 interface modes supported by P8824XG switch are the trunk mode and the access mode.

Table 23. Layer 2 Interface Modes

Mode	Description
switchport mode access	Non trunking mode. Only the native VLAN is available.
switchport mode trunk	Trunking mode. One native VLAN and many tagged VLANs are available.

Layer 2 Interface Defaults

P8824XG switch has the following default values when a physical port or a port-group is set as Layer 2 interface.

Table 24. Layer 2 Interface Defaults

Items	Defaults
Interface mode	switchport mode access
Native vlan	VLAN 1

Layer 2 Interface Configuration/Cancel

The commands for Layer 2 interface configure/cancel are as follows.

Table 25. Layer 2 Interface Setting/Clear Command

Command	Description	Mode
switchport	Set up Layer 2 interface	interface
no switchport	Set up non-Layer 2 interface	interface

When an interface is set up as the first Layer 2 interface, the interface will have the defaults of Layer 2 interface and when the Layer 2 interface configuration is canceled, VLAN settings are also

canceled. Layer 2 interface clear is used when port-grouping physical port

Notice In the default setting of P8824XG switch, all physical ports are Layer 2 interface.

Trunk Port Setting

The following commands are used to set a physical port or a port-group interface as Layer 2 access port.

Table 26. Commands for Trunk Port Configuration

Command	Description	Mode
switchport mode access	Set up the access mode.	interface
switchport access vlan *<1-4094>*	Set up a native vlan.	interface
no switchport access vlan	Set a native vlan as default (VLAN 1)	interface

Table 27. Trunk Port Configuration Command

Command	Description	Mode
switchport mode trunk	Set up trunk mode	interface
switchport trunk native vlan *<1-4094>*	Set up trunk port native VLAN	interface
no switchport trunk native vlan	Set up trunk port native VLAN as default	interface
switchport trunk add *<2-4094>*	Register trunk port tagged VLAN	interface
switchport trunk remove *<2-4094>* **switchport trunk remove all**	Delete trunk port tagged VLAN	interface

The following is the example of setting a physical port as a Layer 2 access port.

```
Switch# configure terminal
Switch(config)# interface gi1
Switch(config-if-gi1)# switchport layer2 interface set
Switch(config-if-gi1)# switchport mode trunk trunk port set
Switch(config-if-gi1)# switchport trunk native 2 native vlan set
Switch(config-if-gi1)# switchport trunk add 3 tagged vlan register
Switch(config-if-gi1)# switchport trunk add 4
Switch(config-if-gi1)# end
```

The following is the example of setting a port-group interface as a 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 trunk trunk port set
Switch(config-if-po2)# switchport trunk native 2 native VLAN set
Switch(config-if-po2)# switchport trunk add 3 tagged vlan register
Switch(config-if-po2)# switchport trunk add 4
Switch(config-if-po2)# end
```

Access Port Setting

The following is the example of setting a physical port or port-group interface as a Layer 2 access port.

Table 28. Command for Access Port Configuration

Command	Description	Mode
switchport mode access	Set up access mode	interface
switchport access vlan <*1-4094*>	Set up native vlan	interface
no switchport access vlan	Set up native vlan as efault (VLAN 1)	interface

The following is the example of setting a physical port as a Layer 2 access port.

```
Switch# configure terminal
Switch(config)# interface gi1
Switch(config-if-gi1)# switchport layer2 interface set
Switch(config-if-gi1)# switchport mode access access port set
Switch(config-if-gi1)# switchport access vlan 5 native vlan set
```

The following is the example of setting a port-group interface as a 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

Port Group Introduction

Port group is used to bring together many physical ports into a logical group to increase bandwidth and to get the link redundancy. A port group interface in P8824XG switch can be used as Layer 2 interface.

The table below shows the number of port groups available in each P8824XG switch model.

Model	Port Group Count	Max. Ports per Group
P7012G	7	8
P706F	7	8
P8824XG	7	8

Port Group Configuration

The following command is for port group configuration.

Table 29. Command for Port Group Configuration

Command	Description	Mode
port-group *ifname* **protocol none**	Generate static port group	config
port-group *ifname* **protocol lacp**	Generate port group configured with lacp	config
no port-group *ifname*	Delete port-group	config
port-group lb-mode layer3	Refer to ip fileld when load-balance.	config
port-group lb-mode layer4	Refer to tcp/udp port when load-balance	config
port-group *ifname* **no port-group**	Set up port group Delete port group	Interface *
show port-group	Display port group configuration	Privileged

MAC Filtering

MAC Filtering Introduction

MAC filtering is used to block traffic to MAC address, and is set by VLAN.

MAC Filtering Configuration

The following table shows the default command for MAC filtering

Table 30. Command for Layer 3 Interface Configuration

Command	Description	Mode
mac-filter *vlan-id mac-addr mode*	MAC filter add	config
no mac-filter *vlan-id mac-addr*	MAC filter delete	config
show mac-filter	Display MAC filter information	privileged

Chapter 3. VLAN

This chapter describes the VLAN of system.

Virtual LAN (VLAN hereinafter) is the logical group of network users and resources. The users and resources are connected through the ports of the switch. VLAN enables simplified network management that was once time-consuming tasks of network administration, while increasing efficiency in network operations.

This chapter covers the following subjects

- VLAN overview
- VLAN types
- VLAN settings
- Displaying VLAN Settings

VLAN Overview

Definition

VLAN (Virtual LAN) is a advanced LAN technology for devices to communicate as if they were on the same physical LAN regardless of their physical network. Devices that belong to the same VLAN constitute a broadcast domain. VLAN is logically classified by a certain function, organization, or application, prevents traffic from flowing into other VLANs, and transmits traffic only to the same VLAN equipment to improve the network performance and security. That is, with VLAN, LAN segments are not classified by the physical hardware connection but flexibly by the logical groups made by the administrator.

For example, all the workstations and servers used by a particular workgroup can be connected in a same VLAN regardless of their physical network connection. That is, the system administrator can reconfigure a network just through a software configuration without physical movement or arrangement of equipment or cable.

VLAN is used to provide segmentation service, which was provided by routers in the conventional LAN configuration. VLAN provides scalability, security, and network management. In VLAN configuration, a router provides broadcast filtering, security, short address, and traffic flow control. The switch in the defined group does not deliver any frames including the broadcast frames between two VLANs.

Advantages of VLAN

Implementing VLANs on your networks has the following advantages:

- **Efficient traffic control**

  With traditional networks, network congestion can be caused by broadcast traffic that is transmitted to all network devices, regardless of whether they require it or not. Only the devices in the same VLAN are the members of the same broadcast domain and receive all broadcast packets. Meanwhile, broadcast traffic is not transmitted to the port of the switch in another VLAN. Therefore VLAN prevents broadcast traffic from spreading to other networks and increases network efficiency.

- **Enhanced network security**

  With traditional networks, anybody who accesses the network can access the network resources. That is, if a user accesses to the network analyzer through a hub, he/she can see the network flow. In a VLAN, only the devices in the same VLAN can and the users can no longer access all the network resources just by connection a computer to the switch port. If a device in VLAN *A* wants to communicate with a device in VLAN *B*, the traffic must pass through a routing device.

- **Flexible network and device management**

  System A administrators of a traditional networks spend much of their time in dealing with moves and changes of facilities. For example, if the equipment is moved to other sub-network, the network administrator should update the IP addresses of each terminal manually. However, the network administrator can solve this problem by implementing logical network through VLAN that ensures easy movement of equipment to support flexible network management.

VLAN Types

VLAN can be created according to the following criteria:

- Physical port
- 802.1Q tag
- Combination of the above criteria

Port-Based VLAN (Port-Based VLANs)

In a port-based VLAN, a VLAN name is given to a group of one or more ports on the switch. A switch port can be a member of only one port-based VLAN. The switch port assigned to a port-based VLAN is called the access port. One access port belongs to only one port-based VLAN. Basically, all ports are assigned as the access ports of VLAN 1 (default VLAN).

For example, P8824XG switch assigns 2 ports to each VLAN A and VLAN B, and 4 ports to VLAN C.

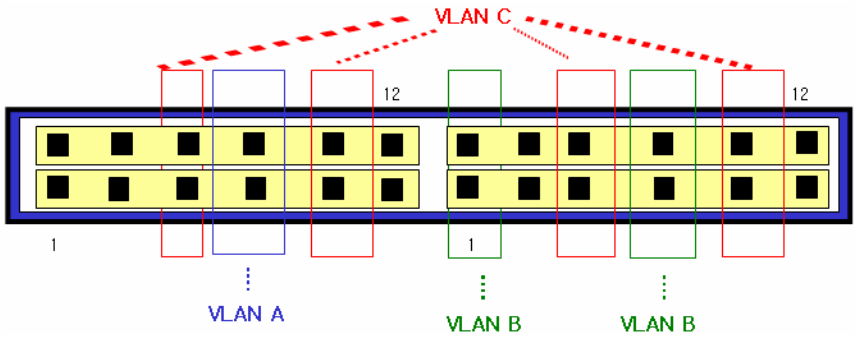


Figure 2. Example of a Port-based VLAN (8000 Switch)

For the members of different VLANs to communicate with one another through they are physically in a same I/O module, the traffic must be routed by the switch. This means each VLAN must be set as a router interface with a unique IP address.

Connecting Switches with a Port-based VLAN

To connect two switches with a port-based VLAN, you have to perform the followings.

1) Assign access ports of each switch to the VLAN.
2) Use one of the access port assigned from each switch to the VLAN to connect the two switches with cable. To connect several VLANs, you have to connect the switches for each VLAN with cable.

The following figure shows how to bind two different P8824XG switches into one VLAN. First, 2 ports of the switch 1 are assigned to VLAN A, and 2 ports of the switch 2 are assigned to a access port of VLAN A. Two switches are connected each other and form single broadcast domain like <Figure 3>.

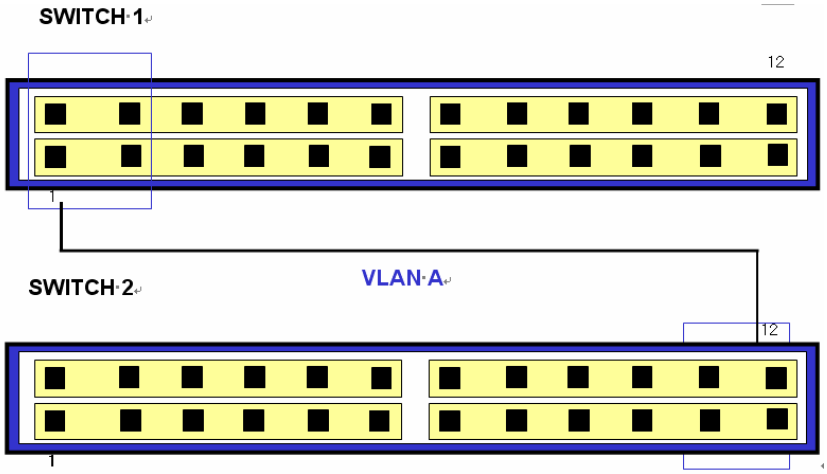


Figure 3. Single Port-based VLANs Connecting 2 Switches

To create multiple VLANs that span two switches in a port-based VLAN, a port on switch 1 must be cabled to a port on switch 2 for each VLAN you want to have span across two switches. At least one port on each switch must be assigned as the access port of the corresponding VLANs, as well. The following figure shows two VLANs spanning two P8824XG switches. Port 1 and 2 in a swtich 1 is an access port of VLAN A, and Port 5, 6, 7 and 8 are assigned as an access port of VLAN B. Port 1 and 2 in a switch 2 are an access port of VLAN A, and Port 9. 10. 11 and 12 are assigned as an access port of VLAN B.

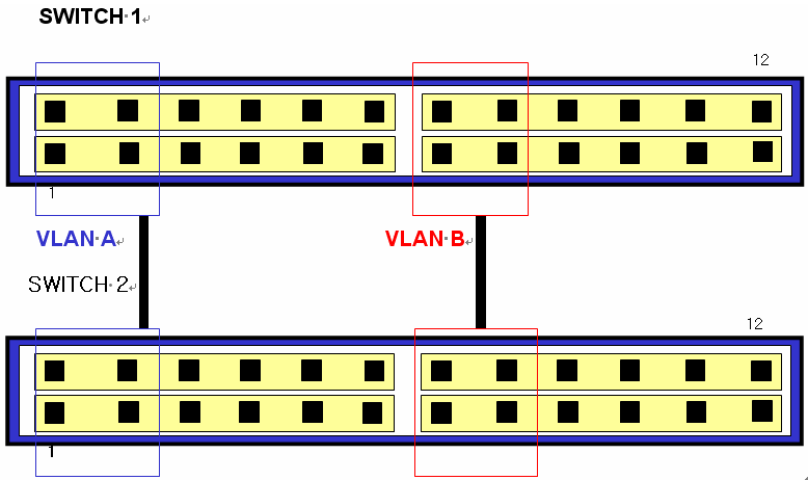


Figure 4. Two Port-based VLANs Connecting 2 Switches

VLAN A binds a switch 1 and switch 2 as connecting a port 2 of a switch 1 and a port 1 of a switch 2. VLAN B binds a switch 1 and switch 2 as connecting a port 8 of a switch 1 and a port 9 of a switch 2.

With this way of configuration, you can create multiple VLANs that connect many switches in a daisy-chained fashion. Each switch must have a dedicated access port for each VLAN connection and each dedicated access port must be connected to the access port that is a member of its

VLAN on the next switch.

Tagged VLANs

Tagging is the process of inserting markers (called a tag) into the Ethernet frame. The tag contains the identification number of a specific VLAN, called the VLANid.

Notice *With 802.1Q tag frame, you can generate a frame larger than 1,518 bytes, the maximum size of IEEE 802.3/Ethernet frame. However, this large frame can affect the frame error counter of other devices that do not support 802.1Q and can cause network connection problems, if there are any bridge and router that do not support 802.1Q on the path.*

Uses of Tagged VLANs

Tag is the most common way to generate a VLAN binding many switches. A point-to-point link connecting two switches or a switch and a router is called trunk. A trunk can transmit many VLANs traffic and extends VLANs from one switch to another switch. The port that is a member of a tagged VLAN and that sends and receives tagged frames is called trunk port. Using tags, several VLANs can send and receive frames by using one or more trunks.

As <Figure 4> describes, in a port-based VLAN, a pair of ports must be assigned in each VLAN to connect two switches. But in a tagged VLAN, multiple VLANs connecting two switches can be generated with a single trunk.

Another advantage of a tagged VLAN is that a port can be a member of multiple VLANs. A tagged VLAN is particularly useful for the network equipment (such as a server) that must belong to multiple VLANs. In this case, the network equipment must be equipped with a network interface card (NIC) that supports 802.1Q tagging.

Assigning a VLAN Tag

Each VLAN may be assigned VLANid when generated. When a port is assigned and used as a trunk port of a tagged VLAN, the port uses a frame with 802.1Q VLAN tag. In this case, the VLANid of the tagged VLAN is used as the frame tag.

Not all ports of VLAN must be tagged. When the traffic from a port is forwarded out of a switch, the switch determines whether each destination port of the frame should use tagged or untagged frame formats for that VLAN. The switch adds or deletes tags, as required, based on the port configuration for that VLAN.

Notice *When a frame with VLAN tag is sent to a port with no VLAN configured, the frame is discarded. For example, if a frame whose VLANid is 30 is sent to a port that is a member of VLANs whose ids are 10 and 20, the switch discards the frame..*

The following figure shows the physical configuration of a network using tagged frames and untagged frames.

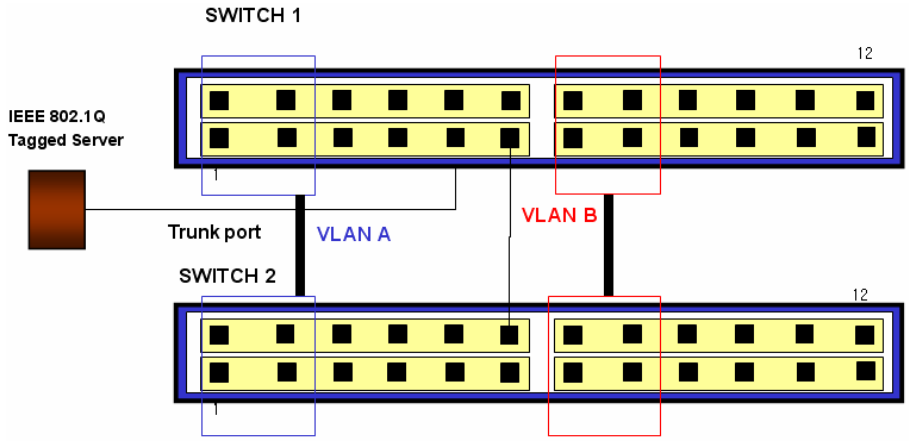


Figure 5. Physical Diagram of Tagged and Untagged frame

The following figure shows the logical diagram of the same network.

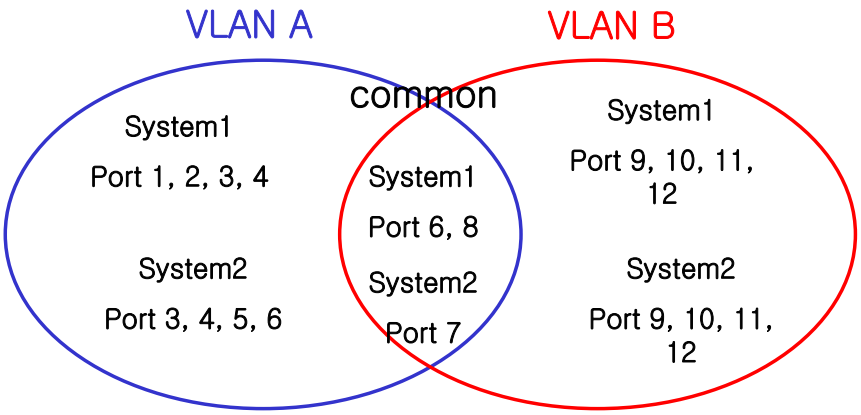


Figure 6. Logical Diagram of Tagged Frame and Untagged frame

- The trunk port (tagged port) of each switch transmits the traffic for both VLAN A and VLAN B.
- The trunk port of each switch is tagged.
- The server connected to port 6 of System 1 is equipped with the NIC that supports 802.1Q tagging
- All other terminals send and receive untagged frames.

When a frame passes through a switch, the switch decides whether to use tagged frames or untagged frames for the destination port. All the frames from/to the server/the trunk port are tagged, but the frames from/to other devices of the network are not untagged.

Mixing Port-based VLAN and Tagged VLAN

You can use both a port-based VLAN and a tagged VLAN in one switch. Under the condition that there is only one port-based VLAN that a port belongs to, a port can be a member of many VLANs. That is, a port can be a member of one port-based VLAN and many tagged VLANs at the same time.

VLAN Names

VLAN ID

You can use a number between 1 and 4094 as VLANid, the identifier of VLAN. When a switch is initialized, a VLAN 1 is generated as default VLAN. Therefore, newly generated VLANs cannot use 1 as their VLANid.

VLANid is used as the tag that the port belonging to the tagged VLAN attaches to a frame when it operates in the trunk mode. If you set a wrong VLANid, frames may be sent to a wrong VLAN, so you have to consider the entire network configuration to set the VLANid.

Default VLAN

Each switch has a default VLAN with the following characteristics.

- Default VLAN uses 1 as VLANid.
- It contains all the interface ports on a new or initialized switch.
- Default VLAN does not use any tags.
- All the ports in the switch initialization status have native VLAN as the default VLAN.

Native VLAN

Each physical port has Port VLAN ID (PVID). In all 802.1Q ports, the ports' native VLAN IDs are assigned as PVID. All the untagged frames are sent to the VLAN that the PVID indicates. When a tagged frame is sent to a port, the tag is used as it is. However, if an untagged frame is sent to a port, the PVID in the frame is regarded as a tag.

As shown in the following figure, since untagged frames and frames with PVID can co-exist in the network, the bridges or end station supporting VLAN can be connected with the bridges or end station not supporting VLAN through cable.

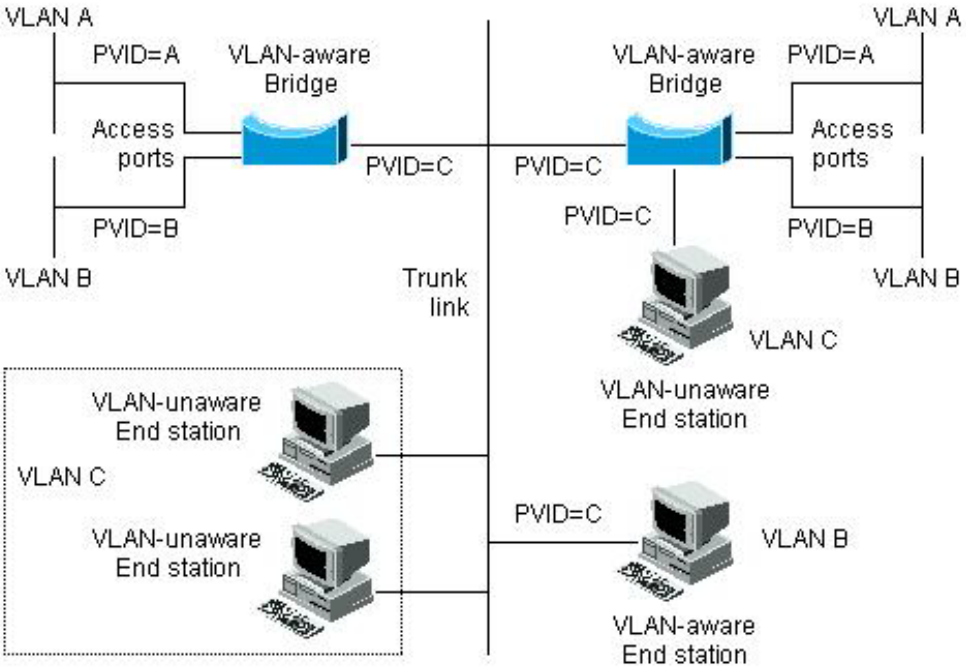


Figure 7. Native VLAN

For example, assume that two end stations not supporting VLAN are connected through the trunk link as shown in the left bottom of <Figure 7>. The two end stations cannot be aware of VLAN, but since the PVID of the bridge that recognizes VLAN is configured as VLAN C, they are included in VLAN C. The end stations that cannot be aware of VLAN transmit only untagged frames, and when a bridge that recognizes VLAN receives these untagged frames, it sends them to VLAN C.

Configuring VLAN on the Switch

This section describes the commands used for VLAN configuration on P8824XG switch. VLAN configuration has the following steps.

3) Create and name the VLAN.
4) Set the mode of the port according to the type of the VLAN where the port will be assigned
5) Assign one or more ports to the VLAN. When you add each port to the VLAN, decide whether to use 802.1Q tags or not.

Commands for VLAN configuration

The following table lists the commands used for VLAN configuration.

Table 31. Commands for VLAN Configuration

Command	Description	Mode
vlan *vlanid*	■ Create, delete, and change VLAN-related values. ■ Default VLAN (VLANid=1) name cannot be changed. ■ *vlanid* – The unique VLAN identifier, a number between 2-4094	config
switchport mode {access|trunk}	■ Set the type of the VLAN where the port will belong. ■ access – Set the port as an access mode. That is, the port is an access port of a port-based VLAN and it works as an interface of a single VLAN that sends and receives untagged frames. ■ trunk – Set the port as a trunk mode. The port is a trunk port of a tagged VLAN and it sends and receives tagged frames.	Interface
switchport access vlan *vlanid*	■ Set the port as VLAN access port. When the mode is set as the access, the port works as a member of the VLAN. ■ A port can be an access port of only one VLAN. ■ *vlanid* – VLANid, a number between 1 and 7000	Interface
switchport trunk add *vlanid*	■ Set the port as the VLAN trunk port. ■ To set the port as the trunk ports of many VLANs, execute this command repeatedly for each VLAN. ■ *vlanid* – VLANid, a number between 2 and 4094 ■ Default VLAN (VLANid=1) name cannot be changed.	Interface
switchport trunk native *vlanid*	■ If the port is 802.1Q trunk mode, that is, a trunk port of a tagged VLAN, set a native LAN for the untagged traffic that is sent and received.	Interface

	■ If you don't set a native VLAN, the default VLAN (VLANid = 1) is set as the native VLAN. ■ *vlanid* : a number between 1 and 4094	
switchport trunk remove {*vlanid*|all}	■ Exclude the port from the members of the specified VLAN. ■ *vlanid* : a number between 2 and 4094. ■ all : Exclude from all VLAN members.	Interface

Examples of VLAN Configuration

The following example shows how to configure a port-based VLAN marketing whose VLAN id is 1000, assign the IP address 132.15.121.1 to VLAN, and assign port gi5 and gi6 to VLAN as access port.

```
Switch(config)# vlan 1000
Switch(config)# interface vlan1000
Switch(config-int-vlan)# ip address 132.15.121.1  255.255.255.0
Switch(config-int-vlan)# interface  gi5
Switch(config-int-gi5)# switchport  mode  access
Switch(config-int-gi5)# switchport  access  vlan  1000
Switch(config-int-gi5)# interface  gi6
Switch(config-int-gi6)# switchport  mode  access
Switch(config-int-gi6)# switchport  access  vlan  1000
```

The following example shows how to configure a port as VLAN trunk port. The example creates VLAN 2000 and configures port gi7 and gi8 as the trunk port of VLAN 2000.

```
Switch(config)# vlan  2000
Switch(config)# interface  gi7
Switch(config-int-gi7)# switchport  mode  trunk
Switch(config-int-gi7)# switchport  trunk  add  2000
Switch(config-int-gi7)# interface  gi8
Switch(config-int-gi8)# switchport  mode  trunk
Switch(config-int-gi8)# switchport  trunk  add  2000
```

The following example shown in the following figure creates the sales VLAN whose VLAN id is 120. VLAN includes both tagged port (trunk port) and untagged port (access port). Port gi1and gi2 have tags, and port gi3 and gi4 are untagged. If not explicitly set, ports are configured as untagged.

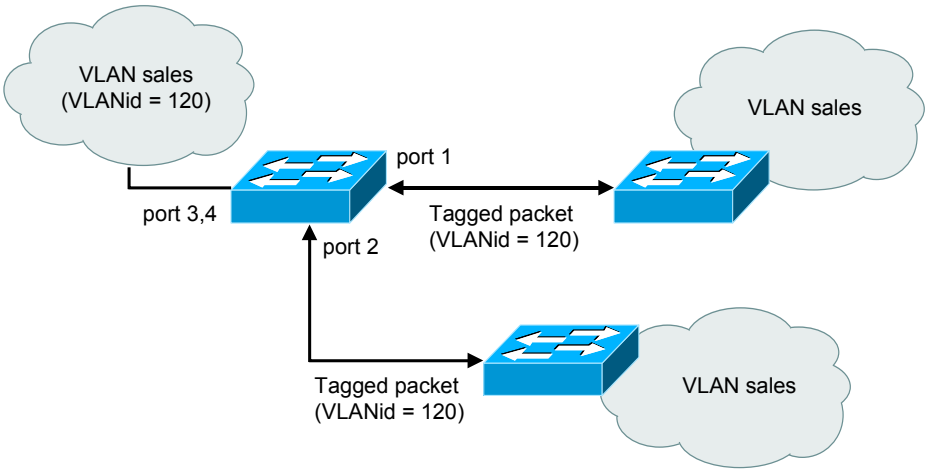


Figure 8. VLAN Configuration Example – Tagged and Untagged VLAN

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

```
Switch(config)# interface gi1
Switch(config-int-gi1)# switchport mode trunk
Switch(config-int-gi1)# switchport trunk add 120
Switch(config-int-gi1)# interface gi2
Switch(config-int-gi2)# switchport mode trunk
Switch(config-int-gi2)# switchport trunk add 120
Switch(config-int-gi2)# interface gi3
Switch(config-int-gi3)# switchport access vlan 120
Switch(config-int-gi3)# interface gi4
Switch(config-int-gi4)# switchport access vlan 120
```

The following example shows how to configure port gi1 as a member of the port-based VLAN Marketing and the tagged VLAN Engineering. VLAN Marketing VLAN ID is 200, and VLAN Engineering VLAN ID is 400.

```
Switch(config)# vlan 200
Switch(config)# vlan 400
Switch(config-vlan)# exit
Switch(config)# interface gi1
Switch(config-int-gi1)# switchport mode trunk
Switch(config-int-gi1)# switchport trunk native 200
Switch(config-int-gi1)# switchport trunk add 400
```

When port gi1 receives untagged frames, the switch sends the frames to the member port of VLAN marketing.

Displaying VLAN Settings

The following command is used to display VLAN configuration information.

Command	Description	Mode
show vlans	■ Display VLAN information summary. • VLANid • Member port	Privileged

```
Switch# show vlans
VLAN MEMBER-LIST
--------------------------------------------------------------------------------
   1 gi8 gi9 gi10 gi11 gi12
   2 gi1 gi2
  11 gi3 gi4 gi5 gi6 gi7


--------------------------------------------------------------------------------
Switch#
```

802.1QinQ

QinQ is basically prohibited to be used in 802.1Q network because 802.1Q provides only 4094 VLAN ID's. In order to resolve this problem so that QinQ can be used, the system has inserted 802.1 QinQ layer between the two 1Q layers. 802.1QinQ is consisted of two VLAN IDs of service providing VLAN ID and service receptive VLAN ID. The service receptive VLAN ID is the VLAN ID which the traffic originally designates. And the service providing VLAN ID is the additive VLAN ID for service providers.
When Q-in-Q is used, first of all you need to make the decision to apply QinQ to the whole network system. For this purpose, 4 bytes will be added to the user port traffic.

1) Service Provider Ethertype: Set up ethertype of an outer tag (default value: 0x8100).
2) Service Provider VLAN ID: Use the native VLAN ID value of customer port for outer tag VLAN ID.
3) Port mode: When Q in Q is applied, each port has to be set to one of the options. Port mode can add an outer tag to user port and the outer tag shall be removed from the port which provides service.

Table 32. 802.1QinQ Command Set

Command	Description	Mode
(no) encapsulation q-in-q	Set QinQ to be enable / disable	Config
(no) q-in-q tunneling ethertype VALUE	Set the ether type of outer tag. While ether type is not configured, the default value is to be 0x8100.	Config
encapsulation q-in-q (default|customer|core)	Set the port mode. default: 0x8100. core : add outer tag as an ethertype customer : configure user port type	Interface

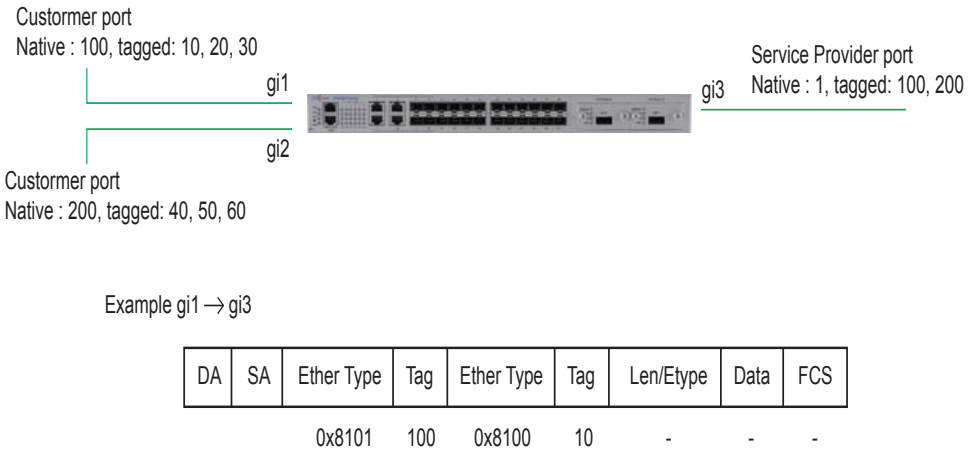


Figure 9. Configuring 802.1 QinQ

```
Switch# configure terminal
Switch(config)# vlan 10,20,30,40,50,60,100,200
Switch(config)# interface gi1
Switch(config-if-gi1)# switchport access vlan 100
Switch(config-if-gi1)# interface gi2
Switch(config-if-gi2)# switchport access vlan 200
Switch(config-if-gi2)# int gi1
Switch(config-if-gi1)# switchport mode trunk
Switch(config-if-gi1)# switchport trunk add 10,20,30
Switch(config-if-gi1)# int gi2
Switch(config-if-gi2)# switchport mode trunk
Switch(config-if-gi2)# switchport trunk add 40,50,60
Switch(config-if-gi2)# int gi3
Switch(config-if-gi3)# switchport mode trunk
Switch(config-if-gi3)# switchport trunk add 100,200
Switch(config-if-gi3)# end

Switch# show switchport
U : untagged packet drop
--------------------------------------------------------------------------
 IFNAME     SWMODE N-VLAN TAGGED-VLAN-LIST
--------------------------------------------------------------------------
 gi1       trunk100      10     20     30
 gi2       trunk200      40     50     60
 gi3       trunk   1     100    200
.
--------------------------------------------------------------------------
total 12 interfaces listed

Switch# configure terminal
Switch(config)# encapsulation q-in-q
```

```
Switch(config)# interface gi1
Switch(config-if-gi1)# encapsulation q-in-q customer
Switch(config-if-gi1)# interface gi2
Switch(config-if-gi2)# encapsulation q-in-q customer
Switch(config-if-gi2)# interface gi3
Switch(config-if-gi3)# encapsulation q-in-q core (in case ethertype changed, or encapsulation q-in-q default)
Switch(config)# q-in-q tunneling ethertype 0x8101
Switch(config)#
```

Private Edge VLAN

Private edge VLAN is the ports exsiting in a segment, in other words within the VLAN, but they cancommunicate only between allowed ports, while the communications between other ports are blocked on Layer 2. In other words, it is to make vlan inside the vlan. So the location in the switch is important in the Private Edge VLAN. Another important thing is the independence between two ports that are being protected between different switches. The protected ports do not generate any traffic (unicast, multicast, broadcast) to other ports, and other ports in the same switch also do not generate any traffic to the protected ports.

Traffic can't be send to the ports protected on L2, and all the traffics can be communicated between the protected ports only through L3 equipment.

Two methods to set the uplink between private edge VLANs in P8824XG:

- IFNAME

Specify the uplink using the port name (ex. gi1, gi2, po1…)

- VLANID

In the network in which STP/RSTP is used, an uplink of root port for the STP and RSTP need to be set. In this case, the uplink can be changed.

Table 33. Private Edge VLAN Setting table

Command	Description	Mode
(no) private-edge-vlan	Enable/disable Private-edge-vlan.	Config
(no) private-edge-vlan *IFNAME*	Enter the IFNAME to set as uplink of the private edge vlan to specific Interface.	Interface
(no) private-edge-vlan stp-root-port *VLANID*	Set the uplink of the private edge vlan as root port of VLANID의 root at specific interface.	Interface
Show private-edge-vlan	Retreive Private-edge-vlan settings.	Privileged

[Example 1]

The ports to be protected are gi2 and gi3, and uplink is gi1. The traffics between the protected ports are now allowed, but only the traffic of gi1 is allowed.

```
Switch# configure terminal
Switch(config)# private-edge-vlan
Switch(config)# interface gi2
Switch(config-if-gi2)# private-edge-vlan gi1
Switch(config-if-gi2)# interface gi3
Switch(config-if-gi3)# private-edge-vlan gi1
```

[Example 2]

The ports to be protected are g1, po1, and po2. For uplink setup in the STP, same VLAN1 is used. In this case, the root port of VLAN1 in the STP is "po2". If src/dest private-edge-vlan port is same, they are marked with "*", and only the changed port of the STP is stored.

```
Switch# configure terminal
Switch(config)# int po1
Switch(config-if-po1)# private-edge-vlan stp-root-port 1
Switch(config-if-po1)# int po2
Switch(config-if-po2)# private-edge-vlan stp-root-port 1
Switch(config-if-po2)# int gi1
Switch(config-if-gi1)# private-edge-vlan stp-root-port 1
Switch(config-if-gi1)# end

Switch# show private-edge-vlan
Private Edge Vlan Mode : enabled
Static Private Edge Vlans: none
STP-ROOT-PORT Private Edge Vlans
  Target Switch Port: STP Root of vlan 1: po2
Members: gi1 po1 *po2
  -(*): Temp Member
```

Abnormal MAC Drop

Use the following commands to drop the packets with abnormal MAC address or trap to the CPU.

Table 34. Abnormal MAC Drop commands

Command	Description	Mode
(no) broadcast-source-mac-drop	Enable/disable to drop the packets with broadcast MAC address as Source MAC address.	Interface
(no) gw-source-mac-drop	Enable/disable to drop the packets with own MAC address as Source MAC address.	Interface
(no) null-source-mac-drop	Enable/disable to drop the packets with all ‘0’ MAC address as Source MAC address.	Interface
(no) self-dest-mac-trapcpu	Enable/Disable to trap to the CPU the packets with own MAC address as Destination MAC address.	Interface

Chapter 4. IP Configuration

This chapter explains how to set IP address.

The basic work required for IP configuration is to assign IP address to the network interface. With IP address assigned, the interface is activated and P8824XG switch assign IP to the following interfaces.

- VLAN interface
- Loopback interface
- Management interface

Assigning an IP address

IP address identifies the network where the received IP datagram is sent. Some IP addresses are reserved for some special purpose and they cannot be used for host, subnet, or network address. The following table lists the range of IP addresses and it shows which addresses are reserved and which addresses are available.

Table 35. Available IP Address

Class	Address Range	Status
A	0.0.0.0 1.0.0.0 ~ 126.0.0.0 127.0.0.0	Reserved Available Reserved
B	128.0.0.0 ~ 191.254.0.0 191.255.0.0	Available Reserved
C	192.0.0.0 192.0.1.0 ~ 223.255.254 224.255.255.0	Reserved Available Reserved
D	224.0.0.0 ~ 239.255.255.255	Multicast group address
E	240.0.0.0 ~ 255.255.255.254 255.255.255.255	Reserved Broadcast

Notice *For the official technology information on IP address, see RFC1166 and Internet Number.*

Notice *To get a network number, please contact your Internet Service Provider (ISP).*

P8824XG switch supports multiple IP addresses per interface. You can specify an unlimited number of secondary addresses. Secondary IP addresses can be used in a variety of situations. The following are the most common applications:

- There might not be enough host addresses for a particular network segment. For example, suppose your subnetting allows up to 254 hosts per logical subnet, but on one physical subnet you must have 300 host addresses. Using secondary IP addresses on the routers or access servers allows you to have two logical subnets using one physical subnet.
- Many older networks were built using Level 2 bridges, and were not subnetted. The judicious use of secondary addresses can aid in the transition to a subnetted, router-based network. Routers on an older, bridged segment can easily be made aware that many subnets are on that segment.
- Two subnets of a single network might otherwise be separated by another network. You can create a single network from subnets that are physically separated by another network by using a secondary address. In these instances, the first network is extended, or layered on top of the second network. Note that a subnet cannot appear on more than one active interface of the router at a time.

The following command is used to assign many IP addresses to a network interface in the interface configuration mode.

Table 36. Command for IP Address Setting

Command	Description
ip address *ipaddress/prefixlen*	■ Assign multiple IP addresses to a interface.

Notice Prefixlen is bit length to divide network among IP addresses.

ARP (Address Resolution Protocol)

The following commands shown in the following table are used to configuration ARP table and ARP table entries.

Table 37. Commands for ARP Table Configuration

Command	Description
show arp	■ Display the entries of ARP table.
arp *ip-address mac- address vlan-name port-name*	■ Set Static ARP to ARP table. ■ IP-address: IP address of ARP entry ■ Mac-address : 48 bit Ehter address of ARP entry ■ VLAN-name : Name of IP interface of ARP destination ■ Port-name: Physical Port Name of ARP destination among IP Interface (: VLAN) member ports

Configuration of Static Routes

The static route is the route defined by the user to send the packets along the specified path from the source to the destination. If the routing protocol cannot be used to configure the route to a destination, the static route is very important. It is also useful to indicate the gateway where the packets that cannot be routed will be sent.
The following command is used to set a static route in the Config mode

Table 38. Commands for Static Route Configuration

Command	Description
ip route {*destination-prefix mask* | *destination-ipaddress/mask*} {*gateway-ipaddress* | **null**} [*distance-value*]	■ Register a static route. ■ Destination-prefix : Specify the network number of the destination-prefix destination. ■ Mask : Specify the mask of the mask destination network. ■ Gateway-IP Address : Specify the IP address of the gateway device. ■ Null : Set the null interface as a gateway. ■ Distance-value : Use a number between 1 and 255

A system remembers the static route until it is deleted (Use no format of IP route command in the Config mode). However, the static route can be overlapped with dynamic routing information by carefully assigning the administrative distance value. Each dynamic routing protocol has the default administrative distance value as listed in the following table. If you want a static route is overlapped with the dynamic routing protocol information, set the administrative distance of the static route to be larger than the dynamic protocol value.

Table 39. Default Administrative Distances of Dynamic Routing Protocol

Item	Defaults
Route Source	Default Distance
Connected interface	0
Static route	1
Exterior Border Gateway Protocol (BGP)	20
OSPF	110
RIP	120
Interior BGP	200
Unknown	255

When an interface is disconnected, all the static routes passing through the interface are deleted from the IP routing table. When no more hop is available for forwarding router address in a static route, the static route is deleted from IP routing table.
To display the static route information, use the following command in the privileged mode.

Command	Description
show ip route static	■ Display IP route information.

IP Configuration Examples

This chapter provides the examples of IP address configuration:

- Assign IP address to network interface
- Creating a Network from Separated Subnets Examples
- ARP
- Static Route

The following example is to assign C class IP address 192.10.25.1 to VLAN 5 Interface of the switch.

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

In the following example, Subnet 1 and 2 of 131.108.0.0 network are separated by the backbone network. Two networks are configured as a logical network.

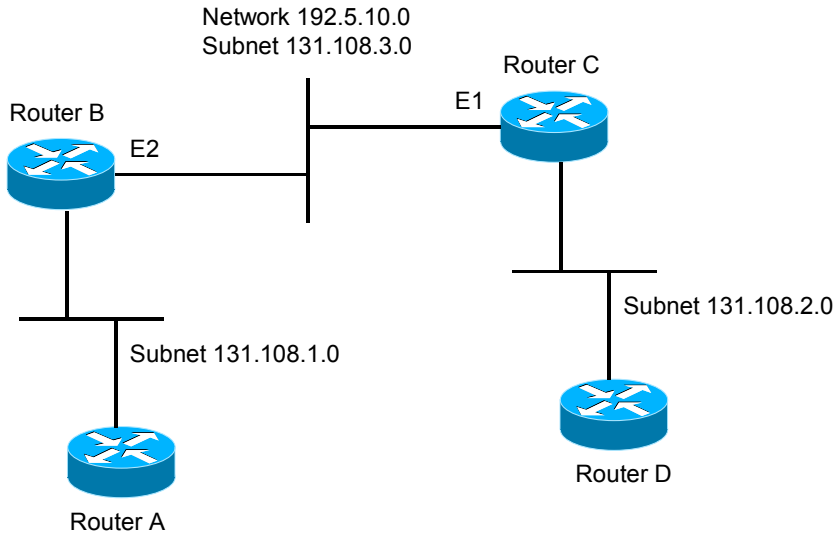


Figure 10. Example Network for IP Configuration – Secondary IP Configuration

Router B Configuratin

Switch(config)# **interface vlan2**
Switch(config-int-vlan2)# **ip address** *192.5.10.1/24*
Switch(config-int-vlan2)# **ip address** *131.108.3.1/24*

Router C Configuratin

Switch(config)# **interface vlan2**
Switch(config-int-vlan2)# **ip address** *192.5.10.2/240*
Switch(config-int-vlan2)# **ip address** *131.108.3.2/24*

The following example shows how to display an entry from ARP table.

Switch# **show arp**

```
----------------------------------------------------------------
 IP Address MAC AddressIPF   PORTRefCnt   Flags
----------------------------------------------------------------
 10.1.2.254 0007.7089.1123   vlan2      gi3      1   S
 10.1.11.46 0006.2bfc.146e   vlan11     gi6      1   S
 10.1.13.1   0001.0281.f775   vlan13     gi1      1   R
 10.1.13.1900000.f083.f6d4   vlan13     gi7      1   K
```

The following command is to register Static ARP entry to ARP table.

Switch(config)# **arp** *142.10.52.196 0010.073c.0514 vlan1 gi2*
Switch# **show arp**

```
----------------------------------------------------------------
 IP Address MAC AddressIPF PORTRefCnt   Flags
----------------------------------------------------------------
 142.10.52.196     0010.073c.0514 vlan1      gi2      1   P
```

The following command is used to delete all the ARP entries of ARP table.

Switch(config)# **no arp** *142.10.52.196*

In the following example, a static route is set so that the host connected to 20.1.1.0 network can communicate with the host of 192.168.2.0 network.

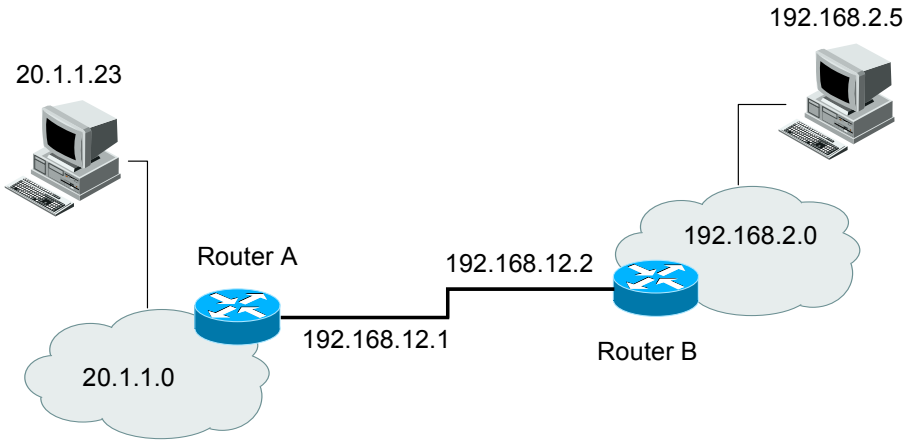


Figure 11. Example Network for IP configuration – Static route

Router A configuration

Switch(config)# **ip route** *192.168.2.0 255.255.255.0* 192.168.12.2
Switch(config)# **show ip route static**
Codes: C - connected, S - static, R - RIP, O - OSPF,
B - BGP, > - selected route, * - FIB route
S>* 192.168.2.0/24 [1/0] via 192.168.12.2 vlan2
Switch(config)#

Router B configuration

Switch(config)# **ip route** *20.1.1.0/8* 192.168.12.1
Switch(config)# **show ip route static**
Codes: C - connected, S - static, R - RIP, O - OSPF,
B - BGP, > - selected route, * - FIB route
S 20.1.1.0/8 [1/0] via 192.168.12.1 vlan2
Switch(config)#

Chapter 5. DHCP

This chapter describes the DHCP configuration of system.

DHCP Configuration

Overview of DHCP Server Functions

Dynamic Host Configuration Protocol (DHCP) assigns reusable IP addresses and configuration parameters to other IP hosts (DHCP clients) in IP network. DHCP is designed for the configuration of large-scale network and complex TCP/IP software in which reduces the workload on the IP network administrator. The most important configuration information that a client receives from the server is the IP address of the client.

DHCP is an extension of BOOTP, but there are two big differences between DHCP and BOOTP.

- DHCP sets a client to be assigned IP addresses for a limited time span so that the IP addresses can be reassigned to other clients.
- DHCP provides the method for a client to set additional IP configuration parameters required to work in a TCP/IP network.

DHCP server provides the DHCP server functions, assigning IP addresses from the address pool in the switch to a client and managing the addresses. If DHCP cannot satisfy DHCP requests in its database, it may send the requests to one or more assistant DHCP servers that the administrator has configured.

IP Address Allocation Mechanism of DHCP Server

DHCP supports three mechanisms for IP address allocation

- Automatic allocation – DHCP allocates a permanent IP address to the client
- Manual allocation – The network administrator assigns an IP address to a client and DHCP is used simply to convey the assigned address to the client..
- Dynamic allocation – DHCP assigns an IP address to a client for a limited period of time.

The available configuration parameters are listed in RFC 2131 and some main parameters are as follows.

- Subnet mask
- Router
- Domain
- Domain Name Server (DNS)

P8824XG Switch as a DHCP Server

The following figure shows the basic steps that occur when a DHCP client requests an IP address from a DHCP server (P8824XG switch).

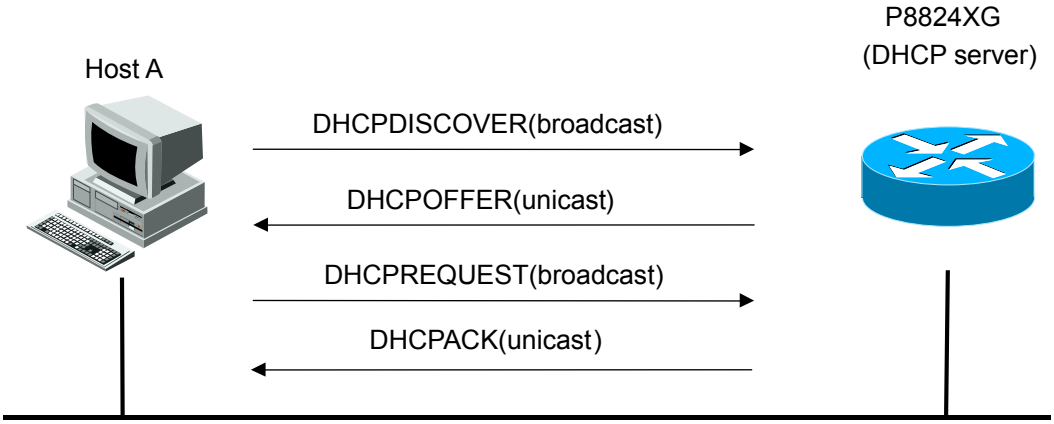


Figure 12. P8824XG Switch as a DHCP Server

1) The client host A sends broadcast message *DHCPDISCOVER* to DHCP server.
2) DHCP server sends the configuration parameters including IP address, a domain name, and a lease for the IP address, to the client by using the unicast message *DHCPOFFER*.

Notice *A DHCP client may receive offers from multiple DHCP servers and can accept any one of the offers; however, the client usually accepts the first offer it receives. Additionally, the offer from the DHCP server is not a guarantee that the IP address will be allocated to the client; however, the server usually reserves the address until the client has had a chance to formally request the address..*

3) The client sends the formal request for the supplied IP address to DHCP server by using the broadcast message *DHCPREQUEST*.
4) DHCP server verifies that the IP address is assigned to the client by sending the unicast message *DHCPACK* to the client.

Notice *The formal request for the offered IP address (the DHCPREQUEST message) that is sent by the client is broadcast so that all other DHCP servers that received the DHCPDISCOVER broadcast message from the client can reclaim the IP addresses that they offered to the client.*

P8824XG Switch as DHCP Relay Agent

The following figure shows the procedure where DHCP server as DHCP relay agent transfers the request message of DHCP client to DHCP server of other networks

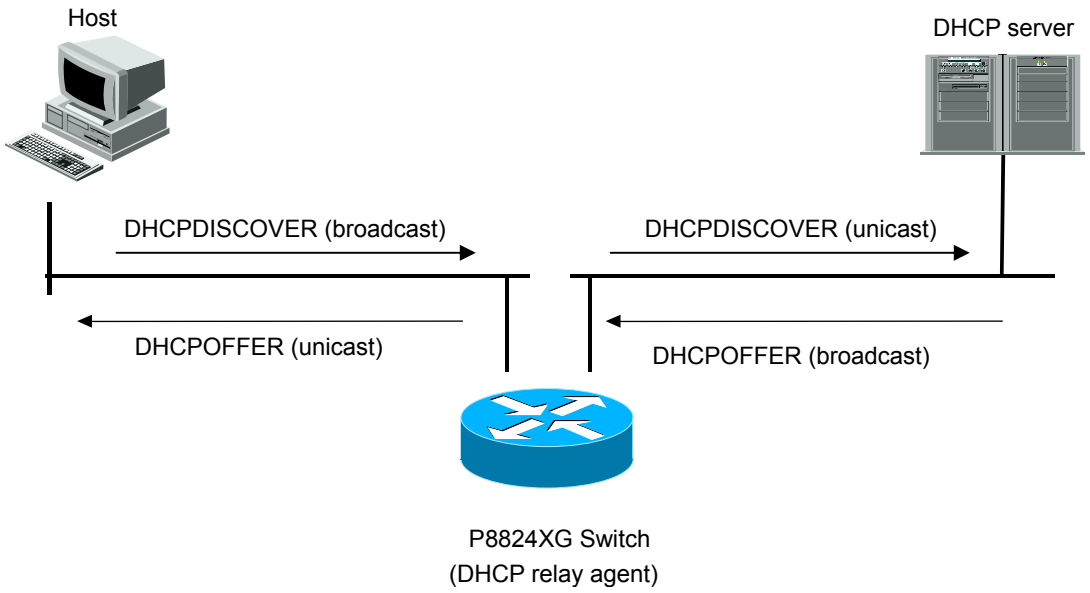


Figure 13. P8824XG Switch as a DHCP Relay Agent

DHCP client sends the broadcast message *DHCPDISCOVER*.

1) If DHCP server cannot satisfy the request of the client, the server uses the unicast message *DHCPDISCOVER* to transfer the request to the DHCP server that the administrator has configured.

2) When the DHCP server receives a message from the DHCP relay agent (P8824XG switch), it sends the information on IP address to the client, and default router to the DHCP relay agent by using the unicast message *DHCPOFFER*.

3) The DHCP relay agent sends the *DHCPOFFER* message to the client.

4) *DHCPREQUEST* and *DHCPACK* messages are transferred by the DHCP relay agent in a same manner between the DHCP server and the client.

Advantages of DHCP Server

DHCP server features bring the following advantages.

- **Reduced Internet access cost** – Using automatic IP address assignment at each remote site substantially reduces Internet access costs. Static IP addresses are considerably more expensive to purchase than are automatically allocated IP addresses.

- **Reduced client configuration tasks and costs** – Since DHCP is easy to configure, you can minimize the costs related to equipment configuration and unprofessional users can also use DHCP with ease.

- **Centralized management** – Because the DHCP server maintains configurations for several subnets, an administrator only needs to update a single, central server when configuration parameters change.

DHCP Address Pool Setting

You can configure a DHCP address pool with a name that is a symbolic string (such as "ubiquoss") or an integer (such as 0). For DHCP address pool setting, change the current mode into the DHCP pool configuration mode where you can set the parameters such as IP subnet number and default router. To set a DHCP address pool, you have to finish the required tasks in the following section. DHCP server provides network pool and host pool.

- **Network Pool**– Configure pool for automatic or dynamic allocation. Different subnets can share IP pool if different network pools are configured into one group.
- **Host Pool** – Configure pool for manual allocation, many hosts with common information can be set into one host pool.

DHCP Address Pool Setting

You can configure a DHCP address pool with a name that is a symbolic string (such as "ubiquoss") or an integer (such as 0). For DHCP address pool setting, change the current mode into the DHCP pool configuration mode where you can set the parameters such as IP subnet number and default router. To set a DHCP address pool, you have to finish the required tasks in the following section.

Notice Different network pool can be configured into one group and different subnets of one VLAN should be in the same group.

Setting DHCP Network Pool Name and Entering DHCP Configuration Mode

To configure the DHCP network pool name and enter DHCP pool configuration mode, use the following command in Global mode

Command	Description
ip dhcp network-pool *name*	■ Generate a name for DHCP address pool ■ Enter the DHCP network pool configuration mode identified as “config-dhcp#” prompt.

Configuration of DHCP Server Boot File

A boot file is used to store the boot image for a client. The boot image is generally the operating system that the client uses to load. The following command is used to specify the boot file for a DHCP client in the DHCP pool configuration mode.

Command	Description
bootfile *filename*	■ Specify the name of the file to be used as a boot image.

Setting Default Router for Client

After the DHCP client is booted, the client sends packets to its default router. The IP address of the default router must be on the same sub network as the client. The following command is used to set the default router for DHCP client in the DHCP pool configuration mode.

Command	Description
default-router *address*	■ Specify the IP address of the default router for DHCP client.

Setting DNS IP Server for Client

DHCP clients query DNS IP servers when they need to correlate host names to IP addresses. To configure the DNS IP servers that are available to a DHCP client, use the following command in DHCP pool configuration mode:

Command	Description
dns-server *address1 address2 address3*	■ Specify the IP address of the DNS server that the DHCP client can use. ■ One IP address is required. ■ You can specify up to three IP addresses in the command line.

Setting the Domain Name for Client

The domain name of a DHCP client includes the client in the general network group. The following command is used to set the domain name string for a client in DHCP pool configuration mode.

Command	Description
domain-name *domain*	■ Specify the domain name for a client.

Setting Group for Network Pool

Network group includes many DHCP Network Pools and Network Pool in the same group shares the IP Pool.

Command	Description
group *group-name*	■ Specify Group name

Notice In case one VLAN consists of many IP address, network pool for each IP address should be configured with the same group name.

Setting the Address Lease Time

By default, each IP address assigned by a DHCP server comes with an one-hour lease, which is the amount of time that the address is valid. To change the lease value for an IP address, use the following command in DHCP pool configuration mode:

Command	Description
lease {days [hours] [minutes]}	■ Specify the lease period. ■ The default is one hour. ■ Infinite: Use automatic allocation sytstem leasing IP address permanenetly to host.

Setting DHCP Subnet and Network Mask

To configure IP address for the newly created DHCP address pool and server network mask, use the following command in DHCP pool configuration mode

Command	Description
network *network-numberlprefix-length*	■ Specify the sub network number and mask for DHCP address pool.

The following example shows how to set DHCP Subnet and Network mask with 100.0.0.0/24.

```
Switch# configure terminal
Switch(config)# ip dhcp network-pool network_pool1
Switch(config-dhcp)# network 100.0.0.0/24
Switch# show running-config
. . .
!
ip dhcp network-pool network_pool1
network 100.0.0.0/24
!
. . .
```

Setting the NetBios WINS IP Server for Client

Windows Internet Naming Service (WINS) is a name resolution service that Microsoft DHCP clients use to correlate host names to IP addresses within a general grouping of networks. To configure the NetBIOS WINS servers that are available to a Microsoft DHCP client, use the following command in DHCP pool configuration mode:

Command	Description
netbios-name-server *address*	■ Specify the IP address of NetBIOS WINS server that Microsoft DHCP client can use.

Setting NetBIOS Node Type for Client

The NetBIOS node type for Microsoft DHCP clients can be one of four settings: broadcast, peer-to-peer, mixed, or hybrid. To configure the NetBIOS node type for a Microsoft DHCP, use the following command in DHCP pool configuration mode:

Command	Description
netbios-node-type *type*	■ Specify NetBIOS node type of Microsoft DHCP client.

Setting IP Address Range to Be Assigned in Network Pool

Set address range to assign to clients in network pool. Non-consecutive many addresses range can be assigned in one network pool.

Command	Description
range *lowest-address highest-address*	■ Set IP address range to be assigned to clients in subnet.

DHCP Host Pool Setting

A manual binding is a mapping between the IP address and MAC address of a client. The IP address of a client can be assigned manually by an administrator or assigned automatically from a pool by a DHCP server and manual bindings are just special address pools. Enter DHCP Host Pool Configuratoin mode to set parameters such as IP and MAC.

To set a DHCP address pool, you have to finish the required tasks in the following section.

Setting DHCP Host Pool Name and Entering DHCP Configuration Mode

To configure the DHCP Host pool name and enter DHCP pool configuration mode, use the following command in Config mode.

Command	Description
ip dhcp host-pool *name*	■ Generate a name for DHCP Host pool ■ Enter the DHCP Host Pool configuration mode identified as “config-dhcp#” prompt.

Table 40. Host Pool Configuration Command

Command	Description
bootfile *filename*	■ Specify file name to use as boot image.
default-router *address*	■ Show IP address of a default router for DHCP client.
dns-server *address1 address2 address3*	■ Specify the IP address of the DNS server that the DHCP client can use. ■ One IP address is required. ■ You can specify up to three IP addresses in the command line.
domain-name *domain*	■ Specify domain name for a client.
netbios-name-server *address*	■ Specify the IP address of NetBIOS WINS server that Microsoft DHCP client can use.
netbios-node-type *type*	■ Specify the NetBIOS node type of Microsoft DHCP client.
network *ipaddr/prefix-len*	■ Manual Binding IP Network be specified in one Host Pool

Notice Manual Binding List in one Host Pool can be allocated in the network range by ***network*** command.

Setting client for Client DHCP Manual Binding

It configures clients to provide manual binding in host pool.

Command	Description
host *ip-address netmask*	■ Generate IP address to allot and network mask to provide to a client ■ Enter the DHCP Host Configuration Mode identified as “config-dhcp-host#”.

Table 41. Manual Binding Command

Command	Description
hardware-address *hardware-address*	■ Specify the hardware address of the client.
client-name *name*	■ This command is optional and it is used to specify the client name by using the standard ASCII characters. ■ The client name does not include the domain name. For example, do not specify mars as mars.ubiquoss.com.

Other Global Command

Table 42. Global Command List

Command	Description
ip dhcp default-lease {days [hours] [minutes]|infinite}	■ Specify the lease period. ■ The default is one hour. ■ Infinite: Use automatic allocation sytstem leasing IP address permanenetly to host
ip dhcp max-lease {days [hours] [minutes]|infinite}	■ Specify the maximum lease period ■ The default is one day.
ip dhcp unbindig-user drop	It discards the packets when users not assigned by switch try to get services.

DHCP Server Enabling

By default, the DHCP server functions of the switch are not enabled. To enable the features in which are disabled, use the following command in global configuration mode

Command	Description
service dhcp server	■ Enable the DHCP server functions of the switch. ■ Use the **no** command to disable the DHCP server functions.

Registering DHCP Relay Agent

If you use P8824XG switch as DHCP replay agent, the switch relays the requests only from the DHCP clients to DHCP server.

Table 43. Command for Registering DHCP Relay Agent

Command	Description
ip dhcp relay-agent *address mask*	■ Permit the DHCP requests from the DHCP relay agent.

Server Configuration in DHCP Relay Agent

To set DHCP server in DHCP relay agent, use the following command in the Global configuration mode.

Command	Description
ip dhcp helper-address *address*	■ Set IP addresses of DHCP server for DHCP relay agent ■ Use the **no** command to delete the DHCP server functions.

DHCP relay information option (OPTION82) Configuration

DHCP relay agent provides DHCP relay information option function to include information about DHCP relay agent itself and client when relaying the request from DHCP client to DHCP server.

Enabling DHCP Relay Information Option function

To enable relay information option function of DHCP Relay Agent, use the following command.

Command	Description
ip dhcp relay information option	■ Enable DHCP relay information (option-82 field) function. ■ By default, the DHCP replay functions of the switch are not enabled.

Relay Information Option Re-forwarding Policy Setting

By default, P8824XG re-forwarding policy replaces the current replay information in the received packet from DHCP client with the replay information of switch

To change default policy, use the following command in global mode.

Command	Description
ip dhcp relay information policy {append|drop|keep|replace}	■ The default is replace. ■ Append : Append relay information of switch to messages with the existing information. ■ Drop : Discard packet with existing relay information if the relay information option is already present. ■ Keep : Existing information is left unchanged on the DHCP relay agent. ■ Replace : Existing information is overwritten on the DHCP relay agent.

Enabling DHCP Relay Function

By default, the DHCP replay functions of the switch are not enabled. To enable these features if they are disabled, use the following command in global configuration mode

Command	Dewscription
service dhcp relay	■ Enable DHCP Replay function of the switch ■ Use no format of this command to disable the DHCP relay functions.

DHCP Server Monitoring and Management

Displaying DHCP Server Pool Information

To display DHCP Address Pool Information in DHCP server, use the following command in the privileged EXEC mode.

Command	Description
show ip dhcp pool	■ Display DHCP Address Pool Information of DHCP server
show ip dhcp pool network-pool [name]	■ Display Information on network pool of DHCP server DHCP
show ip dhcp pool host-pool [name]	■ Display Information on host pool of DHCP server

Displaying DHCP Server Binding

To display DHCP address binding information that DHCP server sends to client, use the following command in the privileged EXEC mode.

Command	Description
show ip dhcp binding	■ Display all bindings in DHCP Server
show ip dhcp binding detail	■ Display details of all binding in DHCP server.
show ip dhcp binding network-pool {address |name}	■ Display binding in network pool of DHCP server. ■ Address : Display binding for address ■ Name: Display binding in the network pool for name.
show ip dhcp binding host-pool {address|name}	■ Display binding in the host pool of DHCP server ■ Address : Display binding for address ■ Name: Display binding in the host pool for name.

DHCP Server Statistics Inquiry

Command	Description
show ip dhcp server statistics	■ Display the server statistics and the counter information related to the sent/received messages

DHCP Server Conflict Inquiry

Command	Description
show ip dhcp conflict *{poolname}*	■ Display all the address conflicts that the DHCP server has logged. ■ Display conflicts information in the specific pool.

DHCP Server Variable Initialization Command

Command	Description
clear ip dhcp binding {*address*|*}	■ Delete automatic address binding form DHCP database. ■ If you specify an *address,* then the automatic binding of the specified IP address will be deleted. ■ If you use "*", all the automatic binding will be deleted
clear ip dhcp server statistics	■ Initialize all the statistics counters of all DHCP servers.

DHCP Relay Monitoring and Management

Table 44. DHCP Relay Monitoring and Management Command

Command	Description
show ip dhcp helper-address	■ Display the DHCP server list.
show ip dhcp relay information option	■ Enable DHCP relay information option and display reforwarding policy
show ip dhcp relay statistics	■ Display the relay statistics and the counter information related to the sent/received messages.
debug ip dhcp relay {events|packets}	■ Enable the DHCP replay debugging.

Example of DHCP Configuration

This section provides the following configuration examples.

- Example of DHCP network pool configuration
- Example of DHCP host pool configuration
- Example of DHCP server monitoring and management
- Example of DHCP relay agent configuration
- Example of manual binding configuration
- DHCP Relay Agent Monitoring and Management

Example of DHCP Network Pool Configuration

The following is the example of the generation of DHCP network pool that uses 192.168.1.0/24 network. The default router of the client is set as 192.168.1.1 and ubiquoss.com is used as the domain name. The IP address of the client is leased for a day and the address ranges to be assigned are 192.168.1.10~192.168.1.100 and 192.168.1.150~192.168.1.230.

```
Switch(config)# ip dhcp network-pool   marketing
Switch(config-dhcp)# domain-name   ubiquoss.com
Switch(config-dhcp)# lease   1
Switch(config-dhcp)# network   192.168.1.0/24
Switch(config-dhcp)# default-router 192.168.1.1
Switch(config-dhcp)# range 192.168.1.10 192.168.1.100
Switch(config-dhcp)# range 192.168.1.150 192.168.1.230
```

The following shows the example of the generation of the DHCP network pool and group setting that uses 192.168.2.0/24 and192.168.3.0/24 network. The default-router of 192.168.2.0/24 network is 192.168.2.1 and the address range is 192.168.2.10~192.168.240. Default-router of 192.168.3.0/24 network is 192.168.3.1 and address ranges are 192.168.3.10~192.168.3.50 and 192.168.3.100~192.168.3.230. And DNS servers are set as 1.2.3.4. And 1.2.3.5. 12 hours of IP address lease is guaranteed to each client.

```
Switch(config)# ip dhcp network-pool   sales1
Switch(config-dhcp)# dns-server   1.2.3.4 1.2.3.5
Switch(config-dhcp)# lease   0 12
Switch(config-dhcp)# network   192.168.2.0/24
Switch(config-dhcp)# default-router   192.168.2.1
Switch(config-dhcp)# range   192.168.2.10 192.168.2.240
Switch(config-dhcp)# group vlan10
Switch(config-dhcp)# exit
Switch(config)# ip dhcp network-pool   sales2
Switch(config-dhcp)# dns-server   1.2.3.4 1.2.3.5
Switch(config-dhcp)# lease   0 12
Switch(config-dhcp)# network   192.168.3.0/24
Switch(config-dhcp)# default-router   192.168.3.1
Switch(config-dhcp)# range   192.168.3.10 192.168.3.50
Switch(config-dhcp)# range   192.168.3.100 192.168.3.230
Switch(config-dhcp)# group vlan10
```

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

Example of DHCP Host Pool Configuration

The following shows the example of the host pool configuration in 192.168.4.0/24 network. The default-router is 192.168.4.1 and and ubiquoss.com is used as the domain name. This is host pool for the clients using 192.168.4.10 and 192.168.4.11 as DNS-server. And, IP addresses of 192.168.4.114, 192.168.4.115, 192.168.4.116 and netmask of 255.255.255.0 are allocated to the clients whose MAC addresses are 00:01:02:94:77:d7, 00:01:02:94:77:d8, and 00:01:02:94:77:d9, respectively.

The IP address allocated in a manual binding is permanently used.

```
Switch(config)# ip dhcp host-pool mars
Switch(config-dhcp)# network 192.168.4.0/24
Switch(config-dhcp)# default-router  192.168.4.1
Switch(config-dhcp)# dns-server  192.168.4.10 192.168.4.11
Switch(config-dhcp)# domain-name  ubiquoss.com
Switch(config-dhcp)# host  192.168.4.114 255.255.255.0
Switch(config-dhcp-host)# hardware-address  00:01:02:94:77:d7
Switch(config-dhcp-host)# exit
Switch(config-dhcp)# host  192.168.4.115 255.255.255.0
Switch(config-dhcp-host)# hardware-address  00:01:02:94:77:d8
Switch(config-dhcp-host)# exit
Switch(config-dhcp)# host  192.168.4.116 255.255.255.0
Switch(config-dhcp-host)# hardware-address  00:01:02:94:77:d9
```

Notice *The same IP address is always allocated to the client configured through manual binding.*

Example of DHCP Server Monitoring and Management

The following is the example of displaying the DHCP address pool information created in the DHCP server.

Switch# show ip dhcp pool

Pool Name	Type	IP address	Total	Used	Usage
mars	Host	192.168.4.115/24	1	1	100%
mars	Host	192.168.4.116/24	1	1	100%
mars	Host	192.168.4.117/24	1	1	100%
marketing	Network	192.168.1.0/24	172	0	0%
sales1	Network	192.168.2.0/24	231	0	0%
sales2	Network	192.168.3.0/24	172	0	0%

Switch# **show ip dhcp pool network-pool sales1**	
Address pool Name	Sales
Type	Network
Default router	192.168.2.1
Lease	0 days, 12 hours, 0 minutes
DNS server	1.2.3.4 1.2.3.5
Network	192.168.2.0 255.255.255.0
Range(s)	
	192.168.2.10 ~ 192.168.2.240
group	vlan10

Switch# **show ip dhcp pool host-pool mars**	
Address pool Name	Sales
Type	Host
Lease	infinite
Default router	192.168.4.1
DNS server	192.168.4.10 192.168.4.11
Domain name	ubiquoss.com
Network	192.168.4.0/24
Host	192.168.4.114 255.255.255.0
Hardware address	00:01:02:94:77:d7
Host	192.168.4.115 255.255.255.0
Hardware address	00:01:02:94:77:d8
Host	192.168.4.116 255.255.255.0
Hardware address	00:01:02:94:77:d9

Notice With show running-config command, you can see the configuration information that the administrator has set.

The following example shows the IP address that the DHCP server allocates to the client.

Switch# **show ip dhcp binding**			
IP address	Hardware address	Lease expiration	Type
192.168.4.114	00:01:02:94:77:d7	Infinite	Maunal
192.168.3.10	02:c7:f8:00:04:22	Wed Mar 12 06:27:39 2003	Automatic

The following example shows the IP address that the DHCP server allocates to the client.

Switch(Config)# **show ip dhcp binding detail**

TYPE	: Manual
IP addr	: 192.168.4.114
HW addr	: 00:01:02:94:77:d7
Client ID	: -
Host Name	: -
Lease	: Infinite

TYPE	: Manual
IP addr	: 192.168.4.115
HW addr	: 00:01:02:94:77:d8
Client ID	: -
Host Name	: -
Lease	: Infinite

TYPE	: Manual
IP addr	: 192.168.4.116
HW addr	: 00:01:02:94:77:d9
Client ID	: -
Host Name	: -
Lease	: Infinite
----------	
total 3 bindings found	

The following shows the example of deleting the binding information of the DHCP server so that the DHCP server can use an IP address that has been already bound to a client (DHCP server attempts to use the IP address of other client).

.

```
Switch(Config)# clear ip dhcp binding 192.168.3.10
Switch(Config)# show ip dhcp binding
IP address     Hardware address Lease expiration Type
192.168.4.114       00:01:02:94:77:d7 Infinit    Maunal
```

The following example shows the statistic data of the DHCP server.

Switch# show ip dhcp server statistics	
Message	Received
Malformed messages	0
BOOTREQUEST	0
DHCPDISCOVER	200
DHCPREQUEST	178
DHCPDECLINE	0
DHCPRELEASE	0
DHCPINFORM	0
ICMPECHO	

Message	Sent
BOOTREPLY	0
DHCPOFFER	190
DHCPACK	172
DHCPNAK	6

Example of DHCP Relay Agent Configuration

The following example shows the DHCP Relay Agent of the switch sets the DHCP server that transfers the requests of the client. If there is no DHCP address pool that satisfies the client's request, the switch transfers the client's request to the DHCP server located in other sub-network.

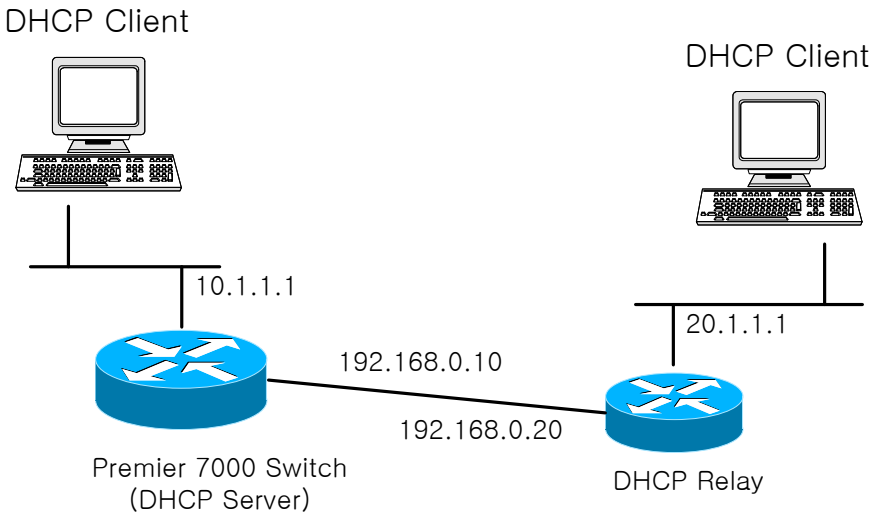


Figure 14. Example Network for DHCP Relay Agent Configuration

```
Switch(config)# ip dhcp helper-address    10.1.1.2
Switch(config)# end
Switch# show ip dhcp helper-address
Server's    IP address : 10.1.1.2
```

Notice To transfer DHCP message to a DHCP server located in other sub-network, the route information on the network must be configured in the DHCP server of the switch.

Chapter 6. NAT

This chapter explains NAT setting of P8824XG switch.

NAT Introduction

Internet is expanding at very fast rate. Network Address Translation (NAT) is a method of connecting multiple computers to the Internet or any other IP network using one IP address. This allows subscribers and small businesses to connect their network to the Internet cheaply and efficiently.

The specific group using the private IP address translates this address into the public IP address to access to Internet. RFC 1631 represents a subset of NAT functionality.

NAT Configuration

Before NAT configuration, you should be aware of inside address that is used in the private network and outside address that is used in the pubic network.

P8824XG switch supports three mechanisms for NAT.

- Satic translation : Translate the specific inside address into the specific outside address.
- Dynamic translation : Translate many inside IP addresses into one or more outside address.
- Local translation : Translate source IP of traffic from P8824XG switch and it is set by protocol, port, and destination.

P8824XG switch supports three mechanisms for dynamic translation based on outside address selection.

- MASQUERADE : No specific outside address and use the address for outside interface.
- PAT : Use only one outside address
- NAT : Use two or more outside addresses

The source IP of the traffic generated by switches can be changed and configured based on protocol, port, and distination

The section below explains NAT configuration of P8824XG switch.

Static NAT Configuration

Static NAT configuration translates one specific private IP address into another public IP address and performs the following command in global mode.

Command	Description
ip nat static inside *IFNAME address* **outside** *IFNAME address*	■ Configure pribate network and public network for static nat

The following is the configuration example.
Switch**# configure terminal**
Switch(config)**# ip nat static vlan1 192.168.0.1 outside vlan2 200.1.1.1**

Dynamic NAT Configuration

Use the following commands to apply dynamic translation,

Setting Dynamic NAT with Masquerade Mode

Setting Dynamic NAT with masquerade mode, packet source IP of inside network is translated into the address for the outside IFNAME, and transmitted.

Command	Description

ip nat dynamic inside *IFNAME netnum/prefix-len* **outside** *IFNAME*	■ Pool configuration for inside network ■ Setting outside interface

The following example shows how to configure the masquerade mode. VLAN1 and 192.168.1.0/24 are defined for private address and set the outgoing interface to VLAN2.

SWITCH**# configure terminal**
SWITCH(config)**# ip nat dynamic inside vlan1 192.168.1.0/24 outside vlan2**
SWITCH(config)**# exit**

Setting Dynamic NAT as PAT Mode

The NAT with PAT (Port Address Translation) is configured as using the following command in global mode. In this case, packet source IP from inside network is translated into one IP for outside pool, and transmitted.

Command	Description
ip nat dynamic inside *IFNAME netnum/prefix-len* **outside** *IFNAME address*	■ Pool configuration for inside network ■ Setting IP to be translated, and outside interface

The following explains how to configure Dynamic NAT with PAT mode, and the packets with source IP address of 192.168.1.0/24 from VLAN 1 are translated into 200.1.1.1 and transmitted.

SWITCH**# configure terminal**
SWITCH(config)**# ip nat dynamic inside vlan1 192.168.1.0/24 outside vlan2 200.1.1.1**
SWITCH(config)**# exit**

Setting Dynamic NAT with NAT mode

The dynamic NAT with PAT (Port Address Translation) is configured by using the following command in global mode. In this case, packet source IP from inside network is translated into one IP of outside pool, and transmitted.

Command	Description
ip nat dynamic inside *IFNAME netnum/prefix-len* **outside** *IFNAME lowest-address highest-address*	■ Pool configuration for inside network ■ Setting outside interface and IP Pool to be translated.

The following explains how to configure dynamic NAT with NAT mode. The packets with source IP address of 192.168.1.0/24 from VLAN 1 are translated into 200.1.1.1 ~ 200.1.1.4 and transmitted.

SWITCH# **configure terminal**
SWITCH(config)# **ip nat dynamic inside vlan1 192.168.1.0/24 outside vlan2 200.1.1.1**
SWITCH(config)# **exit**

Notice Flow-rule (refer to 1.5 of chapter 12) is followed to NAT setting.

SWITCH# **configure terminal**
SWITCH(config)# **ip nat dynamic inside vlan1 192.168.1.0/24 outside vlan2 200.1.1.1**
SWITCH(config)# **flow-rule nat classfy ip 192.168.1.0/24 any** SWITCH(config)# **flow-rule nat match trapcpu**
SWITCH(config)# **policy-map nat flow-rule nat**
SWITCH(config)# **interface vlan10**
SWITCH(config-if-vlan10)# **service-policy nat**
SWITCH(config-if-vlan10)# **exit**
SWITCH(config)# **exit**

Notice Add NAT flow-rule to the policy map when policy-map is already applied to the current VLAN 10.

Setting Local NAT

Local NAT is used to translate the source IP of traffic from P8824XG switch as using the following command.

Command	Description
ip nat local inside *source-netnum/prefix-len protocol portnum destionation-netnum/prefix-len* **outside** *address*	■ Protocol : TCP, UDP, ICMP or “any” for no specific setting ■ Portnum : Port number to apply or “any” for no specific port ■ Destionation-netnum/prefix : the specific destination, or “any” for no specific setting

	■ Address : IP address to be translated

The following example shows the source IP translation of traffic going to FTP server 20.1.1.1 among the packets with source IP 10.1.1.0/24.

SWITCH**# configure terminal**
SWITCH(config)**# ip nat local inside 10.1.1.0/24 tcp 21 20.1.1.1/32 outside 200.1.1.1**
SWITCH(config)**# exit**

Switch# show ip nat static
MODE Private IP Public IPDirection
STATIC 10.2.2.10 200.1.1.101 vlan3->vlan2
total 1 pools found

Notice Port number can be set only when TCP or UDP are set as protocol. And, set “any” for no specific field.

Enabling NAT

Use the following command in the global mode to enable NAT.

Command	Description
service nat	Enable NAT engine.

Switch**# configure terminal**
Switch(config)**# service nat**
Switch(config)**# exit**

NAT Configuration

Static NAT Setting Information Inquiry

Command	Description
show ip nat static	Display the current configuation information of Static NAT

The following is the configuration information when VLAN 3 interface is set as 10.2.3.0/24 and static NAT.

Dynamic NAT Configuration Information Inquriy

Command	Description
show ip nat dynamic	Display the current configuration information of Dynamic NAT

The following is the configuration information when the VLAN 1 interface of 10.1.1.0/16 network is set as dynamic NAT with masquerade, PAT, and NAT mod, respectively.

Switch# show ip nat dynamic
MODE Private IP Public IPDirection
MASQ 10.1.0.0/25- vlan1->vlan2
PAT10.1.0.128/26 200.1.1.100 vlan1->vlan2
NAT10.1.0.192/26 200.1.1.200-200.1.1.204 vlan1->vlan2
total 3 pools found

Local NAT Configuraion Information Inquiry

Command	Description
show ip nat local	Display the current configuration information of local NAT

Switch# show ip nat local
MODE SRC-IPPROTO PORT DEST-IP PUB-IP
LOCAL10.1.1.0/24 tcp 23 210.108.10.0/24 200.1.1.99
LOCAL10.1.1.0/24 tcp 21 20.1.1.1/32 200.1.1.1
total 2 pools found

Chapter 7. IGMP Snooping

This chapter introduces the IGMP Snooping functionality of P8824XG.

IGMP Snooping Introduction

Multicast traffic is processed as unknown MAC address or broadcast frame and all ports in VLAN are flooded.

IGMP Snooping does not forward multicast traffic to all ports in VLAN and add/delete ports for forwarding multicast traffic. Switch snoops IGMP traffic between host and router and get information for multicast group and member port.

The procedure of IGMP Snooping in brief is as follows.

After receiving 'IGMP Join' message in the specific milticast group, add the received port into multicast forwarding table entry. After receiving 'IGMP Leave' message from host, delete the port from the table entry. And, after replaying IGMP Query message to all ports in VLAN, delete port that could not get an IGMP Join message.

IGMP Snooping Configuration

The IGMP Snooping is Operating in global configuration mode and configure the Snooping function on each VLANs.

Enable Global IGMP Snooping

To enable IGMP Snooping globally, use the following command in the global configuration mode.

Command	Description
ip igmp snooping	Enable the IGMP Snooping
no ip igmp snooping	Disable the 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 : 10 sec
- TCN Query Solicit : DISABLED
IGMP snooping is DISABLED on ALL interface
IGMP snooping fast-leave is DISABLED on ALL interface
```

Enable IGMP-TRAP on an Interface

As IGMP Snooping is working on the Switch, IGMP-TRAP on each port interface must be enabled to be able to receive IGMP packets. To configure VLAN for IGMP Snooping, use the following command in the interface configuration mode.

Command	Description
igmp-trap	Enable igmp-trap on the interface
no-igmp-trap	Disable igmp-trap

```
Switch # configure terminal
Switch (config)# interface gi1
Switch (config-if-gi1)# igmp-trap
Switch # show running-configure
...
!
interface gi1
igmp-trap
!
…
Switch #
```

Enable IGMP snooping on a VLAN

The switch enables/disables IGMP Snooping on each VLAN. To configure VLAN for IGMP Snooping, use the following command in the global configuration mode.

Command	Description
ip igmp snooping vlan *<1-4096>*	Enable IGMP Snooping on specific VLAN
no ip igmp snooping vlan *<1-4096>*	Disable IGMP Snooping on specific VLAN

```
Switch # configure terminal
Switch (config)# ip igmp snooping
Switch (config)# ip igmp snooping vlan 1
Switch (config)#
Switch # show ip igmp snooping vlan 1
Global IGMP Snooping configuration:
- Aging Interval : 300 sec
- Last Member Join Interval : 10 sec
- TCN Query Solicit : DISABLED
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 : gi1 gi2 gi3 gi4
Switch #
```

Configure IGMP Snooping Functionality

To configure the IGMP Snooping features, perform the following task.

Setting report-suppression

Basically, the IGMP report-suppression function of IGMP Snooping was disabled, and all the received IGMP Reports are forwarded to the Multicast Router. If IGMP report-suppression is enabled, IGMP Snooping will forward only one IGMP Report per each Multicast Membership Group to the Multicast Router.

This function is applied only to IGMPv1 and IGMPv2 Report message.

Command	Description
ip igmp snooping report-suppression	Set IGMP report-suppression.
no ip igmp snooping report-suppression	Release the preset 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 : 10 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 : gi1 gi2 gi3 gi4
```

Setting Fast-leave

After enabling the Fast-leave funtion of IGMP Snooping and receiving IGMPv2 Leave message from host, deletes the port in forwarding table at once.

This feature is only in case of one host in each port of VLAN. In case of having many hosts in a port, a host that doesn't send IGMPv2 Leave message doesn't possibly get traffic for multicast group for the specific time. It is available only if the host uses IGMPv2 supporting Leave message.

Fast-Leave can be applied to each VLAN and PORT as below, and if the Fast-Leave is set by each VLAN, the prioriry is higher than the PORT, the member of VLAN.

Command	Description
ip igmp snooping vlan <*1-4096*> **fast-leave**	Enables Fast-leave function on the specific VLAN.
no ip igmp snooping vlan <*1-4096*> **fast-leave**	Disables Fast-leave function on the specific VLAN.
ip igmp snooping vlan <*1-4096*> **fast-leave** *IFNAME*	Enables Fast-leave function on the specific port of VLAN.
no ip igmp snooping vlan <*1-4096*> **fast-leave** *IFNAME*	Disables Fast-leave function on the specific port of VLAN.

```
Switch # configure terminal
Switch (config)# ip igmp snooping vlan 1 fast-leave gi1
Switch (config)# ip igmp snooping vlan 1 fast-leave gi2
Switch # show ip igmp snooping vlan 1
Global IGMP Snooping configuration:
- Aging Interval : 300 sec
- Last Member Join Interval : 10 sec
- TCN Query Solicit : DISABLED
vlan1
IGMP snooping is ENABLED on this interface
IGMP snooping fast-leave is ENABLED on gi1 gi2
IGMP snooping mr-learn is DISABLED on this interface
Vlan Members : gi1 gi2 gi3 gi4
Switch # configure terminal
Switch (config)# ip igmp snooping vlan 1 fast-leave
Switch # show ip igmp snooping vlan 1
Global IGMP Snooping configuration:
- Aging Interval : 300 sec
- Last Member Join Interval : 10 sec
- TCN Query Solicit : DISABLED
vlan1
IGMP snooping is ENABLED on this interface
IGMP snooping fast-leave is ENABLED on this interface
IGMP snooping mr-learn is DISABLED on this interface
Vlan Members : gi1 gi2 gi3 gi4
```

```
Switch #
```

Setting Mrouter Configuration

Switch forwards all the Multicast Traffice to the Multicast Router to forward all the Multicast Traffic within the VLAN to other networks. so the ports to which the Multicast Router is connected are added to all the Multicast Forwarding Table Entry as outgoing ports.
Basically, IGMP detects the ports connected to the Multicast Router by carrying out Snooping only for IGMP Traffic, and can detect mrouter ports by enabling PIM/DVMRP protocol manulally.
The mrouter ports known in the above methods are always registered as outgoing ports whenever new Multicast Forwarding Table Entry is created, and forwards to Mrouter ports not only Multicast Traffic but also IGMP Join messages transmitted from the Host.

To set multicast router port manually, use the following command in the Global configuration mode.

Command	Description
ip igmp snooping vlan *<1-4096>* **mrouter interface** *IFNAME*	Sets the mrouter port manually. IFNAMEshould be a Member-Port already existing in the VLAN.
no ip igmp snooping vlan *<1-4096>* **mrouter interface** *IFNAME*	Disables the preset mrouter port.

```
Switch # configure terminal
Switch (config)# ip igmp snooping vlan 1 mrouter interface gi1
Switch # show ip igmp snooping mrouter
VLAN MULTICAST-ROUTER-PORT
0001 gi1
```

To detect Multicast Router Port dynamically through PIM/DVMRP protocol, please carry out the following commands in global configuration mode.

Command	Description
ip igmp snooping vlan *<1-4096>* **mrouter learn pim-dvmrp**	Enable detection of mrouter port by snooping PIM/DVMRP protocol.
no ip igmp snooping vlan *<1-4096>* **mrouter learn pim-dvmrp**	Disable detection of mrouter using PIM/DVMRP protocol.

```
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 : 10 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 : gi1 gi2 gi3 gi4
```

Aging Time Configuration

In IGMP protocols, the membership of Multicast Group is managed in ways in which the Multicast Router that works as a IGMP Querier transfers IGMP Query regularly, and the hosts sends IGMP Join message as a reply. IGMP Snooping adds or deletes the outgoing port in Multicast Forwarding Table Entry using these IGMP protocol message.

If the Multicast Forwarding Table Entry is not renewed for the preset aging time due to failure in getting IGMP Join message, the port are removed from the Multicast Forwarding Table Entry in the outgoing ports.

The default aging time is 300 seconds, and can be set by carrying out the following commands in global configuration mode.

Command	Description
ip igmp snooping aging <*30-3600*>	Set aging time (Default: 300 seconds)
no ip igmp snooping aging	Set the aging time to default.

```
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 : 10 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 : gi1 gi2 gi3 gi4
```

Setting Last-member-join-interval

If the fast-leave function of IGMP Snooping is not enabled in the VLAN, it does not remove the port immediately when it receives an IGMP Leave message, and remove it from Multicast Forwarding Table Entry after preset aging time.

The last-member-join-interval can be set so that the Multicast Membership management can be carried out little bit earlier before the end of the preset aging time.

If the last-member-join-interval is not set, the last-member-join-interval will be set same as aging time, and the port will be removed based on the aging time of the IGMP Snooping. This function is valid only when the fast-leave function is not enabled in the VLAN.

To set last-member-join-interval, use the command in the global configuration mode.

Command	Description
ip igmp snooping last-member-join-interval <*5-300*>	Set last-member-join-interval (Default: 10 seconds)
no ip igmp snooping last-member-join-interval	Set the last-member-join-interval to default

```
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 : gi1 gi2 gi3 gi4
```

tcn (Topology Change Notification) Setup

Basically, IGMP Snooping initializes all the Multicast Forwarding Table Entries when received spanning-tree Topology Change Notification (TCN). Later, new Multicast Forwarding Table Entry is created by IGMP Query of Multicast Router.

The tcn setting provided in this equipment sends IGMP Leave message to the Multicast Router for “0.0.0.0” Group if it receives spanning-tree Topology Change Notification (TCN). The Multicast Router sends IGMP Query message after receiving the IGMP Leave message for “0.0.0.0” Group, and the Multicast Forwarding Table Entry of the network with changed Topology is created newly within short time.

The tcn can be set in all the equipment that is formed as spanning-tree, using the following commands in the global configuration mode.

Command	Description
ip igmp snooping tcn query-solicit	Enable the TCN Query-Solicit.
no ip igmp snooping tcn query-solicit	Disable 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 : 10 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 : gi1 gi2 gi3 gi4
```

igmp filtering Setup

IGMP filtering filters the IGMP Packets from users connected to the switch ports. Therefore the distribution of Multicast service such as the service plan in specific Network environment or provision of service based on application can be managed.

Each Switch Port has IGMP Profile for filtering, and the IGMP Profile includes the blocking or allowing for more than 1 Multicast Group and the Group.

To set the IGMP filtering, the IGMP Profile should be set first, and the IGMP Profile setting can be carried out by the following commands in global configuration mode.

Command	**Description**

ip igmp snooping profile <*1-99*> permit <*multicast address*> range <*multicast address*>	Set the IGMP Profile that allows IGMP Filtering.
ip igmp snooping profile <*1-99*> deny {<*multicast address*> | <*all*>} range <*multicast address*>	Set the IGMP Profile that blocks IGMP Filtering.
no ip igmp snooping profile <*1-99*>	Delete the preset 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
```

To apply IGMP filtering after creating IGMP Profile, use the following commands in the interface mode.

Command	Description
ip igmp snoop-filter <*1-99*>	Apply the IGMP Filtering to the swith ports.
no ip igmp snoop-filter <*1-99*>	Disable the preset IGMP Filtering.

```
Switch # configure terminal
Switch (config)# interface gi1
Switch (config-if-gi1)# ip igmp snoop-filter 1
Switch # show running-configure
…
!
interface gi1
ip igmp snoop-filter 1
!
…
Switch #
```

igmp max-group-count setup

To provide multicast service by classifying each subscriber, Multicast Group number can be limited. To limit number of Multicast Groups, run the following commands in global configuration mode.

Command	Description
ip igmp snooping max-group-count *IFANME* <*count*>	Applies max-group-count to a port of the switch.

no ip igmp snooping max-group-count *IFANME*	Disables max-group-count from a port of the switch.

```
Switch # configure terminal
Switch (config)# ip igmp snooping max-group-count gi1 10
Switch # show running-configure
…
ip igmp snooping
ip igmp snooping max-group-count gi1 10
…
Switch #
```

igmp max-reporter-count setup

To provide multicast service by limiting the number of subscribers for each VLAN interface, the number of Hosts can be limited.

To limit the number of Hosts, run the following commands in global configuration mode.

Command	Description
ip igmp snooping max-reporter-count vlan *<vlan-id> <count>*	Applies max-reporter-count to VLAN interface.
no ip igmp snooping max-reporter-count vlan *<vlan-id>*	Disables the preset max- reporter –count from VLAN interface.

```
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 #
```

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

```
Switch # configure terminal
Switch (config)# ip igmp snooping max-reporter-count port gi1 10
Switch #
Switch # show running-configure
…
ip igmp snooping
ip igmp snooping max-reporter-count port gi1 10
…
Switch #
```

IGMP Proxy-Reporting Overview

Normally, the switching fabric of Network equipment is limited, but the request for IGMP Membership that should be processed at the same time is increasing due to increase of various Multicast Service and Multi-Accessed Network environment. These requests for IGMP Membership from IGMP HOSTs may cause overload of the quipment in the upper networks, and can cause delay or disconnection of Multicast Services.
In this reason, DSL Forum provides the documents that define IGMP Proxy-Reporting functions, and this equipment includes IGMP Proxy-Reporting functions defined by DSL Forum.
IGMP Proxy-Reporting provides all the function defined in IGMP. IGMP Proxy-Reporting uses the IP Address of the VLAN that specified IP Source Address of the IGMP Report and IGMP Query message when an IP address exists in the IGMP Proxy-Reporting enabled VLAN interface, and if the IP address of VLAN is not specified, uses the latest IGMP Host Address managed in IGMP Membership.

IGMP Proxy-Reporting Setup

IGMP Proxy-Reporting service can be enabled / disabled globally. IGMP Proxy-Reporting function can be applied for each VLAN Interface.

Enable IGMP Proxy-Reporting

To enable the IGMP Proxy-Reporting globally, use the following commands in the global configuration mode.

Command	Description
ip igmp snooping proxy-reporting	Enable IGMP Proxy-Reporting.
no ip igmp snooping proxy-reporting	Disable 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

This equipment allows to enable/disable IGMP Proxy-Reporting for each VLAN.
To set the VLAN to which actual IGMP Proxy-Reporting function will be applied, please use the following command in global configuration mode.
In the VLAN where IGMP Proxy-Reporting function is applied, the IGMP packet forwarding is not carried out through IGMP Snooping.

Command	Description
ip igmp snooping proxy-reporting vlan *<1-4096>*	Enable IGMP Proxy-Reporting to the specific VLAN.
no ip igmp snooping proxy-reporting vlan *<1-4096>*	Disable IGMP Proxy-Reporting to the 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 :
```

```
gi1 gi2
_____________________________________________________________
total : 1
Switch #
```

Configure IGMP Proxy-Reporting Functionality

To enable IGMP Proxy-Reporting function, please carry out the following processes.

Specifying Multicast Router Port

To make the information of IGMP Membership managed in the IGMP Proxy-Reporting and upper Multicast Router, a static Multicast Router Port can be specified. The VLAN with Proxy-Reporting enabled recognizes the port in which the IGMP Query Packet is received as Multicast Router Port dynamically.

Command	Description
ip igmp snooping proxy-reporting vlan *<1-4096>* mrouter-port *IFNAME*	Specify Multicast Router Port to a specific VLAN for IGMP Proxy-Reporting.
no ip igmp snooping proxy-reporting vlan *<1-4096>* mrouter-port *IFNAME*	Delete Multicast Router Port specified to a specific VLAN for IGMP Proxy-Reporting.

```
Switch # configure terminal
Switch (config)# ip igmp snooping proxy-reporting vlan 1 mrouter-port
gi1
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 : gi1
VLAN Members :
gi1 gi2
_____________________________________________________________
total : 1
```

Specifying IGMP Static-Group

IGMP Proxy-Reporting provides Static-Group function to minimize the Join Delay Time required to receive the traffics from specific Multicast Group.
Static-Group is provided to receive Multicast Traffic by sending the specified IGMP Report regularly to the Multicast-Router Port.
This function should work together with IGMP Snooping, and the following commands are used in the global configuration mode.

Command	Description
ip igmp snooping proxy-reporting vlan *<1-4096>* static-group *A.B.C.D*	Specifies IGMP Static-Group through IGMP Proxy-Reporting to the specific VLAN.
no ip igmp snooping proxy-reporting vlan *<1-4096>* static-group *A.B.C.D*	Disable the specified 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 #

Command	Description
ip igmp snooping proxy-reporting vlan <*1-4096*> **static-group** *A.B.C.D* to <*count*>	Specifies IGMP Static-Group through IGMP Proxy-Reporting to the specific VLAN as many as the counts.
no ip igmp snooping proxy-reporting vlan <*1-4096*> **static-group** *A.B.C.D* to <*count*>	Disables the specified IGMP Static-Group as many as the counts.

Switch # **configure terminal**
Switch (config)# **ip igmp snooping proxy-reporting vlan 1 static-group 224.1.1.1 to 2**
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**
0080 224.1.1.2 0.0.0.0 00:04:03 **STATIC-GROUP**

total : 2
Switch #

Display System and Network Statistics

Table 45. IGMP Snooping-related monitoring commands

Command	Description
show ip igmp snooping	Shows the IGMP snooping status for all the VLANs.
show ip igmp snooping vlan *<1-4096>*	Shows IGMP snooping status for a specific VLAN.
show ip igmp snooping mrouter	Shows the information for all the mrouters.
show ip igmp snooping mac-entry	Shows the information of the preset Multicast Forwarding Table Entry.
show ip igmp snooping mac-entry vlan *<1-4096>*	Shows the Multicast Forwarding Table Entry set for specific VLAN.
show ip igmp snooping querier	Shows the information for all the IGMP Querier of Multicast Router.
show ip igmp snooping querier vlan *<1-4096>*	Shows the information for all the IGMP Queries of Multicast Router for specific VLAN.
show ip igmp snooping reporter	Shows the information of all the IGMP Reporter.
show ip igmp snooping reporter vlan *<1-4096>*	Shows the information of all the IGMP Reporters for specific VLAN.
show ip igmp snooping profile	Shows the information of preset IGMP Profile.
show ip igmp snooping suppression-forwarder	Shows the information of the forwarder of suppressed multicast group.

Table 46. IGMP Snooping-related monitoring command

Command	Description
show igmpsnooping proxy-reporting interface	Display IGMP Proxy-Reporting status of all VLANs.
show ip igmp snooping proxy-reporting group	Display information of all the managed IGMP Membership
show ip igmp snooping proxy-reporting querier	Display the information of all IGMP querier.

Chapter 8. Multicast Routing

This chapter describes IP multicast routing elements and IP multicast routing setting of P8824XG switch.

IP Multicast Routing Overview

IP Multicasting transmits packet in one Host group with many IP Hosts. This group includes switch in the local network, the private network, or outside of the local network. Host creating traffic transmits only one packet to host being received.

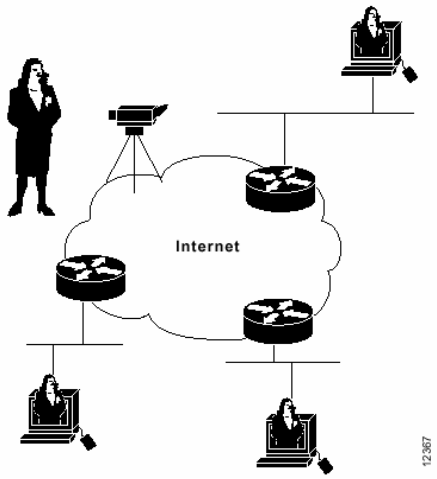


Figure 15. Multicasting to Transmit Traffic to Many Destinations

Many routing protocols such as Protocol-Independent Multicast (PIM), Distance-Vector Multicast Routing Protocol (DVMRP), multicast Open Shortest Path First (MOSPF) find multicast group and create the path for each group. The following table summarizes requirements for each protocol unicast and flooding algorithm.

Table 47. Multicast Protocol

Protocol	Unicast Protocol	Flooding Algorithm
PIM-dense mode	Any	Reverse path flooding (RPF)
PIM-sparse mode	Any	RPF
DVMRP	Internal	RPF
MOSPF	OSPF	Shortest-path first

IGMP Overview

IGMP is a protocol that IP Host registers IP multicast group membership in a router. The router inquires membership regularly to renew group membership stuatus, and the group remains registered if IP host answers.

Multicast group address is Class D IP address and defined in RFC1112.

PIM-SM Overview

PIM-SM is the protocol to connect small number of LANs for various multicast data stream and defines rendezvous point that is an entry point for easy multicast packet routing.

After the specific host transmits multicast packet, multicast router neighbored with the host transmits / registers multicast packet to the rendezvous point. And, multicast packet is transmitted from the sender to the rendezvoud point and then, to the receipent.

IP Multicast Routing Setting

Enable IP Multicast Routing

To forward multicast packet, IP multicast routing should be enabled basically. The following shows the command in the Global Configuration Mode.

Command	Descriptoin
ip multicast-routing igmp-querier	Enables IGMP Querier to manage IGMP Host Membership for Multicast Routing.
ip multicast-routing pim-sm	Enable PIM-SM for Multicast Routing.

Router# configure terminal
Router(config)# **ip multicast-routing pim-sm**
Router(config)# **ip multicast-routing igmp-querier**

Enable IGMP-TRAP on an interface

When enabling IGMP Querier in the router, the IGMP-TRAP should be enabled on each port interface so that it can receive IGMP packets.

Command	Description
igmp-trap	Enables igmp-trap for the interface.
no igmp-trap	Disable igmp-trap.

Router# **configure terminal**
Router(config)# **interface fa1/1**
Router(config-if-fa1/1)# **igmp-trap**

Enable PIM on an interface

To run PIM-SM, the PIM Flag should be enabled on the interface. To enable PIM Flag on an interface, use the following commands in the interface configuration mode.

Commands	Description
ip pim	Enable the PIM Flag on the interface.
no ip pim	Disable the PIM Flag.

Router# configure terminal
Router(config)# interface vlan1
Router(config-if-vlan1)# ip pim
Router# show ip pim interface
Address Interface Version/Mode Nbr JP MCache CISCO DR
Count Intvl Intvl ChkSum
10.1.1.254 vlan1 v2/Sparse 0 60 110 OFF 10.1.1.254
Router#

Enable IGMP on an interface

To run the IGMP Querier, the IGMP Flag should be enabled on the interface. To enable the IGMP Flag on the interface, use the following commands in the interface configuration mode.

Command	Description
ip igmp	Enabled the IGMP Flag on the interface.
no ip igmp	Disable the IGMP Flag.

```
Router# configure terminal
Router(config)# interface vlan1
Router(config-if-vlan1)# ip igmp
Router# show ip igmp interface
Name : vlan1
IGMP is enabled on interface.
Current IGMP version is 2
IGMP leave-timeout is 5 seconds.
IGMP member-checking-interval is 2 seconds.
IGMP querier-timeout is 255 seconds.
IGMP query-interval is 125 seconds.
IGMP query-max-response-time is 10 seconds.
Internet address is 10.1.1.254, subnet mask is 255.255.255.0. Quering Router(10.1.1.254)
```

Configure IGMP Functionality

To set various IGMP properties, carry out the following procedures.

IGMP Access Group

A Multicast router sends IGMP host-query message periodically to identify the Multicast group in whch the network hosts with this router attached are subscribed. Afterward, the router, if the packets with the Multicast group as destinations, forwards them to the member of the group. To limit the Multicast groups that the subnet host serviced by the interface can join, a filter can be set at each interface.

To allow the Interface to filter the access from specific Multicast group, use the following commands in the interface configuration mode.

Commands	Description
ip igmp access-group access-list-number	Controls the Multicast group to which the subnet hosts that are serviced by the interface can join
no ip igmp access-group	Disable the control of groups set to the interface.

```
Router# configure terminal
Router(config)# access-list 1 deny 239.0.0.0 255.0.0.0
Router(config)# interface vlan1
Router(config-if-vlan1)# ip igmp access-group 1
```

IGMP Query Transmit Interval

Multicast router sends IGMP Query message periodically to manage Multicast Membership. The TTL of this message is 1, and this message is sent to 224.0.0.1, all-system-group-address. Multicast routers, when selecting IGMP Querier router to send IGMP Query message for LAN (Subnet), selects the router with the smallest IP Address value. The selected Querier Router has the responsibility to send IGMP Query to all the hosts on the LAN, and send PIM Register and PIM Join message to RP routers.

By default, the IGMP Querier Router send IGMP host-query message every 125 seconds to keep the IGMP overhead of the host and network lower. To modify the sending interval, use the following command in the interface configuration mode.

Commands	Description

ip igmp query-interval seconds	Set the interval that the IGMP Querier Router sends IGMP Query message (Default : 125 seconds)
no ip igmp query-interval	Set the configured IGMP Query Interval as default.

```
Router# configure terminal
Router(config)# interface vlan1
Router(config-if-vlan1)# ip igmp query-interval 60
```

IGMP Leave Timeout

IGMP Querier Router, if it receives an IGMP Leave message that leaves from the Host for specific Multicast Group, checks the Multicast Membership to see if any Host joined in other Multicast group on the VLAN where the Host is included.
After check the membership of the VLAN, if the member for the Multicast Group does not exist anymore, it is removed from the Multicast Membership.
By default, the Multicast Membership Checking duration is 260 seconds.
To change the Leave-timeout of IGMP that the IGMP Querier Router uses, use the following commands in the interface configuration mode.

Command	Description
ip igmp leave-timeout seconds	Set the IGMP member leave timeout. (Default: 260 sec)
no ip igmp leave-timeout	Set the configured IGMP Leave Timeout as default.

```
Router# configure terminal
Router(config)# interface vlan1
Router(config-if-vlan1)# ip igmp leave-timeout 30
```

IGMP Member checking interval

If a IGMP Querier Router receives an IGMP Leave message from a host leaving specific Multicast Group, it checks multicast membership to see if there is other hosts registered to other Multicast Group in the VLAN that Host belongs,

The IGMP Query meesage to be sent to check the Multicast Membership is sent to the all-system-group-address, 224.0.0.1 with TTL configuration of 1.

The default interval for sending specific IGMP Query message is 2 seconds, To change the member-checking-interval, please use the following commands in the interface configuration mode.

Command	Description
ip igmp member-checking-interval seconds	Specify the IGMP member checking interval. (Default: 2 sec.)
no ip igmp member-checking-interval	Set the IGMP member checking interval to the default.

```
Router# configure terminal
Router(config)# interface vlan1
Router(config-if-vlan1)# ip igmp member-checking-interval 1
```

IGMP Version Modification

The default is IGMPv2 but if subnet host does not support IGMPv2, set as IGMPv1 because all systems of subnet should support the same version.

To modify IGMP version that router uses, use the following command in the Interface Configuration mode.

Command	Description
ip igmp version {**2** | 1}	Choose the IGMP version that router uses

Router (config-if-vlan1)**# ip igmp version 2**

IGMP Querier Timeout

If the current Querier in the subnet stops, router sets Timeout until replaceing interface queier. By default, the router waits twice as scheduled by IP UGMP Qyert-interval. If no query message comes, the router performs as Querier. This feature is available with IGMPv2.
The IGMP Non-Querier Router carries IGMP Querier for Multicast Membership, if failed in receiving the IGMP Query message from the IGMP Querier Router for the specified Querier Timeout. This feature is available with IGMPv2.

By default, the Multicast router waits for double the time of query interval value set by the **ip igmp query-interval**.

Command	Description
ip igmp querier-timeout seconds	Specify the SIGMP Querier timeout (Default : 255 sec.)
no ip igmp querier-timeout	Set the preset IGMP Querier timeout as default.

```
Router# configure terminal
Router(config)# interface vlan1
Router(config-if-vlan1)# ip igmp querier-timeout 300
```

IGMP Maximum Query Response Time

By default, the maximum query response time notified to the IGMP by the Query message is 10 seconds.

The change of this value is possible only when the router is using IGMPv2. If the Host receives IGMP query message, it sends the report message at any time within the maximum query response time preset in the query message. In this way, the IGMP report can be distributed to be sent. Therefore by adjusting this value, the flooding of multicast traffic in the Sub-Network can be tuned.
The range of Maximum Query Response Time is 1 ~ 25 seconds, and to change the Maximum query response time, use the following commands in the interface configuration mode.

Command	Description
ip igmp query-max-response-time seconds	Specify the maximum-query-response-time for IGMP query. (Default : 10 sec.)
no ip igmp query-max-reposnse-time	Set the preset query-max-response-time as default.

```
Router# configure terminal
Router(config)# interface vlan1
Router(config-if-vlan1)# ip igmp query-max-response-time 5
```

Configure PIM-SM Functionality

PIM-SM v2 includes the following improvements compared to PIM-SM v1.

- bootstrap router (BSR) provides fault-tolerant automatic RP discovery and distribution mechanism, which allows routers to do group-to-RP mapping without addition setting.
- Various address family can be flexibly encoded for PIM Join/Prune message.
- PIM packets are no longer included in the IGMP packet.

PIM-SM uses BSR to find RP-set information for each group prefix for all the routers in the PIM-SM domand and advertise it.
To prevent “Single point of failure”, many candidate BSRs can be set in the PIM-SM domain. The BSR is selected automatically out of candidate BSRs. bootstrap message is used to identify the BSR with highest priority. The router selected as BSR notifies all the routers in the PIM domain of its being BSR.
The routers selected as Candidate RP notifies the range of group that it will cover to the BSR in unicast. BSR includes this information to the bootstrap message, and sends this message to all the PIM routers in the domain. All the routers can identify RP for specific multicast group based on this information. As long as the router receives the bootstrap message, the router gets the current RP map.

PIM-SM Assert Metric

In Multi-Access Network, parallel Multicast Routing Paths can exist as Multicast Packet Originator or RP. In this network, there can be multicast group member that receives duplicated same packets from many Multicast Routers.
To solve this problem, PIM-SM uses the PIM-SM Assert message to decide the specified Assert Router.
If all the Multicast Routers are using the same unicast protocol, the router with best metric is specified as an Assert Router. For example, if all the routers are using RIP, the router with the least number of hops will be selected, and if the metric is same, the router with the highest IP address will be selected.
The default Metric for this Assert is 0xFFFFFFFF, and the change of configuration runs on the interface configuration mode. To change the Assert Metric, please use the following commands in the interface configuration mode.

Command	Description
ip pim assert-metric Metric Value	Specify the metric of Assert message. (Default : 0xFFFFFFFF)
no ip pim assert-metric	Set the current Assert Metric to the default.

```
Router# configure terminal
Router(config)# interface vlan1
Router(config-if-vlan1)# ip pim assert-metric 10
```

PIM-SM Assert Preference

The default value of Metric Preference for Assert is 0x7FFFFFFF, and the router with the biggest Preference becomes the Assert Router.
To change the Metric Preference, use the following commands in the interface configuration mode.

Command	Description
ip pim assert-preference Preference Value	Specify the Metric Preference of Assert message (Default : 0x7FFFFFFF)
no ip pim assert-preference	Set the current Metric Preference to the default.

```
Router# configure terminal
Router(config)# interface vlan1
Router(config-if-vlan1)# ip pim assert-Preference 10
```

PIM-SM BSR Border

This function is used to block the interface from receiving from or sending bootstrap router (BSR) messages. To configure BSR Border, use the following command in the interface configuration mode.

Command	Description
ip pim bsr-border	Block the interface from receiving from or sending the BSR message.
no ip pim bsr-border	Unblock the interface from receiving from or sending the BSR message.

```
Router# configure terminal
Router(config)# interface vlan1
Router(config-if-vlan1)# ip pim bsr-border
```

PIM-SM JoinPrune Interval

Multicast Router sends PIM-SM JoinPrune message to the upstream Multicast Router in the routing path of SPT or RPT to keep Multicast Membership and keeps sending Multicast Traffic. The default transmission interval of PIM-SM JoinPrune message is 60 seconds. To change the transmission interval of PIM-SM JoinPrune message, use the following commands in the interface configuration mode.

Command	Description
ip pim jp-interval Seconds	Set the transmission interval of PIM-SM JoinPrune message (Default : 60 seconds)
no ip pim jp-interval	Set the current transmission interval of JoinPrune message as the default value.

```
Router# configure terminal
Router(config)# interface vlan1
Router(config-if-vlan1)# ip pim jp-interval 30
```

PIM-SM mcache check interval

This function is to check whethere there is flooding of Multicast Traffic at the specified interval. If there is no Multicast Traffic, it delets Multicast Entry from the Multicast Cache, and updates Multicast Membership Entry.

The default interval for checking Multicast Cache is 110 seconds.
To change the Multicast Cache Check interval, use the following commands in the interface configuration mode.

Command	Description
ip pim mcache-check-interval Seconds	Set the Multicast Cache Check interval. (Default : 110 seconds)
no ip pim mcache-check-interval	Set the current Multicast Cache Check interval as the

	default value.

```
Router# configure terminal
Router(config)# interface vlan1
Router(config-if-vlan1)# ip pim mcache-check-interval 220
```

PIM-SM Neighbor Filter

To filter unwanted PIM-SM protocol messages from the PIM-SM Neighbors that are included in the subnet, use the following commands.

Commands	Description
ip pim neighbor-filter access-list-number	Block PIM-SM protocol message by the specified access-list.
no ip pim neighbor-filter	Release the current neighbor-filter.

```
Router# configure terminal
Router(config)# interface vlan1
Router(config-if-vlan1)# ip pim neighbor-filter 1
```

PIM-SM Register Filtering

The First-Hop Router that received Multicast Packets sends the PIM Register message to the RP to register Multicast Source information. The Multicast Source information that can be registered can be the unwanted source or can be registered in the unwanted group, and the Network operator can limit so that RP or First-Hop Router does not carry out Register Filtering for the specific unwanted source or group.

If the Register Filtering is set, PIM-SM Register message can't be sent to or received from the VLAN Interface. To set the Register Filtering for each group, please use the following commands in the interface configuration mode.

Command	Description
ip pim register-filter-group access-list-number	Block the group registered by the specified access-list.
no ip pim register-filter-group	Disable the preset register-filter.

```
Router# configure terminal
Router(config)# interface vlan1
Router(config-if-vlan1)# ip pim register-filter-group 1
```

To set the Register Filtering for each source, use the following commands in the interface configuration mode.

Command	Description
ip pim register-filter-source access-list-number	Blocks the source registered by the specified access-list.
no ip pim register-filter-source	Disable the preset register-filter.

```
Router# configure terminal
Router(config)# interface vlan1
Router(config-if-vlan1)# ip pim register-filter-source 1
```

PIM-SM Whole Packet Checksum

The router located at the First-Hop that received Multicast packets sent from the Multicast Originator includes the packets in the PIM-SM Register message and send them to RP through unicast routing. The RP that received this PIM-SM Register message sends the multicast packets included in the message to the Multicast Membership Entry.
In RFC standard, the checksum of PIM-SM Register message calculate Header part only, but in case of CISCO router, it calculates whole Register message.
So to interwork with CISCO routers, the calculation of Checksum should be based on the entire message.
To set the Whole Packet Check, use the following commands in the interface configuration mode.

Command	Description
ip pim whole-packet-checksum	Set the Interface to work with CISCO router.
no ip pim whole-packet-checksum	Disable the preset whole-packet-checksum.

```
Router# configure terminal
Router(config)# interface vlan1
Router(config-if-vlan1)# ip pim whole-packet-checksum
```

Candidate BSR

If a router can work as a candidate BSR, it should be connected to the Backbone of the network.
To set the router as a Candidate BSR, please use the following commands in the global configuration mode.

Command	Description
ip pim bsr-candidate ifname [hash-mask-length] [priority]	Set the router work as a BSR candidate.
no ip pim bsr-candidate ifname	Disable the preset BSR candidate.

```
Router(config)# ip pim bsr-candidate vlan1 32 100
Router# show ip pim bsr-router
This system is a ACTIVE BSR.
BSR address : 100.1.1.254 Priority : 0 Hash-Mask-Length : 4
Start-Time : 00:03:17 Next Bootstrap in 00:00:44
```

Candidate RP

If a router can work as a candidate RP, it should be connected to the Multicast Backbone of the network. RP can provide service for entire IP Multicast address space or for part of it. Candidate RP sends candidate RP advertisement message to the BSR.
To set the router as a Candidate RP, please use the following commands in the global configuration mode.

Command	Description
ip pim rp-candidate ifname [rp-priority] [access-list-number]	Set the router to work as a RP candidate.
no ip pim rp-candidate ifname	Disable the preset RP candidate.

```
Router(config)# access-list 1 permit 224.1.1.0 255.255.255.0
Router(config)# access-list 1 permit 224.2.2.0 255.255.255.0
Router(config)# ip pim rp-candidate lo0 10 1
Router(config)# ip pim rp-candidate lo0 20 2
Router# show ip pim rp
SET of Rendezvous Point(RP) Informations.
Group : 224.1.1.0 MaskLen : 24 Priority : 10 Holdtime : 150 Group : 224.2.2.0 MaskLen : 24 Priority : 20
```

```
Holdtime : 150
Next Cand_RP_Advertisement in 00:00:44
```

Static RP

This function is used to specify an interface of a specific Multicast Router as a RP interface in the network environment where candidate RP and BSR can't be set.
The information of Static RP is not included in the Bootstrap message, and the RP information of the received Bootstrap always gets the priority higher than the information of the Static RP.
To configure the information of Static RP to the router, use the following commands in the global configuration mode.

Commands	Description
ip pim rp-address address access list number	Set the Static RP information to the router.
no ip pim rp-address address access list number	Disabled the preset Static RP information.

```
Router(config)# access-list 1 permit 224.1.1.0 255.255.255.0
Router(config)# ip pim rp-address 200.1.1.254 1
Router# show ip pim rp
SET of Rendezvous Point(RP) Informations.
RP addr : 200.1.1.254
Group : 224.1.1.0 MaskLen : 24 Priority : 196 Holdtime : 65535(Exp:18:12:15)
```

Static Group

When IGMP and PIM-SM join to the Multicast membership entry, Join Delay Time happens. The Static Group can make the traffic transfer to the Local Sub-Network faster by receiving the Multicast Traffic in advance from the First-hop-Router that is connected to RP or Server to the router with Static Group set.
To set Static Group to the router, use the following commands in the global configuration mode.

Commands	Description
ip pim static-group <multicast-address>	Set the Static Groupinformation to the router.
no ip pim static-group <multicast-address>	Disable the preset Static Group information.

Commands	Description
ip pim static-group <multicast-address> to <count>	Set the Static Group as many as the count.
no ip pim static-group <multicast-address> to <count>	Disable the Static Group as many as the count.

```
Router(config)# ip pim static-group 224.1.1.1
Router# show ip mroute
IP Multicast Routing Table
Timers: Uptime/Expires
Flags : C - Directly Connected Host, L - Local(Router is member)
P - Pruned All, F - Register
J - Join SPT, R - RP Bit
X - Proxy Join Timer flag
Interface state: Interface, Next-Hop, State/Mode
```

```
(*, 224.1.1.1), 00:00:02/00:03:01, RP 192.168.1.254, flags: SRX
Incoming interface: vlan10, RPF nbr 10.1.1.2 STATIC-GROUP
Outgoing interface list: Null
(20.1.1.254, 224.1.1.1) 00:00:02/00:03:01, RP 192.168.1.254, flags: S
Incoming interface: vlan10, RPF nbr 10.1.1.2
Outgoing interface list: Null

total (*, G) : 1, (S, G) : 1
```

Static Join

There are times when Multicast Traffic should be sent even to the network without any member registered at the Multicast Membership depending on the environment of Multicast Network.
In this case, the VLAN interface of the network to which the Multicast Traffic should be sent can be set as Static Join to forward the Multicast Traffic continuosly without checking the existence of Member.
To set Static Join to the router, use the following command in the global configuration mode.

Commands	Description
ip pim static-join multicast-address IFNAME	Set the Static Joininformation to the router.
no ip pim static-join multicast-address IFNAME	Cancel the Static Join information.

Commands	Description
ip pim static-join multicast-address IFNAME to <count>	Set the Static Joininformation to the router up to the specified count.
no ip pim static-join multicast-address IFNAME to <count>	Cancel the Static Joininformation to the router up to the specified count.

```
Router(config)# ip pim static-join 224.1.1.1 vlan20
Router# show ip mroute
IP Multicast Routing Table
Timers: Uptime/Expires
Flags : C - Directly Connected Host, L - Local(Router is member)
P - Pruned All, F - Register
J - Join SPT, R - RP Bit
X - Proxy Join Timer flag
Interface state: Interface, Next-Hop, State/Mode

(*, 224.1.1.1), 00:00:02/00:03:01, RP 192.168.1.254, flags: SRX
Incoming interface: vlan10, RPF nbr 10.1.1.2
Outgoing interface list:
      vlan20, Forward/Sparse, 00:00:15/18:12:15 STATIC-JOIN
(20.1.1.254, 224.1.1.1) 00:00:02/00:03:01, RP 192.168.1.254, flags: S
Incoming interface: vlan10, RPF nbr 10.1.1.2
Outgoing interface list:
      vlan20, Forward/Sparse, 00:00:15/18:12:15
total (*, G) : 1, (S, G) : 1
```

Static Multicast Route Path

PIM-SM is work based on Unicast Routing Protocol. But depending on Network environment or operation of router, when specifying Route Path in the path other than Unicast Routing Protocl for specific Multicast Group or Multicast Server, use the following commands in the global configuration mode for Multicast Route Path.

The Multicast Route Path is valid only in PIM-SM, and has priority than Unicast Routing Path.

Command	Description
ip mroute path <address> <neighbor-address>	Set the multicast route RPT/SPT pathinformation to the router.
no ip mroute path <address> <neighbor-address>	Disable the preset multicast route RPT/SPT path information.

```
Router(config)# ip mroute path 10.1.1.254 20.1.1.1
Router # show ip mroute path
Codes: S - Multicast Route Path, G - Multicast Group Route Path
S> 10.1.1.254/32 via 20.1.1.1, vlan20
```

RPF Load-balance

If there is more than one RPF interfaces with same metric for RPT or SPT, PIM-SM can receive the Multicast Traffic from the upstream neighbor by distributing by each Group.
If this RPF Interface is specified as Load-balance, it can increase the efficience of bandwidth by receiving the Multicast Traffic in many interfaces separately.
To configure this function, please use the following commands in the global configuration mode.

Command	Description
ip pim rpf load-balance	Set the RPF Load-balance to the router.
no ip pim rpf load-balance	Disable the preset RPF Load-balance information.

```
Router(config)# ip pim rpf load-balance
Router(config)#
```

IP Multicast Routing Monitoring Commands

Command	Description
show ip igmp groups	Show the Multicast group at which hosts are registered.
show ip igmp interface	Show the information related with multicast of Interfaces.
show ip mroute	Show the Multicast Routing Table.
show ip mroute path	Show the specified Multicast Routing path.
show ip pim interface	Show the information of interfaces in which PIM is set.
show ip pim neighbor	Show the PIM neighbors.
show ip pim bsr-router	Show the BSR router information.
show ip pim rp	Show the RP information.
show ip pim rp-hash	Show RP-HASH information.

Chapter 9. Routing Protocol

This chapter describes the IP unicast routing protocols available in P8824XG. This chapter assumes that the users are familiar with IP unicast routing. If you are not familiar with IP unicast routing, please refer to the following documents.

- RFC 1058 — Routing Information Protocol (RIP)
- RFC 1256 — ICMP Router Discovery Messages
- RFC 2453 — RIP Version 2
- RFC 2328 — OSPF Version 2
- RFC 1771 — BGP Version 4

Routing Protocol Overview

P8824XG supports Routing Information Protocol (RIP) and Open Shortest Path First (OSPF) for IP unicast routing protocols, and also BGP4 (RFC 1771) for Inter Domain Routing.

RIP is one of distance-vector protocols based on Bellman-Ford (or distance-vector) algorithm. The Distance-vector algorithm has been used for many years and is widely deployed and understood.

OSPF is one of link-state protocols based on Dijkstra link-state algorithm. OSPF is a newer Interior Gateway Protocol (IGP) and solved a number of problems associated with using RIP in today's complex networks.

BGP is a protocol to receive/send routing information among Management Domain (Autonomous System: AS), and manages routing among domains unlike RIP and OSPF. P8824XG switch supports BGP-4.

RIP vs OSPF

The distinction between RIP and OSPF lies in the fundamental differences between distance-vector protocols and link-state protocols. Using a distance-vector protocol, each router creates a unique routing table from summarized information obtained from neighboring routers. Using a link-state protocol, every router maintains an identical routing table created from information obtained from all routers in the autonomous system. Each router builds a shortest path tree, using itself as the root.

The biggest advantage of using RIP is that it is relatively simple to understand and implement, and it has been the *de facto* routing standard for many years.

RIP has a number of limitations that can cause problems in large networks, including the following:

- A limit of 15 hops between the source and destination networks
- A large amount of bandwidth taken up by periodic broadcasts of the entire routing table
- Slow convergence
- Routing decisions based on hop count; no concept of link costs or delay
- Flat networks; no concept of areas or boundaries

OSPF offers many advantages over RIP, including the following:

- No limitation on hop count
- Route updates multicast only when changes occur
- Faster convergence
- Support for load balancing to multiple routers based on the actual cost of the link
- Support for hierarchical topologies where the network is divided into areas

The details of RIP and OSPF are explained later in this chapter.

RIP overview

RIP is the Interior Gateway Protocol (IGP) first used in Advanced Research Projects Agency Network (ARPAnet) since 1969. RIP was primarily intended for use in homogeneous networks of moderate size.

To determine the optimal path to a distant network, the router using RIP always selects the path with the least number of hops to the destination. Each router in the selected routing path is considered to be one hop

Routing Table

The routing table in a router using RIP has the entries of all the known destination networks. Each routing table entry contains the following information.

- IP address of destination network
- Metric (Hop count) to destination network
- IP address of the next router
- Timer that records the time after the entries was last updated.

The router exchanges the update messages with each directly-connected neighbor routers every 30 seconds (default value), or if there is change to the overall routed topology (also called *triggered updates*). When there is no update message from the neighbor routers within the route timeout period (default: 180 seconds), the router assumes that the connection with the neighbor routers is no more valid.

Route Advertisement of VLANs

VLANs that are configured with an IP address, but are configured to not route IP or are not configured to run RIP, do not have their subnets advertised by RIP. Only those VLANs that are configured with an IP address and are configured to route IP and run RIP have their subnets advertised.

RIP Version 1 vs. RIP Version 2

A new version of RIP, RIP version 2, expands the functionality of RIP version 1 to include the following:

- Variable-Length Subnet Mask (VLSMs)
- Next-hop address
  Support of next-hop address enables path optimization in certain environments.
- Multicasting
  RIP version 2 packets can be multicast instead of being broadcast, reducing the load on hosts that do not support routing protocols

OSPF overview

OSPF is a link-state routing protocol that distributes routing information among the routers in one IP domain (*autonomous system* (AS)). In a link-state routing protocol, each router keeps database of autonomous system topology. Each participating router has an identical database maintained from the perspective of that router.

From Link-state DB (LSDB), each router generates the shortest path tree where it is root. This shortest path tree provides the paths to each destination in AS. If there are many paths for a destination and they cost the same, traffic can be distributed to all these paths. The path cast is expressed in a metric.

Link-state Database

When initialized, each router sends the Link State Advertisement (LSA) for its interface. LSAs are collected by each router and saved in LSDB of each router. OSPF uses Flooding to distribute LSAs between routers. Any changes in routing information are sent to all the routers in the network. All the routers in one area have one LSDB that is exactly the same. The following table describes LSA type numbers.

Table 48. LSA Type number

Type Number	Description
1	Router link
2	Network link
3	Summary link
4	AS summary link
5	AS external link
7	NSSA external link

Areas

In OSPF, parts of network can be grouped by area. The topology in one area is hidden from others in the autonomous system. Hiding the information enables a significant reduction in LSA traffic, and reduces the computations needed to maintain the LSDB. The routing within an area is determined by the topology of the area.

OSPF defines the following three types of routers.

- **Internal Router (IR)**
  An internal router has all of its interfaces within the same area.

- **Area Border Router (ABR)**
  The router that has interfaces in many areas, ABR must exchange the summary advertisement with other ABRs.

- **Autonomous System Border Router (ASBR)**
  ASBR works as the gateway between OSPF and other routing protocol, or other autonomous systems.

AREA 0

Any OSPF network that contains more than one area is required to have an area configured as area 0, also called the *backbone*. All the areas in autonomous system must be connected to the backbone. When you design a network, you have to start from area 0 and extend the network to other areas.

The backbone allows summary information to be exchanged between ABRs. Every ABR hears the

area summaries from all other ABRs. The ABR then forms a picture of the distance to all network outside of its area by examining the collected advertisements, and adding in the backbone distance to each advertising router.

Stub areas

OSPF allows certain areas to be configured as *stub areas*. A stub area is connected to only one other area and contains a single exit point. The area that connects to a stub area can be the backbone area. All routing out of a stub area is based on default routes. Stub areas are used to reduce memory and computation requirements on OSPF routers.

Virtual links

In the situation when a new area is introduced that does have a direct physical attachment to the backbone, a *virtual link* is used. A virtual link provides a logical path between the ABR of the disconnected area and the ABR of the backbone. A virtual link must be established between two ABRs that have a common area, with one ABR connected to the backbone.

Route Redistribution

RIP and OSPF can be enabled simultaneously on the switch. Route redistribution allows the switch to exchange routes, including static routes, between the two routing protocols.

Notice Although RIP and OSPF can be run simultaneously on the switch, you cannot apply them both to the same VLAN..

Border Gateway Protocol (BGP)

The Border Gateway Protocol (BGP) is an inter-autonoumous ystem routing protocol, and the primay function of a BGP speaking system is to exchange routing information with other BGP systems.

The first version of BGP was announced in June 1989 as RFC-1105; a second version was announced in June 1990 as RFC-1163; a third one in October 1991 as RFC-1267; the fourth version was announced in July 1994 as RFC-1654, and revised in March 1995 as RFC-1771. These versions are often referred to as BGP-1, BGP-2, BGP3, and BGP-4. BGP-4 has been in use in the Internet and is supported in 7012G switch.

A key element of the BGP-4 design is the support for the CIDR (Classless Inter-Domain Routing) that was introduced to mitigate the rapid consumption of network address and to combat the explosion of the routing tables.

BGP Overview

A major design choice of BGP is that the protocol run over TCP. Exchanging connectivity information over a reliable transport protocol has a number of advantages and possibly a couple of drawbacks.

Delegating all “error control” functions to TCP makes the protocol much simpler;

BGP protocol message has the 19 bytes of the fixed-length header, the last byte of the header is the packet type. The packet types are as follows.

1. OPEN
2. UPDATE
3. NOTIFICATION
4. KEEPALIVE

(1) Initial Exchange

The switches that support BGP normally wait for BGP connections on port 179. A switch that wants to establish an association will first open a TCP connection toward that port on the peer router. Once the connection has been set, each side sends an OPEN message to negotiate the association’s parameters.
The parameters of the OPEN message are the BGP version number, the AS number of the sending router, a hole-time, identifier, and a set of options.
The identifier field carries one of the IP interface addresses of the BGP switches. Each switch must choose one identifier and use it for all BGP associations, regardless of he interface used to transmit the BGP packets.

(2) Update

Once the connection has been established, the BGP stations will start exchanging “updates”, which

include a set of path attributes and a list of reachable networks. When an update is received, the path is compared to the current path used for reaching the advertised network. If the new path is shorter than the old path, the routing tables are modified and corresponding updates are sent to the BGP neighbors.

(3) Keep-Alive Features

As was the case with OSPF, there is a need for BGP switches to constantly monitor the connectivity of their neighbors. In order to obtain a sufficient rate of probing, the BGP stations will periodically send KEEPALIVE messages. These messages are composed simply of a 19-byte BGP header. The hold-time is negotiated during the opening exchange and its default is 90 seconds.

(4) Error Notification

If a BGP station receives an ill-formatted or otherwise erroneous message, or if it fails to receive any message during a period longer than the hold time, it will report the error to its peer by sending a nofification message, then gracefully close the TCP connection.

RIP Configuration

Commands

The following commands are used for RIP configuration.

1) Enable a RIP routing process whitch places you in configuration mode.

router rip

2) Assiciate a network with a RIP routing process.

network ip-address

With this command, the network with RIP is set. For example, if RIP is set in 192.168.0.0/24 network, all address between 192.168.0.0 and 192.168.0.255 are operated by RIP. And RIP packet is transmitted / received through this interface

The following show commands to configure RIP. After enabling RIP, set the items as follows and run RIP protocol.

default-information originate

- To generate a default route into Routing Informaton Protocol (RIP), use the the **default-information originate** command in configuration mode.
- Control that RIP specifies one default route.

default-metric <*1-16*>

- There are times when a router runs one or more IP routing protocols. Each routing protocol has different metrics. For example, RIP has hop count and OSPF has dimensionless cost. If one routing protocol intends to decide a path by using another routing protocol, it has to convert the route metric to a different routing protocol.
- The command for metric conversion is default-metric. Select and define the value of redistribute routes within <1-16>.

distance <*1-255*> [*A.B.C.D/M*] [*WORD*]}

- This command is used to adjust administrative distance. The range of this value is 1~255. The default of RIP is 120 and if one or more routing protocols are working in one router system, this administrative distance value is used.
- If RIP and OSPF routing protocol are running in a router, each path is decided with OSPF not RIP. Because OSPF distance value is 110 and RIP is 120, the router selects the path with smaller distance value. When necessary, you can adjust the value. That is, give a smaller value than OSPF to RIP so that RIP path can be set.
- You can change the distance of some particular network by setting A.B.C.D/M network. In this case, you can set an access list.

distribute-list {*WORD1* | prefix *WORD2*} {in | out} [*WORD3*]

- This command is used for filtering in case of incoming or outgoing routing update.

- WORD1 : Access list name
- WORD2 : IP prefix-list name
- WORD3 : Interface name
- In : Filter incoming routing updates
- Out : Filter outgoing routing updates

neighbor *A.B.C.D*

- This command is used to specify the address of the neighbor router

network *A.B.C.D/M*

- This command is used to specify the IP network that enables rip routing.

no

- This command is used before each command to clear the commands described above or to return values to default.

offset-list *WORD* { **in** | **out** } **<***0-16***>** [*ifname*]

- This command is used to increase or decrease the metric value of RIP.
- This command is used to adjust metric and hop count when the router updates incoming or outgoing RIP by using standard list.
- WORD : Access list name
- In: Perform offset for incoming update.
- Out: Perform offset for outgoing update.
- <0-16>: offset value

passive-interface *IFNAME*

- This command is used to control the routing update in the interface specified with IFNAME.
- If you apply this command to a certain interface of the router, the interface does not advertise the outgoing path, but keeps receiving the routing information.

redistribute ospf [{metric <*0-16*>} | {route-map *WORD*}]

- This command is used to redistribute RIP routing information to OSPF domain
- WORD: route-map entry name

route A.B.C.D/M

- This command is used to set RIP static route.

timers basic < 1-4294967295> < 1-4294967295> < 1-4294967295>

- This command is used to adjust the timer value in this protocol.

- The first value is the value of routing table update timer and the default value is 30. The unit is second.
- The second value is the routing information timeout timer value and the default is 180. The unit is second.
- The third value is the garbage collection timer value and the default is 120. The unit is second.

version *<1-2>*

- This command is used to set the running version of RIP protocol. The default is Version2.

RIP Configuration

Let us take a look at an example of RIP protocol configuration from the following network configuration diagram of the following figure.

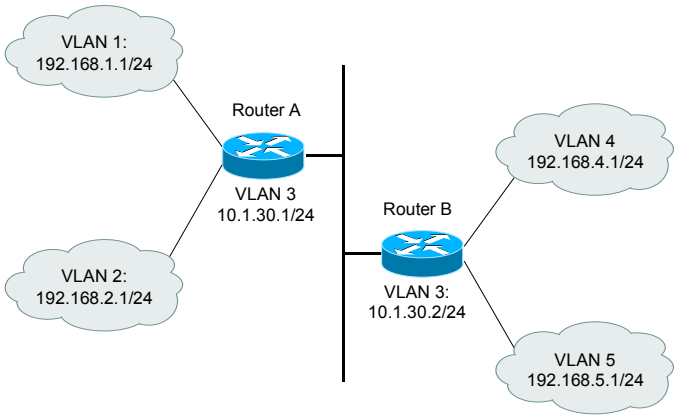


Figure 16. RIC Network Configuration

Table 49. RIP Network Configuration Example and Diagram

Router A	Router B
vlan1 192.168.1.1/24	vlan4 192.168.4.1/24
vlan2 192.168.2.1/24	vlan5 192.168.5.1/24
vlan3 10.1.30.1/24	vlan3 10.1.30.2/24

The following commands are used to enable RIP protocol for each interface.

Router A configuration

```
Router A(config)# router rip
Router A(config-rip)# network 192.168.1.1/24
Router A(config-rip)# network 192.168.2.1/24
Router A(config-rip)# network 10.1.30.1/24
Router A(config-rip)# end
Router A# show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF,
   B - BGP, > - selected route, * - FIB route
C>* 10.1.30.0/24 is directly connected, vlan3
C>* 192.168.1.0/24 is directly connected, vlan1
C>* 192.168.2.0/24 is directly connected, vlan2
R>   192.168.4.0/24 [120/1] via 10.1.30.2, vlan3, 00:01:42
R>* 192.168.5.0/24 [120/1] via 10.1.30.2, vlan3, 00:01:42
Router A#
```

Router B configuration

```
Router B(config)# router rip
Router B(config-rip)# network 192.168.4.1/24
```

```
Router B(config-rip)# network 192.168.5.1/24
Router B(config-rip)# network 10.1.30.2/24
Router B(config-rip)# end
Router B# show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF,
   B - BGP, > - selected route, * - FIB route
C>* 10.1.30.0/24 is directly connected, vlan3
R>* 192.168.1.0/24 [120/1] via 10.1.30.1, vlan3, 00:02:13
R>* 192.168.2.0/24 [120/1] via 10.1.30.1, vlan3, 00:02:13
C>* 192.168.4.0/24 is directly connected, vlan4
C>* 192.168.5.0/24 is directly connected, vlan5
Router B#
```

Distance Configuration

Let us change the distance value (RIP default is 120) of Router B in <Figure 16> network diagram to 130 with distance command.

```
Router B(config)# router rip
Router B(config-rip)# distance 130
Router B(config-rip)# end
Router B# show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF,
   B - BGP, > - selected route, * - FIB route

C>* 10.1.30.0/24 is directly connected, vlan3
R>* 192.168.1.0/24 [130/1] via 10.1.30.1, vlan3, 00:02:13
R>* 192.168.2.0/24 [130/1] via 10.1.30.1, vlan3, 00:02:13
C>* 192.168.4.0/24 is directly connected, vlan4
C>* 192.168.5.0/24 is directly connected, vlan5
Router B#
```

You can see the distance value is changed from 120 to 130 in the above. Now, we are to change the distance value of a certain network. You can use the following method. Return the values to the original network state and perform the following configuration works again.

You can reset the distance values as follows.

```
Router B(config)# router rip
Router B(config-rip)# no distance 130
Router B(config-rip)# distance 130 ?
A.B.C.D/M    IP source prefix
<cr>
Router B(config-rip)# distance 130 192.168.0.0/16 ?
WORD    Access list name
<cr>
Router B(config-rip)# distance 130 192.168.0.0/16 1
Router B(config-rip)# end
```

The intention of the above configuration is to set the distance value of 192.168.1.0 to 130 and that of 192.168.2.0 to 120.
After you finish the above configuration, you have to start the access list configuration to apply the distance values.

```
Router B(config)# access-list 1 permit 192.168.1.0 255.255.255.0
Router B(config)# end
  Router B# show ip route
  Codes: C - connected, S - static, R - RIP, O - OSPF,
    B - BGP, > - selected route, * - FIB route

  C>* 10.1.30.0/24 is directly connected, vlan3
  R>* 192.168.1.0/24 [130/1] via 10.1.30.1, vlan3, 00:02:13
  R>* 192.168.2.0/24 [120/1] via 10.1.30.1, vlan3, 00:02:13
  C>* 192.168.4.0/24 is directly connected, vlan4
  C>* 192.168.5.0/24 is directly connected, vlan5
  Router B(config)#
```

Distribute-list Configuration

Now, router B wants to delete the path of 192.168.1.0 network that is advertised in router A in the above network example. In this case just follow the steps below. First, apply the distribute-list to RIP process of Router B, and then use the access-list. Set the distribute-list as follows.

1) Deny 192.168.1.0 network coming to Router B by using the access-list.

```
Router B(config)# router rip
Router B(config-rip)# distribute-list 2 in
Router B(config-rip)# end
```

2) Set the access list that denies 192.168.1.0 path. The reason for setting as follows is to deny only the 192.168.1.0 path and permit other paths

```
Router B(config)# access-list 2 deny 192.168.1.0 255.255.255.0
Router B(config)# access-list 2 permit any
Router B# show ip route
  Codes: C - connected, S - static, R - RIP, O - OSPF,
    B - BGP, > - selected route, * - FIB route

  C>* 10.1.30.0/24 is directly connected, vlan3
  R>* 192.168.2.0/24 [120/1] via 10.1.30.1, vlan3, 00:12:15
  C>* 192.168.4.0/24 is directly connected, vlan4
  C>* 192.168.5.0/24 is directly connected, vlan5
  Router B#
```

3) You can see the 192.168.1.0 path from Router A is filtered. With “show ip protocol” command, you can check the use of filtering.

```
Router B# show ip protocols
Routing Protocol is "rip"
  Sending updates every 30 seconds with +/-50, next due in 29 seconds
  Timeout after 180 seconds, garbage collect after 120 seconds
  Outgoing update filter list for all interface is not set
  Incoming update filter list for all interface is 2
  Default redistribution metric is 1
  Redistributing:
  Default version control: send version 2, receive version 2
    Interface     Send   Recv     Key-chain
    vlan322
    vlan422
    vlan522
  Routing for Networks:
    10.1.30.0/24
    192.168.4.0/24
    192.168.5.0/24
  Routing Information Sources:
    GatewayBadPackets BadRoutes   Distance Last Update
    10.1.30.1 0     20    120     00:00:05
  Distance: (default is 120)
    Address Distance   List
    192.168.0.0/16       130   1
Router B#
```

4) Now apply the access list to a case where Router B blocks 192.168.4.0 path from going out to other direction.

```
Router B(config)# router rip
Router B(config-rip)# distribute-list 3 out
Router B(config-rip)# exit
Router B(config)# access-list 3 deny 192.168.4.0 255.255.255.0
Router B(config)# access-list 3 permit any
```

5) You can see that 192.168.4.0 path is not in the routing table of Router A.

```
Router A# show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF,
  B - BGP, > - selected route, * - FIB route

C>* 10.1.30.0/24 is directly connected, vlan3
C>* 192.168.1.0/24 is directly connected, vlan1
C>* 192.168.2.0/24 is directly connected, vlan2
R>* 192.168.5.0/24 [120/1] via 10.1.30.2, vlan3, 00:20:04
Router A#
```

Offset-List Configuration

Now let us increase the metric value of all incoming RIP route to Router A by 2 by using the offset-list.

```
Router A(config)# router rip
Router A(config-rip)# offset-list 4 in 2
Router A(config-rip)# exit
Router A(config)# access-list 4 permit any
Router A(config)# [Ctrl] + [z]
Router A# show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF,
   B - BGP, > - selected route, * - FIB route
C>* 10.1.30.0/24 is directly connected, vlan3
C>* 192.168.1.0/24 is directly connected, vlan1
C>* 192.168.2.0/24 is directly connected, vlan2
R> 192.168.4.0/24 [120/3] via 10.1.30.2, vlan3, 00:06:26
R>* 192.168.5.0/24 [120/3] via 10.1.30.2, vlan3, 00:29:04
  Router A#
```

You can see the metric values of 192.168.4.0 and 192.168.5.0 are increased to 3 in the above. You can also set offset-list for outgoing as in the distribute-list.

Passive-Interface Configuration

When you apply this command to a certain interface of the router, the interface does not advertise outgoing paths. For example, when Router A in the example network sets a passive-interface in vlan3 of Router A, Router A receives all the paths but Router B cannot get any update of the paths that Router A sends to vlan3.

```
Router A(config)# router rip
Router A(config-rip)# passive-interface vlan3
Router A(config-rip)# end
Router A# show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF,
   B - BGP, > - selected route, * - FIB route
C>* 10.1.30.0/24 is directly connected, vlan3
C>* 192.168.1.0/24 is directly connected, vlan1
C>* 192.168.2.0/24 is directly connected, vlan2
R>    192.168.4.0/24 [130/1] via 10.1.30.2, vlan3, 00:14:28
R>* 192.168.5.0/24 [120/1] via 10.1.30.2, vlan3, 00:37:06
Router A#
Router B# show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF,
   B - BGP, > - selected route, * - FIB route
C>* 10.1.30.0/24 is directly connected, vlan3
C>* 192.168.4.0/24 is directly connected, vlan4
C>* 192.168.5.0/24 is directly connected, vlan5
Router B#
```

OSPF Configuration

To use OSPF Routing Protocol, you should enable OSPF. The following shows the procedures.

(1) Use OSPF mode instead of Config mode.

router ospf

(2) Specify the network to enable OSPF protocol and area that OSPF protocol is in.

network ip-address/M area (area-id | area-address)

After enabling OSPF, use the following command and operator can use the proper protocol based on requirements and needs.

Command

The following commands are used for OSPF configuration.

router ospf ☞ This command is used to generate OSPF instance

```
Router# configure terminal
Router(config)# router ospf
Router(config-ospf)# ?
```

The command list after router ospf command execution is as follows.

Table 50. Commands after Router ospf Command Execution

Command	Description
area	OSPF area parameters
auto-cost	Calculate OSPF interface cost according to bandwidth
compatible	OSPF compatibility list
default-information	Control distribution of default information
default-metric	Set metric of redistributed routes
distance	Define an administrative distance
distribute-list	Filter networks in routing updates
end	End configuration mode and return to EXEC mode.
exit	Exit configuration mode or close an active terminal session
Help	Description of the help system
neighbor	Specify neighbor router
network	Enable routing on an IP network
no	Negate a command or set its defaults
ospf	OSPF specific commands
passive-interface	Suppress routing updates on an interface
redistribute	Redistribute information from another routing protocol
refresh	Adjust refresh parameters
router-id	router-id for the OSPF process

timers	Adjust routing timers

The following section will describe the commands of the following table in detail.

area

As below, the area ID can be expressed in a decimal number between 0~4294967295 or in an IP address format such as A. B. C. D.

```
Router(config-ospf)#area ?
<0-4294967295>   OSPF area ID as a decimal value
A.B.C.D          OSPF area ID in IP address format
Router(config-ospf)#
```

The sub commands that are displayed when the area id is given a number (0 in here) are listed in following table.

Table 51. Sub Commands

Command	Description
authentication	Enable authentication
default-cost	OSPF area ID as a decimal value
export-list	Set the filter for networks announced to other areas
import-list	Set the filter for networks from other areas announced to the specified one
range	Configure OSPF area range for route summarization
shortcut	Configure the area's shortcutting mode
stub	Configure OSPF area as stub
virtual-link	Configure a virtual link
auto-cost	Calculate OSPF interface cost according to bandwidth
compatible	OSPF compatibility list
default-information	Control distribution of default information
default-metric	Set metric of redistributed routes
distance	Define an administrative distance
distribute-list	Filter networks in routing updates
end	End configuration mode and return to EXEC mode.
exit	Exit configuration mode or close an active terminal session
help	Description of the help system
neighbor	Specify neighbor router
network	Enable routing on an IP network
no	Negate a command or set its defaults
ospf	OSPF specific commands
passive-interface	Suppress routing updates on an interface
redistribute	Redistribute information from another routing protocol
refresh	Adjust refresh parameters
router-id	router-id for the OSPF process
timers	Adjust routing timers

Each of subcommands in the table is as follows.

- **Authentication**

Authentication is used in the area. You can use a password or encryption.

```
Router(config-ospf)#area 0 authentication
  message-digest   Use message-digest authentication
<cr>
Router(config-ospf)#
```

- Using a password is using <cr> value (Means “enter’.) and you have to use the following command in the related interfaces. Enter the password to use in AUTH_KEY.

Router(config-if-vlan20)# ip ospf authentication-key AUTH_KEY

- If the passwords of the above command are not the same in the connection interfaces of two routers, the routers can get the routing information through the interfaces. That is, the routers can get the routing information of each other. Using encryption is not different from the above method. Only the command is different.

- **default-cost**

  The metric value of the external router that the stub area reports to, the default is 1.

- **export-list**

  This command is used to filter the paths reporting other areas by using the access list.

- **import-list**

  This command is used to filter the paths other areas are reporting by using the access list.

- **range**

  This command is used only in the border router and it provides the representative path to the matching address.

- **shortcut**

  This command is used to set the shortcut mode over the area.z

- **stub**

  This command is used to define Stub area. The following command sets area 2 as stub area. When No-summary is added, no inter-area path comes to this area..

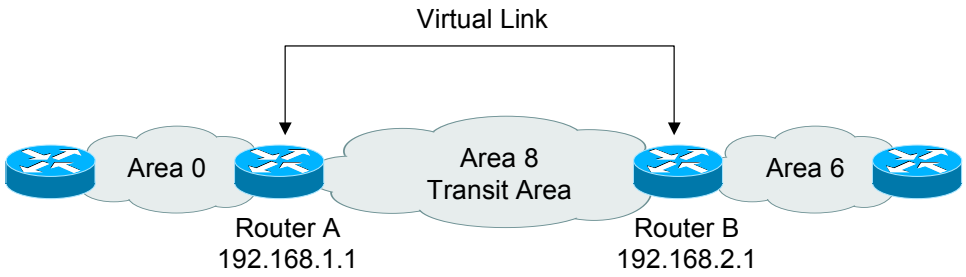
```
Router(config-ospf)#area 2 stub
  no-summary   Do not inject inter-area routes into stub
<cr>
Router(config-ospf)#
```

- **virtual-link**

  This command is used as follows.

area <transit area id> **virtual-link** <remote router id>

<Figure 16> helps your understanding and shows Virtual Link network. Area 6 is connected to the backbone area 0 by using the virtual-link and area 8 by using the transit-area.



Router A : area 8 virtual-link 192.168.2.1
Router B : area 8 virtual-link 192.168.1.1

Figure 17. Virtual Link Network

- **auto-cost**

To calculate OSPF cost of the interface based on the bandwidth, enter the reference bandwidth in the range of <1-4294967> and enter by the unit of Mbps.

- **Compatible**

List of OSPF compatible. There is only rfc1583 now.

- **default-information**

  This command is used that ABR generates and creates Default route (0.0.0.0/0) to one OSPF Area.

default-information originate [always] [metric metric-value]
[metric-type type-value] [route-map map-name]

- **default-metric**

  Select the metric value of the redistributed path between <0-16777214>.

- **distance**

distance <1-255> [A.B.C.D/M] [WORD]}

- This command is used to adjust administrative distance. The range of this value is 1~255. The default of RIP is 120 and if one or more routing protocols are working in one router system, this administrative distance value is used.
- If RIP and OSPF routing protocol are running in a router, each path is decided with OSPF not RIP. Because OSPF distance value is 110 and RIP is 120, the router selects the path with smaller distance value. When necessary, you can adjust the value. That is, give a value smaller than OSPF to RIP so that RIP path can be set..
- You can change the distance of some particular network by setting A.B.C.D/M network.

In this case, you can set an access list.

- **distribute-list**

distribute-list {WORD1 | prefix WORD2} {in | out} [WORD3]

This command is used for filtering in case of incoming or outgoing routing update.

- WORD1 : Access list name
- WORD2 : IP prefix-list name
- WORD3 : interface name
- In : Filter incoming routing updates
- Out : Filter outgoing routing updates

- **neighbor**

neighbor A.B.C.D

- This command is used to specify the address of the neighbor router. 7012G switch can set Hello interval <0-65535> and change priority <0-255>

- **network**

network *A.B.C.D/M* **area** <*area id*>

- This command is used to specify the network to run OSPF unlike RIP.

- **ospf**

In this mode commans are used to specify RFC1583, compatibility, router-id setting.

- **passive-interface**

passive-interface *IFNAME*

- This command is used to control the routing update in the interface specified with *IFNAME*.
- If you apply this command to a certain interface of the router, the interface does not advertise the outgoing path, but keeps receiving the routing information.

- **redistribute**

redistribute (kernel|connected|static|rip|bgp) [metric <0-16777214>] [metric-type (1|2)] [route-map WORD]

- This command is used to distribute RIP routing or static information to OSPF routing domain. The distributed information is OSPF extenal route.

- **refresh**

This command is used to set the cycle of LSA refresh between <10-1800> seconds

- **router-id**

This command is used to set the router ID of the OSPF.

Configuration of Example OSPF Network

Now, let's build up a network using OSPF routing protocol. The following <Figure 17> is the diagram of OSPF network example. You can build up the following OSPF network by using the example.

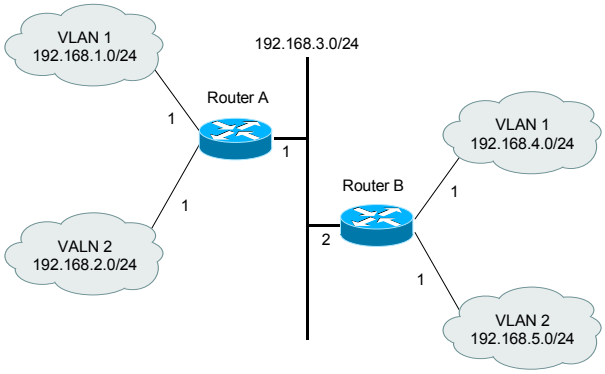


Figure 18. OSPF Network Example

The above figure is Area 0 backbone network (192.168.0.0/24). Now we are to set the network of the above figure with OSPF routing protocol.

1) First generate and start up OSPF instance in the router

```
Router A# config terminal
Router A(config)# router ospf
Router A(config-ospf)#
```

2) Since you have started OSPF routing process, you have to report the neighbor networks of the outer to other networks. That is, Router A reports 192.168.1.0, 192.168.2.0, and 192.168.3.0. For this, first set the network number, network mask, and the area where the network belongs.

```
Router A(config-ospf)# network 192.168.1.0/24 area 0
Router A(config-ospf)# network 192.168.2.0/24 area 0
Router A(config-ospf)# network 192.168.3.0/24 area 0
```

3) Set Router B in the same way as above.

```
Router B# config terminal
Router B(config)# router ospf
Router B(config-ospf)#

Router B(config-ospf)# network 192.168.3.0/24 area 0
Router B(config-ospf)# network 192.168.4.0/24 area 0
Router B(config-ospf)# network 192.168.5.0/24 area 0
```

4) Now, the two routers are all running OSPF routing process. The routing table of the two routers is as follows.

```
Router B# show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF,
   B - BGP, > - selected route, * - FIB route

C>* 192.168.0.0/24 is directly connected, vlan20
O>* 192.168.1.0/24 [110/20] via 192.168.3.2, vlan3, 00:01:31
O>* 192.168.2.0/24 [110/20] via 192.168.3.2, vlan3, 00:01:31
C>* 192.168.3.0/24 is directly connected, vlan3
C>* 192.168.4.0/24 is directly connected, vlan4
C>* 192.168.5.0/24 is directly connected, vlan5
Router B#

Router A# show ip route
Codes: C - connected, S - static, R - RIP, O - OSPF,
   B - BGP, > - selected route, * - FIB route

C>* 192.168.0.0/24 is directly connected, vlan20
C>* 192.168.1.0/24 is directly connected, vlan1
C>* 192.168.2.0/24 is directly connected, vlan2
C>* 192.168.3.0/24 is directly connected, vlan3
O>* 192.168.4.0/24 [110/20] via 192.168.3.1, vlan3, 00:01:04
O>* 192.168.5.0/24 [110/20] via 192.168.3.1, vlan3, 00:01:04
Router A#
```

In the above routing information, there are three directly-connected paths and two paths learned from OSPF in each Router A and B respectively. The information of this routing table can be analyzed as follows.

- [110/20] means the administrative distance is 110 and cost is 20. “directly connected” means the network is directly connected to the interface of the router.
- Via 192.168.3.1 is the middle network that transfers OSPF.
- 00:01:04 means the time past after the path is generated. OSPF does not update the routing table as regularly as RIP.
- Fa3/1 indicates the interface where the packets to the destination network go through.

The cost of OSPF network is the quotient of the bandwidth divided by 100,000,000 (100 Mbps). The interface of each router has the information on the bandwidth. To see the information, use “show interface” command.

```
Router A# show interface vlan3
Name: vlan3
  Type: Fast Ethernet 100Base-FX
  Status: Up 100M Full-Duplex
  Ethernet address 00:07:70:50:00:05
  IP address 192.168.3.1/24 Broadcast 192.168.3.255
```

MTU 1500, Metric 0
Layer2 statistics:
92184 packets input, 7499899 bytes
Received 10 broadcasts, 92144
multicasts
1 CRC, 0 oversize, 0 dropped
1428 packets output, 121516 bytes
Sent 2 broadcasts, 1412 multicasts
Router A#

To disable all the running OSPFs, execute no router command.

Router B(config)# **no router ospf**

If there is only one area as in the above sample network figure, there is no need to use area 0. It is all right using other area number. But if there are more than one areas, there must be area 0.

Route Re-Distribution

Both RIP and OSPF can be started at the same time in one system. Route re-distribution enables the system to exchange routing information between two routing protocols including the static route.

To export paths from OSPF to RIP and from RIP to OSPF, you have to use the configuration functions very carefully. To perform both RIP and OSPF at the same time, first you have to configure the two protocols and then check the operation of each protocol. Then, you can set the network so that the paths can be exported from OSPF to RIP and from RIP to OSPF.

Passive-Interface Configuration

When you apply this command to a certain interface of the router, the interface does not advertise outgoing paths. For example, when Router A in the example network sets a passive-interface in vlan3 of Router A, Router A receives all the paths but Router B cannot get any update of the paths that Router A sends to vlan3.

Router A(config)# **router ospf**
Router A(config-ospf)# **passive-interface** vlan3
Router A(config-ospf)# **end**
Router A# **show ip route**
Codes: C - connected, S - static, R - RIP, O - OSPF,
B - BGP, > - selected route, * - FIB route

C>* 10.1.30.0/24 is directly connected, vlan3
C>* 192.168.1.0/24 is directly connected, vlan1
C>* 192.168.2.0/24 is directly connected, vlan2
O> 192.168.4.0/24 [130/1] via 10.1.30.2, vlan3, 00:14:28
O>* 192.168.5.0/24 [120/1] via 10.1.30.2, vlan3, 00:37:06
Router A#

Router B# **show ip route**
Codes: C - connected, S - static, R - RIP, O - OSPF,
B - BGP, > - selected route, * - FIB route

C>* 10.1.30.0/24 is directly connected, vlan3
C>* 192.168.4.0/24 is directly connected, vlan4
C>* 192.168.5.0/24 is directly connected, vlan5
Router B#

BGP Configuration

BGP configuration includes Basic Configuration and Advanced Configuration. To use BGP protocol, configure the followings.

- Enabling BGP protocol
- BGP neighbor router configuration

Enabling BGP Protocol

To enable BGP Protocol, follow the steps below.

1) Enable BGP Routing
   To enable BGP routing, establish a BGP routing process by using the following commands beginning in global configuration mode.

router bgp <1-65535>

The last number is AS number that is Autonomous System Number given by network operator to distinguish BGP Networks.

2) Flag a network as local to this autonomous system and enter it to the BGP table

network A.B.C.D/M

Neighbor Configuration

Two switches connecting TCP to exchange BGP Routing Information are called peer or neighbor. BGP supports two kinds of neighbors: internal and external. *Internal neighbors* are in the same autonomous system (iBGP Peer); *external neighbors* are in different autonomous systems (EBGP Peer). Normally, external neighbors (eBGP peer) are adjacent to each other and share a subnet, while internal neighbors (iBGP Peer) may be anywhere in the same autonomous system.

To configure BGP neighbors, use the following command in router configuration mode:

neighbor ip-address remote-as number

After configuring BGP and neighbor, default BGP Protocol is run. Network operator sets the following items alternatively.

1) Filtering
2) BGP Attribute configuration
3) Routing policy modification
4) Miscellaneous fuctions

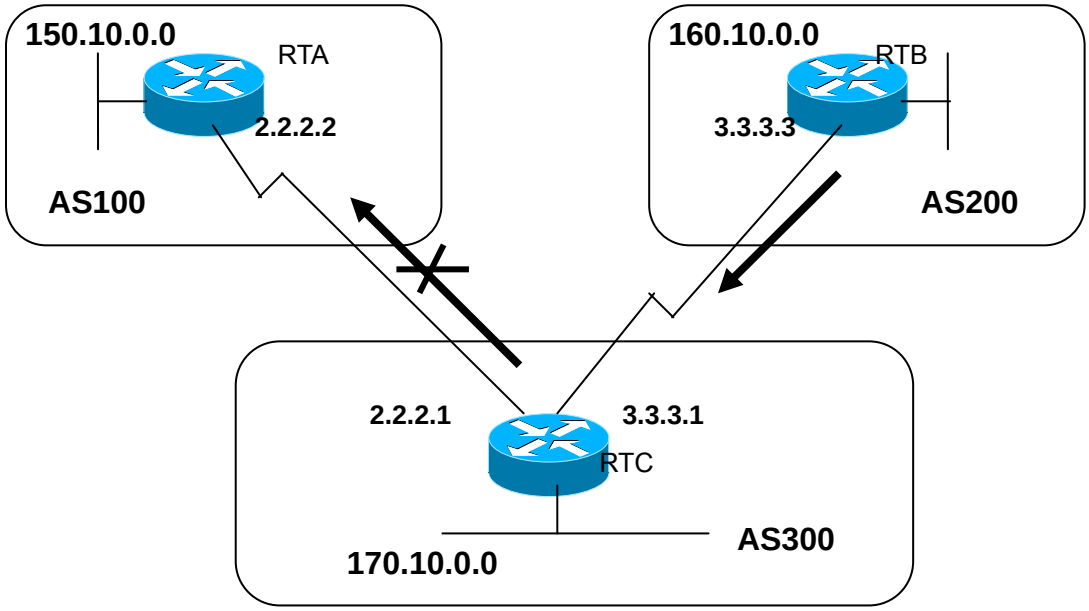
BGP Filtering

BGP update sending/receiving can be managed by filetering functions such as route filtering, path filtering, and community filtering. Even though the functions havethe same results, you need to choose the proper one based on the network configuration.

Route Filtering

To limit routing information that router receives or advertises, it filters BGP based on routing update going/coming to the specific neighbor. The specific Access-list is applied to the Input/Output update to the specific neighbor with the following command.

neighbor {ip-address|peer-group-name} **distribute-list** access-list-number **{in|out}**



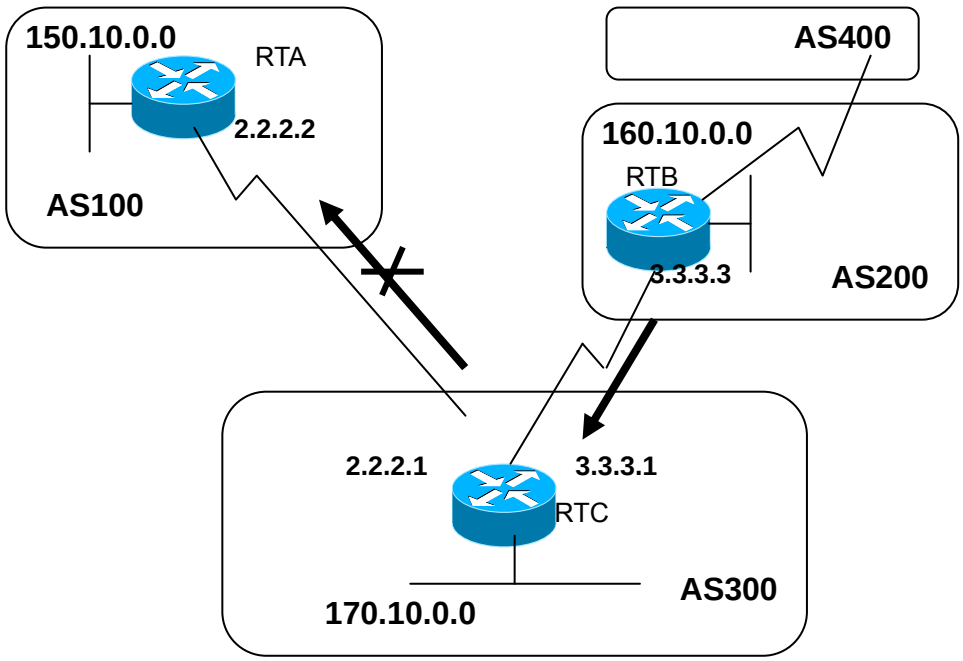
RTB generates network 160.10.0.0 and transmits this information to RTC. If RTC does not transmit it to AS 100, apply Access-list and connection to RTA to filter the information update.

RTC#
router bgp 300
network 170.10.0.0
neighbor 3.3.3.3 remote-as 200
neighbor 2.2.2.2 remote-as 100
neighbor 2.2.2.2 distribute-list 1 out
access-list 1 deny 160.10.0.0 0.0.255.255
access-list 1 permit 0.0.0.0 255.255.255.255
!-- filter out all routing updates about 160.10.x.x

Path Filtering

In addition to filtering routing updates based on network numbers, you can specify an access list filter on both incoming and outbound updates based on the BGP autonomous system paths. To block created information from AS 200 to AS 100, define access-list in RTC with the following command.

ip as-path access-list access-list-number {permit|deny} as-regular-expression
neighbor {ip-address|peer-group-name} filter-list access-list-number {in|out}

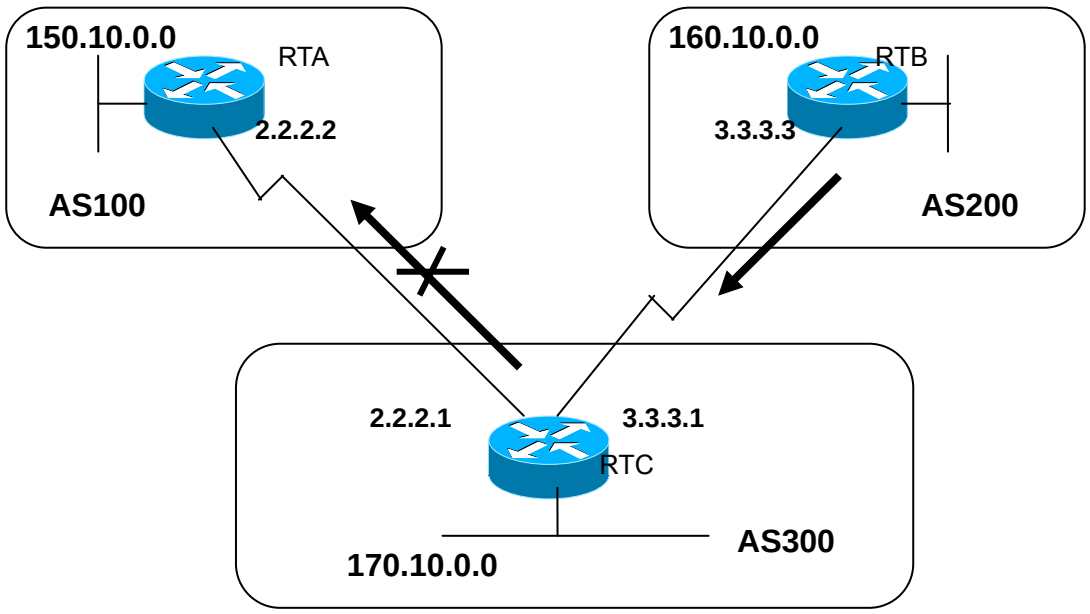


The following shows the configuration that RTC updates 160.10.0.0 to RTA with the Path Filtering.

RTC#
router bgp 300
neighbor 3.3.3.3 remote-as 200
neighbor 2.2.2.2 remote-as 100
neighbor 2.2.2.2 filter-list 1 out
!-- the 1 is the access list number below
ip as-path access-list 1 deny ^200$
ip as-path access-list 1 permit .*

Community Filtering

The *communities* attribute is a way to group destinations into communities and apply routing decisions based on the communities.



To Prevent that RTC Updates Routes Transmitted to Its EBGP Peer

The following shows that RTB sets Community attribute not to update routes from RTB to its dBGP Peer with 'no-export' communit attribute.

RTB#
router bgp 200
network 160.10.0.0
neighbor 3.3.3.1 remote-as 300
neighbor 3.3.3.1 send-community
neighbor 3.3.3.1 route-map setcommunity out
route-map setcommunity
match ip address 1
set community no-export
access-list 1 permit 0.0.0.0 255.255.255.255

Cisco router uses "**neighbor send-community"** command to transmit this attribute to RTC but ubiQuoss Networks system sets this command as a default. So, command 'neighbor 3.3.3.1 send-community' can be canceled, and command 'no neighbor 3.3.3.1 send-community' should be displayed to disable.

RTC does not transmit this information to its external peer RTA when RTC

The following shows the example that RTB adds 100 200 to the community attribute. This value 100 200 is added to the current community value before transmiting to RTC, or replacing the current community value with the value 100 200 when no addtivie command.

```
RTB#
    router bgp 200
    network 160.10.0.0
    neighbor 3.3.3.1 remote-as 300
neighbor 3.3.3.1 route-map setcommunity out

route-map setcommunity
match ip address 2
set community 100 200 additive
access-list 2 permit 0.0.0.0 255.255.255.255
```

Community list specifies the communities used for Route Map Match Gate to set or filter the attribute based on the different community number list.

```
ip community-list community-list-number {permit|deny} community-number
```

The following shows how to define the route map.

```
route-map match-on-community
match community 10
!-- 10 is the community-list number
set weight 20
ip community-list 10 permit 200 300
!-- 200 300 is the community number
```

With this route map, the special parameter such as the metric value or weight can be filtered or set based on this community value in case of the special update. You can see RTB is transmitting Update having Community 100 200 to RTC. Configure the following to set Weight based on this value.

```
RTC#
router bgp 300
neighbor 3.3.3.3 remote-as 200
neighbor 3.3.3.3 route-map check-community in
route-map check-community permit 10
match community 1
set weight 20
route-map check-community permit 20
match community 2 exact
set weight 10
route-map check-community permit 30
match community 3
ip community-list 1 permit 100
ip community-list 2 permit 200
```

```
ip community-list 3 permit internet
```

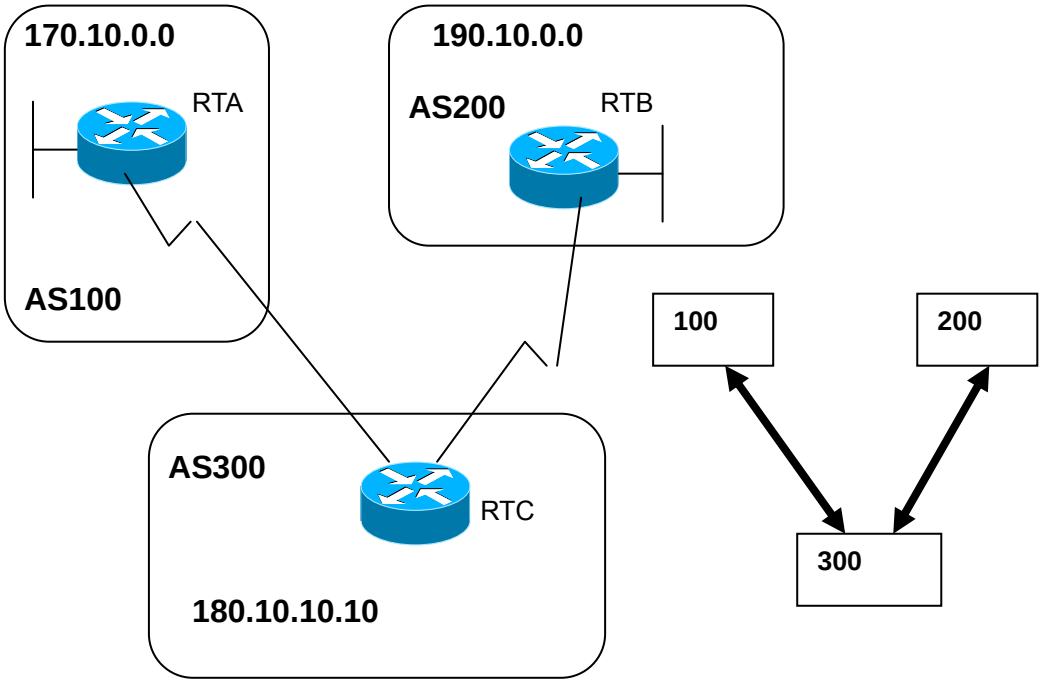
The route with the community attribute 100 is matched with List 1 and weight is set as 20. The route with the community attribute 200 is matched with List 2 and Weight is set as 10. The keyword “exact” shows that there should not be other values if community should have community 200. The last community list is used to prevent other updates from dropping because routes not matched is dropped to the default. The keyword “internet” is all routes because these is a member of Internet community.

BGP Attribute Configuration

The following shows the attributes used by BGP.

- As-path attribute
- Origin attribute
- Nexthop attribute
- Local Preference attribute
- Metric attribute
- Community attribute
- Weight attribute

As_path Attribute



The number of AS is added to the route update when one route goes through one AS. AS_Path attribute is AS number list that one route passes through to get the certain destination. AS_SET is all AS groups that one route passes through. Network 190.10.0.0 is displayed by RTB in AS200, and RTC adds AS300 to this route AS-path when this route passes AS300. So, the path for RTA to get to 190.10.0.0 is (300,200).

This is applied to 170.10.0.0 and 180.10.0.0.. RTB should pass AS300 and AS100 to get to 170.10.0.0, and RTC should pass AS200 to 190.10.0.0 and AS 100 to 170.10.0.0.

Origin Attribute

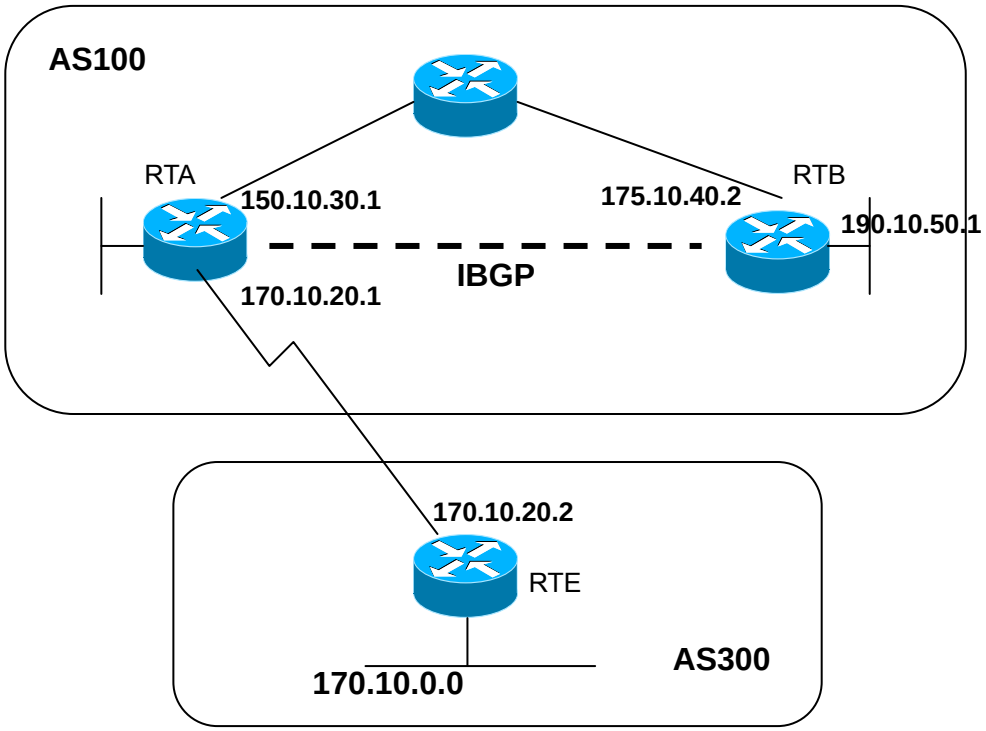
This is an attribute to define Pass Information Source and there are three mechanism.

- **IGP**:
  NLRI(Network Layer Reachability Information) is inside of the AS. This is used when BGP

Network command is used or IGP information is redistributed to BGP. This pass information origin is IGP and displayed as “i” in the BGP table.

- **EGP**:
  NLRI is got through BGP and displayed as “e” in the BGP table.

- **INCOMPLETE**:
  NLRI is unknows or got through the miscellaneous ways. This is used when the static route is redistributed to BGP and displayed “?” in the BGP table.



RTA#
router bgp 100
neighbor 190.10.50.1 remote-as 100
neighbor 170.10.20.2 remote-as 300
network 150.10.0.0
redistribute static
ip route 190.10.0.0 255.255.0.0 null0

RTB#
router bgp 100
neighbor 150.10.30.1 remote-as 100
network 190.10.50.0

RTE#
router bgp 300
neighbor 170.10.20.1 remote-as 100
network 170.10.0.0

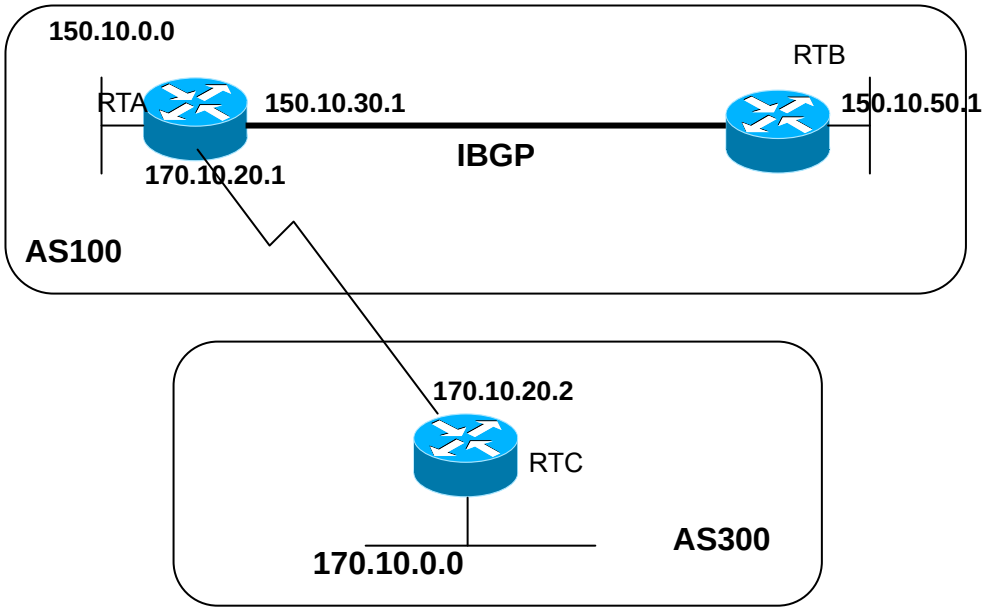
The configuration above shows

- RTA gets to 170.10.0.0 through 300i.
  The next AS pass is 300 and the route origin is IGP.)
- RTA gets to 190.10.50.0 through i.
  (The means the next AS pass is 100 and the route origin is IGP.)
- RTA gets to 150.10.0.0 through 100i.
  (The means the next AS pass is 100 and the route origin is IGP.)
- RTA gets to 190.10.0.0 through 100?.
  The means the next AS pass is 100 and theroute origin is Imcomplete.)

BGP Nexthop Attribute

The nexthop attribute is the nexthop IP address to get to the certain destination. EBGP is the assigned neighbor IP address by neighbor command. The configuration below shows RTC transmits nexthop 179.10.20.2 when transmitting 170.10.0.0 to RTA, and RTA transmits nexthop 170.10.20.1 when transmitting 150.10.0.0 to RTC. According to protocol, the nexthop by EBGP itself shoud be transmitted with IBGP. RTA transmits nexthop to 170.10.20.2 when transmitting 170.10.0.0 to its IBGP peer RTB, and RTB transmits nexthop to not 150.10.30.1 but 170.10.20.2.

Policy is needed for RTB to get to 170.10.20.2 with IGP and if not, RTB discards the packet toward



170.10.0.0.

RTA#
router bgp 100
neighbor 170.10.20.2 remote-as 300
neighbor 150.10.50.1 remote-as 100
network 150.10.0.0
RTB#
router bgp 100
neighbor 150.10.30.1 remote-as 100

RTC#
router bgp 300
neighbor 170.10.20.1 remote-as 100
network 170.10.0.0

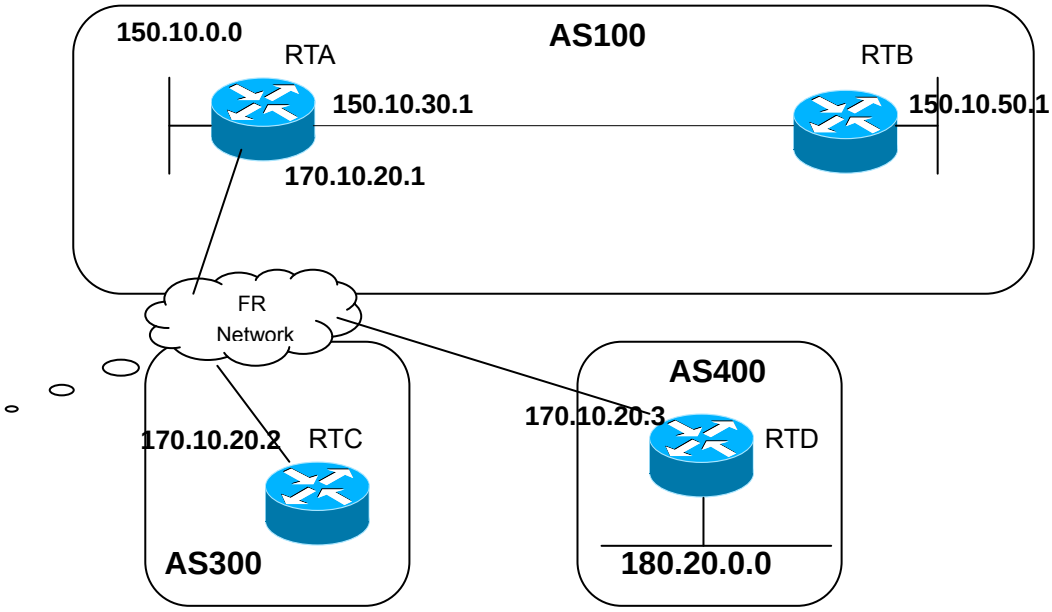
- When RTC transmits 170.10.0.0 to RTA, the nexthop is 170.10.20.2.
  When RTA transmits 170.10.0.0 to RTB, the nexthop is 170.10.20.2.

BGP Nexthop (Multiaccess Networks)

RTC connects RTA and EBGP. RTC get access to 180.20.0.0 through 170.10.20.3, and when it transmits 180.20.0.0 information with BGP update to RTA, it uses not its IP 170.10.20.2 but 170.10.20.3 as a next hop. The reason is that the network among RTA, RTC, and RTD is a multi-access network and it is more useful to use RTD as a next hop for RTA to get to 180.2.0.0.
NBMA network, the common media among RTA, RTC, and RTD, causes more complicated problems.

The following shows you should be careful in the multi access network and NBMA network

BGP Nexthop (NBMA)



If the common media is NBMA network like Frame Relay, RTC uses 170.10.20.3 as the next hop when transmitting 180.20.0.0 information to RTA. If RTA does not have the direct PVC and cannot get access to the next hop, the routing is failed. For this, the Nexthopself command was created.

Nexthopself

With the Nexthopself command, the protocol does not assign the nexthop and the assigned IP is used for the nexthop. The command is as follows.

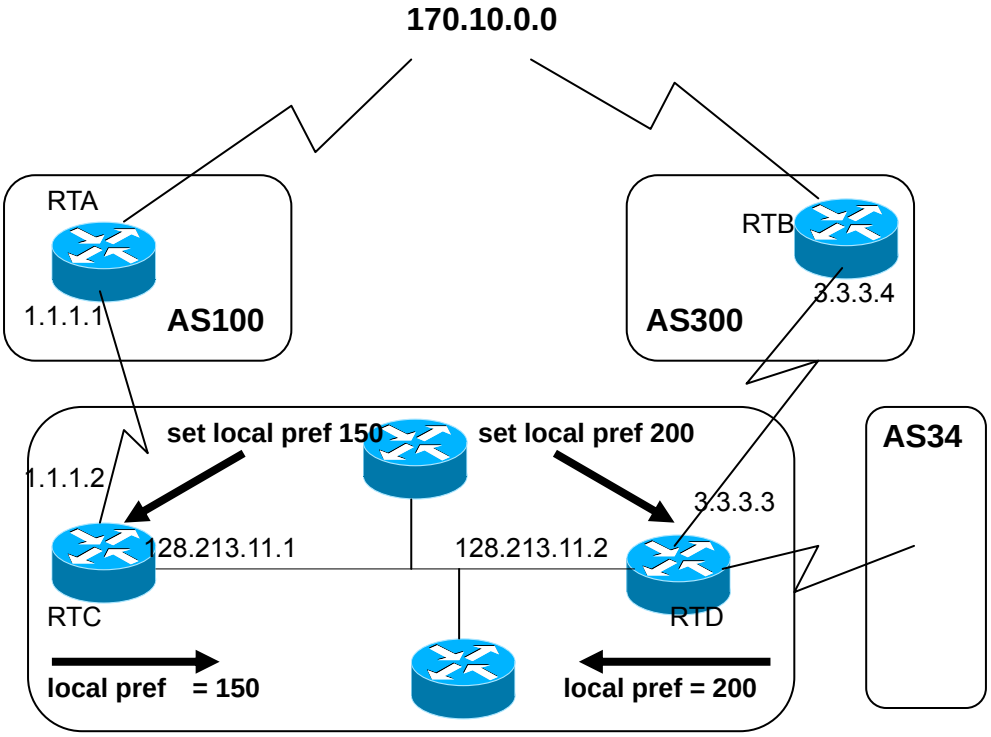
neighbor {ip-address|peer-group-name} next-hop-self
In case of the previous example, the following shows how to solve the problem.

RTC#
router bgp 300
neighbor 170.10.20.1 remote-as 100
neighbor 170.10.20.1 next-hop-self
RTC transmits 180.20.0.0 to the nextHop = 170.10.20.2.

Local Preference Attribute

Local preference notices path preference to AS in order to get the specific network from the AS. The path with higher value ocal preference is preferred more and the default is 100. The local preference is an attribute to be exchanged among routers in the same AS unlike wegith attribute.
This is set with **bgp default local-preference** < *value*> command or route map.

The bgp default local-preference < *value*> command changes local preference value for moving to the peer router in the same AS. The following example shows two AS update 170.10.0.0 of AS256.
Local preference helps the way to get out of AS256 to get to the same network. Supposing RTd is the exit point. The following shows the local preference value is set as 200 for AS 300update, 150 for AS 150.



RTC#
router bgp 256
neighbor 1.1.1.1 remote-as 100
neighbor 128.213.11.2 remote-as 256
bgp default local-preference 150
RTD#
router bgp 256
neighbor 3.3.3.4 remote-as 300
neighbor 128.213.11.1 remote-as 256
bgp default local-preference 200

RTC sets the local preference of all update as 150 and RTD asa 200. RTC and RTD recognized that the network 170.10.0.0 information from AS300 has the higher local preference than one from AS100. So, all traffic of AS256 assigned as 170.10.0.0 is transmitted to RTD.

But, using route map has more flexibility. With this route map, the specific update is set as the specific local preference as the following configuration.

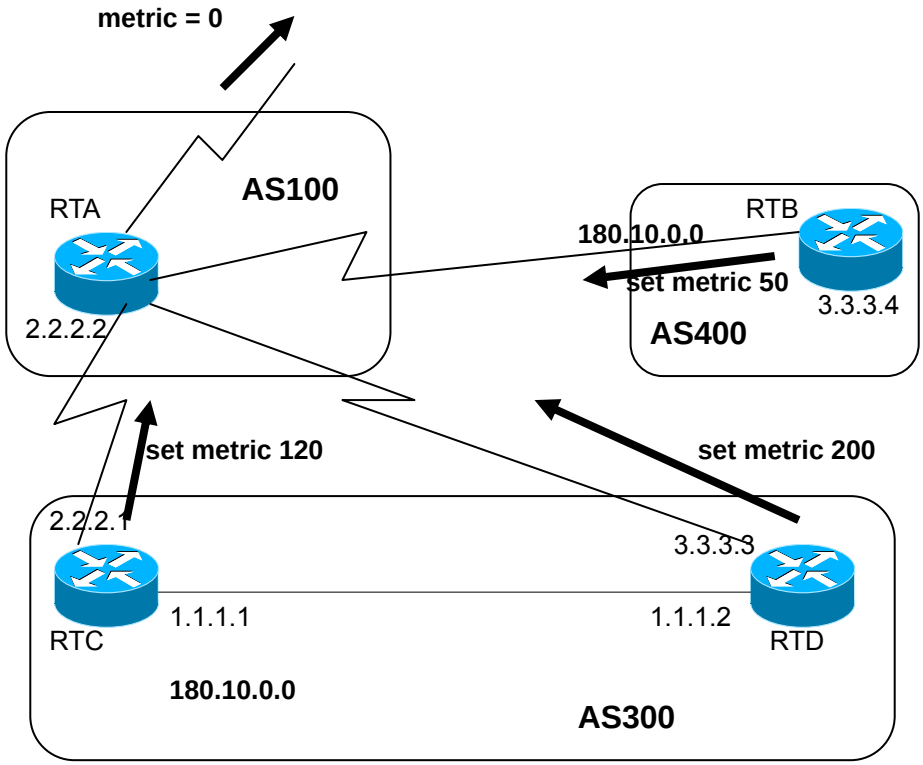
```
RTD#
router bgp 256
neighbor 3.3.3.4 remote-as 300
neighbor 3.3.3.4 route-map setlocalin in
neighbor 128.213.11.1 remote-as 256
....
ip as-path access-list 7 permit ^300$
...
route-map setlocalin permit 10
match as-path 7
set local-preference 200
route-map setlocalin permit 20
set local-preference 150
```

With the configuration above, the update from AS300 is set as Local preferenc 200 and other updates from AS34 are set as Local preference 150.

Metric Attribute

Metric Attribute, Multi_exit_discriminator (MED), provides path preference for the specific AS to the external route. When there are various entry points to the specific AS, it helps other AS to choose the point to get to the route and the path with the lower value is chosen.

Unlike local preference, metric is exchanged among AS. It is transmitted to one AS and remained in AS. Metric is used to choose the path in AS when update with the certain metric comes in AS. When the same update information is sent to other AS, metric value is set as 0(default). Compare the metric from neighbor in the same AS when no specific setting and it needs special configuarion command “bgp always-compare-med” to compare metric from neighbor in different AS.



AS100 gets network information of 180.10.0.0 through RTC, RTD, and RTB. RTC and RTD are in AS300 and RTB is in AS400.

Supposing the metric from RTC is set as 120 from RTD as 200, and from RTB as 50. By default, router compares the metric from neighbor in the same AS. RTA can only compare the metric from RTC, and RTD and chooses RTC as the best nexthop because netric value 120 is lower than 200. When RTA gets the information with metric 50 from RTB, it cannot compare this value with metric 120 because RTC and RTB are in the different AS. (RTA chooses the path based on the different attributes).
The following shows to add **bgp always-compare-med** command to RTA in order RTA compares the metric.

```
RTA#
    router bgp 100
```

```
    neighbor 2.2.2.1 remote-as 300
    neighbor 3.3.3.3 remote-as 300
    neighbor 4.4.4.3 remote-as 400
    ....
RTC#
    router bgp 300
    neighbor 2.2.2.2 remote-as 100
    neighbor 2.2.2.2 route-map setmetricout out
    neighbor 1.1.1.2 remote-as 300
route-map setmetricout permit 10
    set metric 120
RTD#
    router bgp 300
    neighbor 3.3.3.2 remote-as 100
    neighbor 3.3.3.2 route-map setmetricout out
    neighbor 1.1.1.1 remote-as 300
route-map setmetricout permit 10
    set metric 200
RTB#
    router bgp 400
    neighbor 4.4.4.4 remote-as 100
    neighbor 4.4.4.4 route-map setmetricout out
route-map setmetricout permit 10
    set metric 50
```

From the configuration above, RTA chooses RTC as the nexthop. (Supposing the different attributes are same). The following shows how to configure RTA in order to compare the metric.

```
RTA#
router bgp 100
neighbor 2.2.21 remote-as 300
neighbor 3.3.3.3 remote-as 300
neighbor 4.4.4.3 remote-as 400
bgp always-compare-med
```

RTA chooses RTB as the best nexthop to get to 180.10.0.0, and also set metric value as redistributing the route to BGP with the command **"default-metric** *number"*. The following shows the configuration when RTB redistributes static information.

```
RTB#
router bgp 400
redistribute static
default-metric 50

ip route 180.10.0.0 255.255.0.0 null 0
!-- Causes RTB to send out 180.10.0.0 with a metric of 50
```

Community Attribute

Community attribute is an optional and transitive attribute from the value 0 to 4,294,967,200, and groups many destinations as the special communities to apply routing decide (accept, prefer, and redistribute). To set the community attriubute, use the following route map.

set community community	number [additive]

The following shows the common community-number.

- **no-export** (Do not advertise to EBGP peers)
- **no-advertise** (Do not advertise this route to any peer)
- **internet** (Advertise this route to the internet community, any router belongs to it)

The following shows the route map that sets community.

```
route-map communitymap
match ip address 1
set community no-advertise
```

or

```
route-map setcommunity
match as-path 1
set community 200 additive
```

If additive keyword is set, thevalue 200 replaces the current community value, and if additive keyword is set, the value 200 is added. After setting the community attribute, this system transmits this to the neighbor by default. But Cisco system should use the following command.

```
neighbor {ip-address|peer-group-name} send-community
```

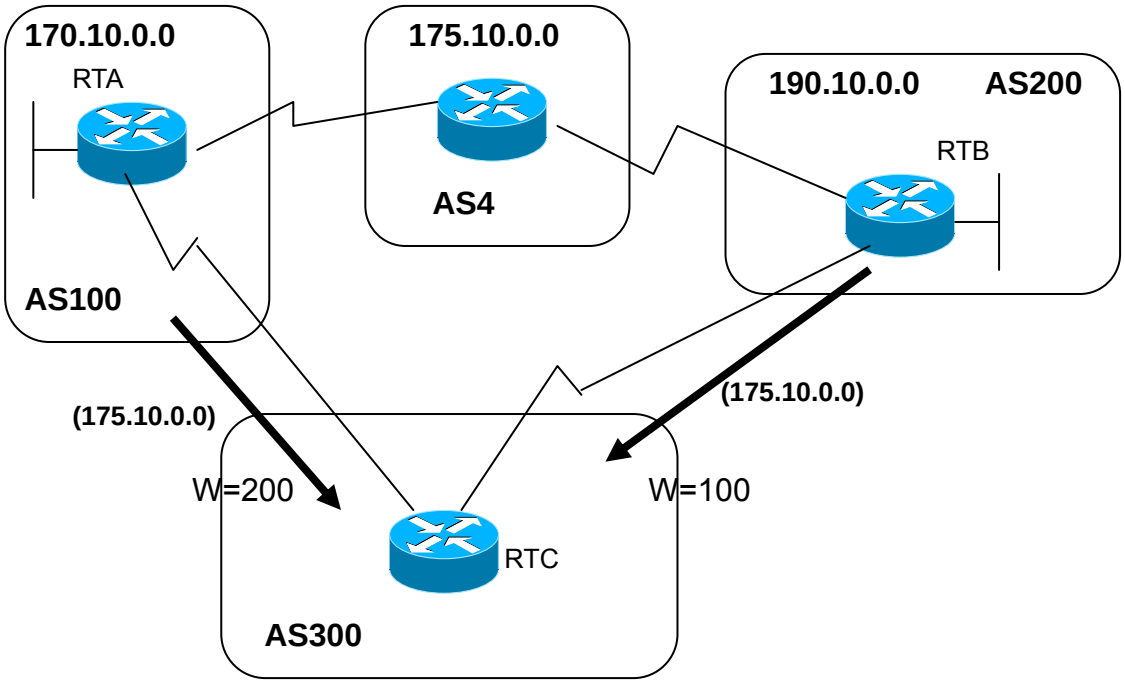
```
RTA#
router bgp 100
neighbor 3.3.3.3 remote-as 300
neighbor 3.3.3.3 send-community
neighbor 3.3.3.3 route-map setcommunity out
```

By default, this system enables the neighbor send-community and the command ‘neighbor 3.3.3.3 send-community’ is not useful.

Weight Attribute

Weight Attribute defined by this system has the same function as Cisco system and is applied to the certain router. This is between 0~65535. The path by itself has the value 32768 by default and the others have “0”.

With many routes to the same destination, the route with the higher weight is chosen.



RTA and RTB get the information of network 175.10.0.0 from AS4 and transmit it to RTC. And RTC has two paths to network 175.10.0.0. If RTC gives the higher weight to RTA, RTC chooses RTA as the netxthop.

- Using the **neighbor** command: **neighbor** {*ip-address*|*peer-group*} **weight** *weight*.
- Using AS path access-lists: **ip as-path access-list** *access-list-number* **{permit|deny}** *as-regular-expression* **neighbor** *ip-address* **filter-list** *access-list-number* **weight** *weight*.
- Using route-maps.

With many routes to the same destination, the route with the higher weight is chosen. The following shows the three mechanisms with the example above.

#1. Neighbor Weight Command
RTC#
router bgp 300
neighbor 1.1.1.1 remote-as 100
neighbor 1.1.1.1 weight 200
!-- route to 175.10.0.0 from RTA has 200 weight
neighbor 2.2.2.2 remote-as 200
neighbor 2.2.2.2 weight 100
!-- route to 175.10.0.0 from RTB will have 100 weight

#2. IP as-pathand filter-list
RTC#
router bgp 300
neighbor 1.1.1.1 remote-as 100
neighbor 1.1.1.1 filter-list 5 weight 200
neighbor 2.2.2.2 remote-as 200
neighbor 2.2.2.2 filter-list 6 weight 100

```
...
ip as-path access-list 5 permit ^100$
!-- this only permits path 100
ip as-path access-list 6 permit ^200$
```

#3. Route Map

```
RTC#
router bgp 300
neighbor 1.1.1.1 remote-as 100
neighbor 1.1.1.1 route-map setweightin in
neighbor 2.2.2.2 remote-as 200
neighbor 2.2.2.2 route-map setweightin in
...
ip as-path access-list 5 permit ^100$
...
route-map setweightin permit 10
match as-path 5
set weight 200
!-- anything that applies to access-list 5, such as packets from AS100, have weight 200
route-map setweightin permit 20
    set weight 100
    !-- anything else would have weight 100
```

Routing Policy Modification

Routing Policy helps to choose the information with Route-map,Filter-list, and Prefix-list when sending/receiving the neighbor router and routing information. And BGP has new routing information for the new policy as canceling the current routing information or recovering the current path when the routing policy is modified.

In order BGP router get the information for the new policy, it sets the Inbound reset, and in order to provide the new information, it sets “Outbound reset”. As the new information for the new policy is provided, the neighbor router gets the new information.

If BGP router and neighbor router in the user network supports route refresh capability function, they can renew routing information with “Inound reset”. The following shows the advantages of routing reset.

- ✓ Needless additional operation setting of operator.
- ✓ Needless additional memory for routinhg information modification.

The following shows the command to confirm the neighbor router supports Route Refresh Capability function.

neighbor capability route	refresh

This command specifies Route Refresh Capability function to the neighbor router, and if the neighbor router supports this function, the message “ Received route refresh capability from peer”

is printed out.

With Route Refresh Capability function by all BGP router, user gets path information sent already with Soft reset. The following shows the command to set routing information for the new policy.

clear ip bgp [* | AS | address] soft in

On the other hand, Outbound reset transmits the routing information again with the command “Soft” without setting beforehand. The following shows the command to provide the routing information again.

clear ip bgp [* | AS | address] soft out

To recover the modified routing policy to the default, operator uses Route Refresh Capability function and does not need to cancel modified policies individually.

The switch without Route Refresh Capability function cancels the routing information with the command “Neighbor Soft-reconfiguration”. But, operator should be careful to use because network can have the problem.

To creat new information not reset BGP information, operator should store all information to BGP network, which is not recommendable because of memory loading. But, providing modified information does not need memory, and neighbor routers get the modified information consecutively after BGP router transmits this.

The following show the procedures how to reset BGP with the Routing policy.

1) After reconfiguring BGP router, all information from the neighbor router are stored in BGP router from this point.

neighbor ip-address soft-reconfiguration inbound

2) Register the modified information in table with the stored information.

clear ip bgp [* | AS | address] soft in

The following shows the command to confirm the modified routing information with the routing table and BGP neighbor router.

show ip bgp neighbors ip-address [advertised-routes|received-routes|routes]

Miscellaneous Functions

Neighbor command is used with the Route map to filter input/output update or set parameter.

Route map related to the neighbor door does not affect on input update when matching based on IP address.

neighbor ip-address route-map route-map-name

Use of Set as-path Prepend Command

The following shows the command to adjust path information for BGP decision process modification as using the route map.

set as-path prepend<As-path#><As-path#> ...

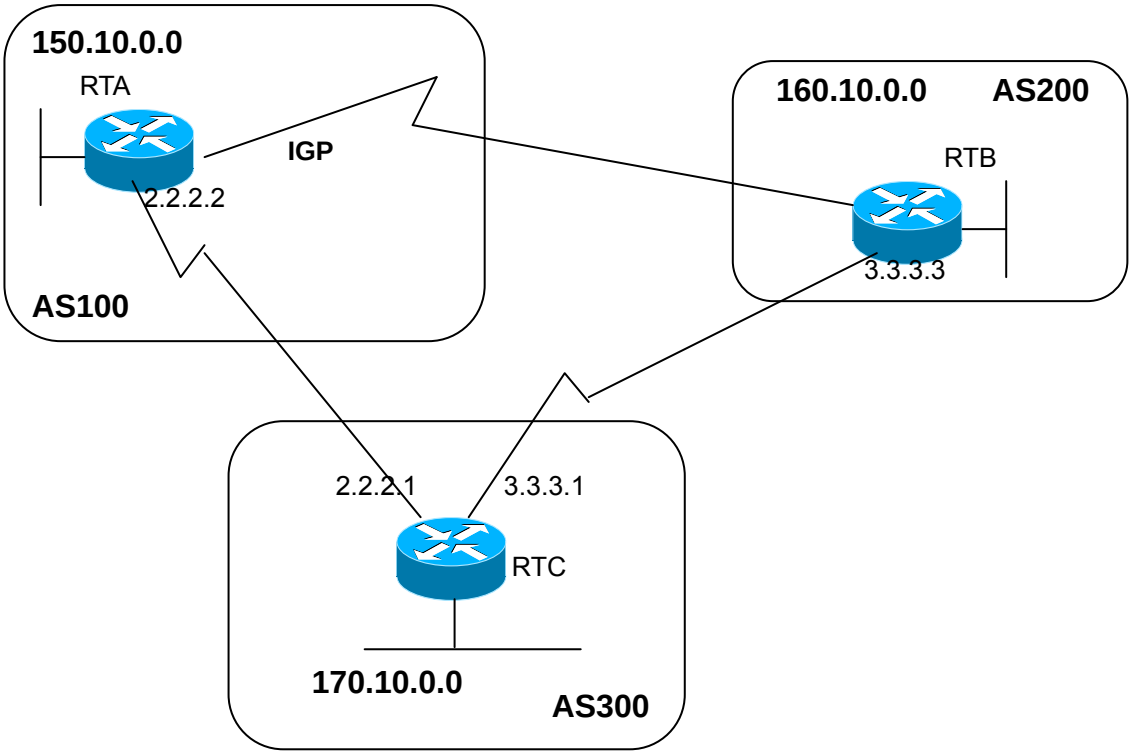
BGP Peer Groups

BGP Peer Groups is a BGP Neighbor groups for the same update policy that is set by route map, distribute-list, and filter-list. They define the same policies to each neighbor but apply them as naming Peer group. Every member of the peer group has all configuration options, and overrides it as defining new options with no effect on the member or output update.

The following shows the configuration to define the peer group.

neighbor *peer-group-name* **peer-group**

BGP backdoor



The configuration above shows that RTA & RTC and RTB & RTC are connected with EBGP. RTA and RTB use IGP protocol (OSPF and RIP). EBGP update has “20” of distance value smaller than IGP distance value. By default, RIP distance value is 120 and OSPF has 110.

RTA transmits update information of 160.10.0.0 with the two routing protocols. One is EBGP with distance value 20 and the other is IGP with distance value more than 20.

The following shows the default distance value of BGP and it can be changed by distance command.

distance bgp *external-distance internal-distance local-distance*
external-distance:20
internal-distance:200
local-distance:200

RTA chooses EBGP update information from RTC having smaller distance value. And, The following shows what RTA needs to do to get information of 160.10.0.0 through RTB.

- Change the external distance value of EBGP or the external distance value of IGP. (not recommendable)
- Use BGP backdoor

The following shows the command that BGP backdoor makes IGP route as the preferred route.

network address backdoor

The assigned address is a network address to receive through IGP. And BGP is recognized as the assigned network locally.

RTA#
router ospf

router bgp 100
neighbor 2.2.2.1 remote-as 300
network 160.10.0.0 backdoor

Network 160.10.0.0 is recognized as the local entry but is not transmitted like the common network entry.

RTA gets information of 160.10.0.0 from RTB through OSPF with distance value 110 and RTC through EBGP with distance value 20 simultaneously. EBGP is usually preferred but OSPF is chosed due to backdoor command.

Route Flap Dampening

Route Dampening minimizes the unstability by oscillation between route flapping and network. Flapping route gets penalty (default is 1000) for each flap. IF the accumulated penalty excesses suppress-limit, route transmission is stopped. The penalty is decreased by 50% when it gets to “half-time” every 5 sec.The route is retransmitted after the decreased penalty is under the defined “reuse-limit” value.

By default status, Route dampening is off. The following shows the command to adjust the Route dampening.

- **bgp dampening** (will turn on dampening)
- **no bgp dampening** (will turn off dampening)
- **bgp dampening** <*half-life-time*> (will change the half-life-time)

And the following shows command to change all parameters simultaneously.

- **bgp dampening** <*half-life-time*> <*reuse*> <*suppress*> <*maximum-suppress-time*>
- <*half-life-time*> (range is 1-45 min, current default is 15 min)
- <*reuse-value*> (range is 1-20000, default is 750)
- <*suppress-value*> (range is 1-20000, default is 2000)
- <*max-suppress-time*> (maximum duration a route can be suppressed, range is 1-255, default is 4 times half-life-time)

The following shows the terms for the Route dampening.

Table 52. Items for Route Dampening

Items	Description
History state	This does not include the best path for the route but information for the route flapping.
Damp state	This shows the panelty value excesses and information is not transmitted to the neighbor.
Penalty	This is value added to router by the route flapping and the default is 1000. This is accumulated and the status is changed from “history” to “damp” by suppress limit.
Suppress limit	This is a suppress limit of panelty by route and the default is 200.
Half-life-time	The penalty imposed to route is to be half every 5 sec after the period set in Half-life-time (default is 15 min).
Reuse-limit	The path cleared is recovered if penalty imposed to flapping is under Reuse-limit. The default is 750 and the procedure to clear Path Invaid is performed every 10 sec.
Maximum suppress limit	This is the maximum period that route can be invalid and the dafauld is 4 times than half-lif-time.

Chapter 10. LACP

This chapter describes how to configure IEEE 802.3ad Link Aggregation Control Protocol (LACP) on the switch.

This chapter consists of the following sections:

- Understanding the Link Aggregation Control Protocol
- Configuring 802.3ad Link Aggregation Control Protocol
- Displaying 802.3ad Statistics and Status

Understanding Link Aggregation Control Protocol

This chapter includes the following descriptions:

- LACP Modes
- LACP Parameters

LACP Modes

Port group configuration of P8824XG can be done manually or automatically with IEEE 802.3ad LACP (Link Aggregation Control Protocol).

.

To configure port group with LACP, use the active or passive mode. To start automatic port group configuration with LACP, at least one end of the link needs to be configured to active mode to initiate negotiating. This is due to that ports in passive mode passively respond to initiation and never initate the sending LACP packets.

The following shows the possible mode in LACP.

Mode	Description
off	Modes that prevents the port from grouping. (default)
passive	LACP mode that places a port into a passive negotiating state. The port responds to LACP packets only when it receives the LACP packets and does not start LACP packet negotiation first.
active	LACP mode that places the port into an active negotiating state, in which the port starts negotiations with other port by sending LACP packets.

LACP Parameters

The parameters used in configuring LACP are follows.

- System Priority
  System priority must be assigned in the switch that is running LACP. System priority can be configured automatically or through the CLI. System priority is used with the switch MAC address to form the system ID and is also used during negotiation with other systems.

- Port Priority
  Port priority must be configured in each port of the switch automatically or through CLI. The port priority is used with the port number to form the port identifier. The port priority is used to decide which ports should be configured in standby mode when there is a hardware limitation that prevents all compatible ports from aggregating.

- Administrative key
  Administrative key must be assigned to each port in the switch automatically or through CLI. The ability of a port to aggregate with other ports is defined with the administarative key. Ability of a port to aggregate with other ports is determined by the following factors:

- Physical characteristics of port, such as data rate, duplex mode and point-to-point or shared medium.
- Configuration constraints

When LACP is enabled, LACP always attempts to aggregate the mamximum number of ports. If LACP is not able to aggregate all the ports that are compatible, then all the ports that cannot be aggregated are put in hot standby state and are used only if one of the port group port fails.

Configuring 802.3ad Link Aggregation Control Protocol

This chapter explains how to configure port group with LACP.

- Specifying the System Priority
- Specifying the Port Priority
- Specifying an Administrative Key Value
- Specifying the Timeout Value
- Changing the LACP Mode
- Clearing LACP Statistics

Specifying the System Priority

The system priority value shoud be an integer between 1 and 65535. Higher the number represents lower the priority. The default priority is 32768.

To specify the system priority, follow the step below from privileged EXEC mode:

		Command	Description
Step1		**configure terminal**	Enter the Global configuration Mode.
Step2		**lacp system-priority** *priority*	Specify the system Priority.
Step3		**end**	Return to Privileged EXEC Mode.
Step4		**show lacp sys-id**	Verify Setting.
Step5		**copy running-config startup-config**	(Optional) Save Setting into configuration file.

To return the system priority to default setting, use Global configuration command "**no lacp system-priority"**

This example shows how to specify the system priority as "20000".

```
Switch# configure terminal
Switch(config)# lacp system-priority 20000
Switch(config)# end
```

Specifying the Port Priority

The port priority value shoud be an integer between 1 and 65535. Higher numbers represent lower priority and the default priority is 32768.
To specify the port priority, follow the step below from privileged EXEC mode.

		Command	Description
Step1		**configure terminal**	Enter Global configuration Mode.
Stpe2		**interface** *interface-id*	Enter Interface configuration mode, and specify the interface to configure.
Step3		**lacp port-priority** *priority*	Specify the port priority
Step4		**end**	Return to Privileged EXEC Mode
Step5		**show running-config**	Verify Setting.
Step6		**copy running-config startup-config**	(Optional) Save Setting into Configuration file.

To return the port priority to default setting, use Interface Configuration Command "**no lacp port-priority"**

This example shows how to specify the port priority of Interface gi1 as "10".

```
Switch# configure terminal
Switch(config)# interface gi1
Switch(config-if-gi1)# lacp port-priority 10
Switch(config)# end
```

Specifying an Administrative Key Value

Administrative Key Value of port or system can be set manually and automatically where the range is between 0-255.

To specify the administrative key value, follow the steps below from the Privileged EXEC Mode.

		Command	Description
Step1		**Configure terminal**	Enter Global configuration Mode.
Stpe2		**interface** *interface-id*	Enter Interface configuration mode, and specify the interface to configure.
Step3		**lacp admin-key** *key*	Specify the administrative key.
Step4		**end**	Return to the Privileged EXEC Mode.
Step5		**show running-config**	Verifying Setting.
Step6		**copy running-config startup-config**	(Optional) Save Setting into Configuration file.

To specify the administrative key value to interface automatically, use Interface Configuration Command " **no lacp admin-key".**

The example below shows how to specify the administrative key of interface gi1 as "10".

```
Switch# configure terminal
Switch(config)# interface gi1
Switch(config-if-gi1)# lacp admin-key 10
Switch(config)# end
```

Specifying the Timeout Value

LACPDU Timeout Value of port can be specified. The timeout value can be short (1sec) or long (30 sec).

Note LACPDU Timeout Command affects the LACPDU time out of other relative switch.

To specify the timeout value, follow the steps below from the Privileged EXEC Mode.

		Command	Description
Step1		**configure terminal**	Enter Global configuration Mode
Stpe2		**interface** *interface-id*	Enter Interface configuration mode, and specify the interface to configure.
Step3		**lacp timeout** {**short**|**long**}	Specify LACPDU Timeout
Step4		**end**	Return to the Privileged EXEC Mode.
Step5		**show running-config**	Verify Setting.
Step6		**copy running-config startup-config**	(Optoinal) Save Setting into Configuraion file.

To return the LACPDU Timeout as default, use Interface Configuration Command " **no lacp timeout".**

This example shows how to specify LACPDU Timeout of the relative system connected to Interface gi1 as default.

```
Switch# configure terminal
Switch(config)# interface gi1
Switch(config-if-gi1)# lacp timeout short
Switch(config)# end
```

Changing the LACP Mode

The interface of LACP mode can be configured.

To change the LACP mode, follow the steps below from the Previleged EXEC Mode.

		Command	Description
Step1		**Configure terminal**	Enter Global Configuration Mode.
Stpe2		**interface** *interface-id*	Enter Interface configuration mode, and specify the interface to configure. Specify interface to set LACP mode and use Interface Configuration Mode.
Step3		**lacp mode** {**active** | **off** | **passive**}	Change the LACP Mode. To change LACP mode to active or passive, the switch port mode of the port has to be changed to no-switchport mode (use interface configuration command "**no switchport**").
Step4		**end**	Return the Privileged EXEC Mode.
Step5		**show running-config**	Verify Setting.
Step6		**copy running-config startup-config**	(Optional) Save Setting into Configuration file.

This example shows how to enable LACP of Interface gi1.

```
Switch# configure terminal
Switch(config)# interface gi1
Switch(config-if-gi1)# no switchport
Switch(config-if-gi1)# lacp mode active
Switch(config)# end
```

Clearing LACP Statistics

To clear/delete LACP statistics, follow the steps below from the previliege EXEC mode.

		Command	Description
Step1		**clear lacp [***aggregator-id***] counters**	Clear LACP statistics of the corresponding port group.
Stpe2		**show lacp counters**	Verify modification.

This example shows how to clear LACP statistics of the ‘port group’ 1.

```
Switch# clear lacp 1 counters
```

Displaying 802.3ad Statistics and Status

To search/check LACP statistics, use the privileged EXEC command “**show lacp counters”.**

To search/check LACP statistics of the specific port group, use the privileged EXEC command “**show lacp** *aggregator-id* **counters”.**

To search/check LACP protocol information and status of switch, use the privileged EXEC command “ **show lacp internal”.** To search/check LACP protocol information and status of the relative switch, use the privileged EXEC command “ **show lacp neighbor ”.**

Chapter 11. Statistics Monitoring and QoS

This chapter describes how to view the current operating status of P8824XG switch, how to display information in the log, and how to take advantage of available Remote Monitoring (RMON) capabilities.

Viewing statistics on a regular basis allows you to see how well your network is performing. If you keep daily records, you will see the trends emerging and notice problems arising before they cause major network faults. This way, statistics can help you get the best out of your network.

Status Monitoring

The status monitoring facility provides information about P8824XG switch. With show and its sub-commands, P8824XG switch provides the various statuses monitoring information displayed on your terminal screen.

Table 53. Status Monitoring Command

commands	Description
show log	■ Displays the current snapshot of the log. ■ You can save maximum 500 logs.
show memory usage	■ Show the status of the system memory usage.
show cpu usage	■ Show the current CPU usage.
show version	■ Displays the hardware and software versions currently running on the switch.

Port Statistics

P8824XG switch provides statistical information of the ports. The information lists values for the current counter of each port on each operational module in the system.
To view port statistics, use the following command:
Show interface [interface name]
The following statistic information of the ports are collected by the switch:

- **Link Status** – The current status of the link.
- **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.

You can see the following various statistic data with Sho interface command.

```
Switch# show interface
gi1 is down
  type GBIC,SC
  ifindex 28(k34)    BROADCAST MULTICAST
  gbic not inserted
  no auto-negotiation
  speed set 1G
  duplex set full

  Last clearing of counters 01:09:07
  1 minutes input rate 0 bytes/sec, 0 packets/sec
  1 minutes output rate 0 bytes/sec, 0 packets/sec
```

```
    0 packets input, 0 bytes
    Received 0 broadcasts, 0 multicasts
    0 CRC, 0 oversize, 0 dropped
    0 packets output, 0 bytes
    Sent 0 broadcasts, 0 multicasts

gi2 is down
  type GBIC,SC
  ifindex 29(k35)   BROADCAST MULTICAST
  gbic not inserted
  no auto-negotiation
  speed set 1G
  duplex set full

  Last clearing of counters 01:09:07
  1 minutes input rate 0 bytes/sec, 0 packets/sec
  1 minutes output rate 0 bytes/sec, 0 packets/sec
    0 packets input, 0 bytes
    Received 0 broadcasts, 0 multicasts
    0 CRC, 0 oversize, 0 dropped
    0 packets output, 0 bytes
   Sent 0 broadcasts, 0 multicasts
   --More--
```

Table 54. Port Statistics Inquiry Command

Command	Description	Mode
show port counter	Display In/Out packet accumulation of system interface.	Interface
Show port statistics IFNAME	Display bit/s, bytes/s, pkts/s of Rx/Tx by 5 sec, 1 min, and 5 min of the interface.	Config

The following displays packet accumulation of all ports and statistics by 5 sec, 1 min, and 5 min of the specific interface with Show port counter.

```
Switch# show port counter

ifname I-Kbps O-Kbps    InOctets    InUpkt   InNUpkt   OutOctets   OutUpkt OutNUpkt
-------------------------------------------------------------------------------
   gi1   0 00     0     00     0     0
   gi2   0 00     0     00     0     0
   gi3   0 0 1778273344 27785521     0 1703531840 26617684     1
   gi4   0 0 1704062592 26625978     0 1505886656 23529478     1
   gi5   0 00     0     00     0     0
   gi6   0 00     0     00     0     0
   gi7   0 00     0     00     0     0
   gi8   0 00     0     00     0     0
```

```
gi9   0 00     0     00     0     0
gi10   0 00     0     00     0     0
gi11   0 0     82534336   1289599     0     72563328   1133802     0
gi12   0 0     72563328   1133802     0     82534336   1289599     0

Switch# show port statistics gi3

Last clearing of counters 00:28:14

-------------------------------------------------------------------------
  RX   | TX
  bits/s       bytes/spkts/s |     bits/s       bytes/spkts/s
-------------------------------------------------------------------------
 5sec :     74910208       9363776146309     63776256       7972032124563

 1min :     13620760       1702595 26602       5314688664336 10380

 5min :       6623696827962 12936       2997952374744    5855
```

With the following command, you can reset the statistics with Show interface command or Set low/high threash for the specific period of the interface and report it through Syslog, Snmp trap.

Table 55. Port Statistics Inquiry Setting Command

Command	Description	Mode
load interval <5-100>	Set the average period from using Show interface.	interface
no load interval	Set the average from using Show interface as the default. (60 sec)	interface
input-load-monitor *<5-100> <1-1000> <1-1000>*	Set low/high threash for the specific period of the interface and report it through Syslog, Snmp trap.	interface
no input-load-monitor	Clear Input-load-monitor.	interface

The following command is to initialize statistics accumulation.

Table 56. Port Statistics Initialization Command

Command	Description	Mode
clear counters	Initialize statistics accumulation of the system interface.	privileged
clear counters *IFNAME*	Initialize statistics accumulation of the specific interface.	privileged
clear counters snmp	Initialize SNMP statistics accumulation of the system interface.	privileged

Logging

P8824XG switch log shows all information on configuration and alarm. The system message logging software saves log messages in the switch memory and sends messages to other devices. The system message logging function supports the followings.

- Enables the user to select the logging type to collect.
- Enables the user to select the device to which he/she sends the collected logging.

P8824XG switch saves and sends debug-level logs in the internal buffer and the system console by default. The user can control system messages by using CLI. The switch saves up to 500 log messages in the system memory. The system administrator can monitor the system messages from local through console or from remote through Telnet or syslog server log.

P8824XG switch has 0-7 severity levels as shown in the table.

Table 57. P8824XG Switch Log Level

Severity level	Description
Emergencies (0)	System is not available.
Alerts (1)	Immediate action is required.
Critical (2)	Critical status
Errors (3)	Errors message.
Warnings (4)	Warnings message.
Notifications (5)	Normal status but important information.
Informational (6)	Informational message given to user
Debugging (7)	Debugging message

System Log Message Context

The system log messages of P8824XG switch consist of the following information.

- **Timestamp**
  - The timestamp records the month, day and year of the event, along with the time (hours, minutes, and seconds) in the form HH:MM:SS MM/DD/YYYY.
  - You can decide whether timestamp is displayed or not with log session timestamp [*enable*|*disable*] command

- **Severity level**
  - Indicates the log message level defined in the < >
  - Integer between 0 and 7

- **Log description**
  - Text string including detailed information on event

The following is the log message for system booting.

```
%10:00:04 10/29/2001 %-5-%System starting ...
%10:00:07 10/29/2001 %-5-%DHCP server started
%10:00:07 10/29/2001 %-7-%snmpAgnt initialization
%10:00:10 10/29/2001 %-5-%null interface attached
%10:00:10 10/29/2001 %-5-%IF3M: VLAN 1 created
%10:00:11 10/29/2001 %-5-%IF3M: gi1 --> Link Up
%10:00:11 10/29/2001 %-5-%IF3M: gi2 --> Link Up
%10:00:11 10/29/2001 %-5-%IF3M: gi3 --> Link Up
%10:00:11 10/29/2001 %-5-%IF3M: gi4 --> Link Up
%10:00:11 10/29/2001 %-5-%IF Manager Started
%10:00:11 10/29/2001 %-5-%IF Statistics Module started
%10:00:11 10/29/2001 %-5-%System started.
%10:00:11 10/29/2001 %-5-%Configuration loading ...
```

Default Logging Value

Table 58. System Log Defaults

Configuration parameter	defaults
Display logging to console	enabled
Display logging to Telnet session	enabled
Logging buffer size	500
Display 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	Errors(3)

Table 59. Commands for System Message Logging Configuration

Command	Description
logging console {*enable*|*disable*}	■ Set whether to display logging to console.
logging session {*enable*|*disable*}	■ Set whether to display logging to current session.
logging session timestamp {*enable*|*disable*}	■ Set whether to display timestamp to current session.
logging session level <0-7>	■ Set the level of the log message displayed to current session.
show log [last] [number-of-message]	■ Display logging buffer and check logging configuration

RMON (Remote MONitoring)

Using the Remote Monitoring (RMON) capabilities of the P8824XG switch allows network administrators to improve system efficiency and reduce the load on the network.

The following sections explain more about the RMON concept and the RMON features supported by the P8824XG switch.

RMON Overview

RMON is international standard defined by the Internet Engineering Task Force (IETF) documents RFC 1271 and RFC 1757, which allows remote LAN monitoring.

A typical RMON setup consists of the following two components:

- **RMON Probe**
  - An intelligent, remotely controlled device or software agent that continually collects statistics about a LAN segment or VLAN.
  - The probe transfers the information to a management workstation on request, or when a predefined threshold is crossed.

- **RMON Manager**
  - Communicates with the RMON probe and collects the statistics from it.
  - The workstation does not have to be on the same network as the probe, and can manage the probe by in-band or out-of-band connections.

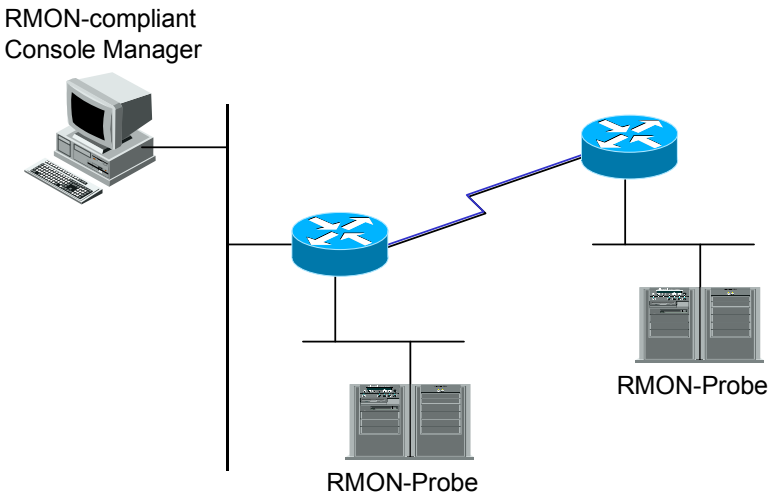


Figure 19. RMON Manager and RMON Probe

While the existing SNMP MIBs manage only gears with SNMP agent, RMON MIBs can extend the management object to the LAN segment where the device is connected. RMON agent informs the status of the entire traffic of LAN segment, each host connected to each segment, and the traffic

status between hosts.

RMON agent must have the entire statistic data, history data, host-related data, host matrix and as well as the alarming function that warns when the thereshold, which is set to predict and remove certain packets for filtering, is reached.

P8824XG switch supports only statistics, history, alarm, and event groups among the nine RMON groups defined in the table. All the RMON functions are set as disabled by default.

Table 60. RMON Items

Items	Description
Statistics	■ Provide statistic information of the number of packets/bytes generated in one segment, the broadcast/multicast count, the conflict count, packet count by length, and errors (fragment, CRC Alignment, jabber, insufficient length, excessive length).
History	■ Provide the information on the traffic and errors generated during the time span that the operation manager has set. ■ Setting short-term/long-term time span and the interval is limited to 1-3.600 seconds. ■ Display of the usage by time and comparing the data with other segment data.
Alarm	■ Check a particular value regularly and report to the manager when the value reaches the standard and the agent has its record. ■ Setting an absolute or relative value as the standard. An alarm occurs only when the value goes over or down the upper limit/the lowest limit in order to prevent continuous alarms.
Host	■ Manages the traffic of each device connected to the segment, and the error count by hosts.
N high level hosts	■ Find the host that generates the most traffic during a certain period among the hosts found in the above host table. ■ The manager can get information by setting the data type, the interval, and the number of hosts that he/she wants.
Traffic matrix	■ Collect the information on the traffic and errors generated between two hosts based on data link layer, that is, MAC address. ■ With this information, you can see who uses a certain host most often. ■ If a host in other segment users the host the most, you cannot find the actual user because the user uses the host through the router.
Filter	■ Used by the manager to monitor the trend of a particular packet.
Packet collection	■ The manager collects and analyzes the packets generated in the segment.
Event	■ When a certain event occurs, this item saves the log and sends a warning message to the manager. The trap generation and the logging storage are optional.

RMON Alarm and Event Group Setting

The user can set RMON configuration through CLI or SNMP manager. RMON configuration is set in the privileged mode with the following commands.

Table 61. RMON Alarm and Event Setting Command

Command	Description	Mode
rmon alarm *index* ifEntry *variable ifIndex interval* {delta|absolute} rising-	■ Add alarm to RMON alarm table. ■ Index: An integer between 1 and 65535 ■ Variable is MIB object	Config

threshold *value* [*event-number*] falling-threshold *value* [*event-number*] [owner *string*]	■ Interval is the time interval for the observation of alarm variable and the unit is second. ■ Delta means the observation of the difference between samples of MIB variables. Absolute means the absolute value of MIB variable. ■ Set the rising-threshold and falling-threshold. ■ The event configuration is optional. When the delta or absolute value of the alarm variable reaches to the rising threshold or the falling threshold, the related event occurs. ■ You can specify the owner of the alarm.	
rmon event *index* [log] [trap *community*] [owner *string*] [description *string*]	■ Add an event to RMON event table. ■ Log specifies whether to generate RMON log when an event occurs. Trap specifies whether to send trap when an event occurs.	Config
no rmon alarm *alarm-index*	■ Delete an alarm from RMON alarm table.	Config
no rmon event *event-index*	■ Delete an event from RMON event Table.	Config
show rmon alarms	■ Show RMON alarm table.	Privileged
show rmon events	■ Show RMON event table.	Privileged

```
Switch# configure terminal
Switch(config)# rmon alarm 10 ifEntry inErrors 1 20 delta rising-threshold 15 1 falling-threshold 0 owner hong
Switch(config)# rmon event 1 log trap rmontrap owner hong description  “Noti : Too Much InErrors”
Switch(config)# exit
Switch# show rmon alarm
  Alarm 10 is active, owned by hong
  Monitors ifEntry.14.1 every 20 seconds
  Taking delta samples, last value was 0
  Rising threshold is 15, assigned to event 1
  Falling threshold is 0, assigned to event 0
  On startup enable rising or falling alarm

Switch# show rmon event
Event 1 is active, owned by hong
  Description is “Noti: Too Much InErrors”,
  0 Event firing cases log and trap to community eventrap, last fired  0: 0: 0
Switch#
```

Table 62. Commands for RMON Statistics and History Setting

Command	Description	Mode
rmon history *index* ifEntry *ifIndex* [buckets *bucket-number*] [interval seconds] [owner *string*]	■ Collects history by the specified number of buckets with the given interval ■ ‘index’ ranges from 1 to 65535.	Config

	■ The default number of buckets is 50.	
no rmon history *index* ifEntry *ifindex*	■ Disables collecting history data.	Config
show rmon history	■ Shows RMON history table.	Privileged
show rmon statistics	■ Shows RMON statistics table.	Privileged

```
Switch# show rmon statistics
---------------------------------------
            SHOW STATISTICS
---------------------------------------

The Index of stats     : 1
Interface              : fa1
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              : gi2
Drop Events            : 0
Total Octets           : 0
Total Packets          : 0
……
Switch#
```

```
Switch# configure terminal
Switch(config)# rmon history 1 ifEntry 9 buckets 100 interval 5 owner park
Swtich(config)# end
Switch# show rmon history
---------------------------------------
            SHOW HISTORY
---------------------------------------


====== fa1 ======
Control-index      : 1
ifindex            : 9
interval           : 5
buckets            : 50
owner              : park
```

--- gi2 : bucket 1 ---
DropEvents : 0
Octets : 0
(skipped)
Switch# **show rmon statistics**

RMON STATISTICS

The Index of stats : 1 (gi1)

DropEvents	:	0	Jabbers	:	0
Octets	:	0	Collisions	:	0
Pkts	:	0	Pkts64Octets	:	0
BroadcastPkts	:	0	Pkts65to127Octets	:	0
MulticastPkts	:	0	Pkts128to255Octets	:	0
CRCAlignErrors	:	0	Pkts256to511Octets	:	0
UndesizePkts	:	0	Pkts512to1023Octets	:	0
OversizePkts	:	0	Pkts1024to1518Octets	:	0
Fragments	:	0			

The Index of stats : 2 (gi2)

DropEvents	:	0	Jabbers	:	0
Octets	:	0	Collisions	:	0
Pkts	:	0	Pkts64Octets	:	0
BroadcastPkts	:	0	Pkts65to127Octets	:	0
MulticastPkts	:	0	Pkts128to255Octets	:	0
CRCAlignErrors	:	0	Pkts256to511Octets	:	0
UndesizePkts	:	0	Pkts512to1023Octets	:	0
OversizePkts	:	0	Pkts1024to1518Octets	:	0
Fragments	:	0			

(Omitted)
Switch# **show rmon statistics gi2**

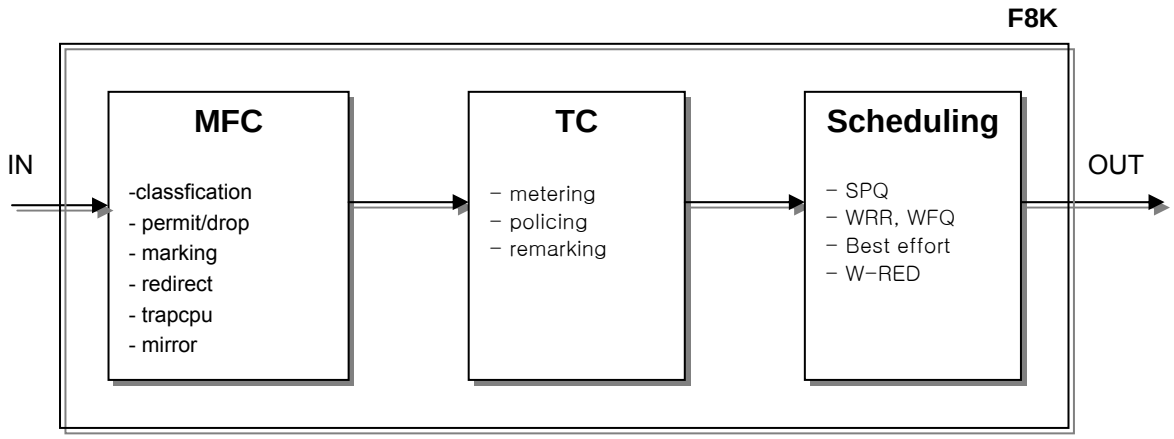
RMON STATISTICS

The Index of stats : 2 (gi2)

DropEvents	:	0	Jabbers	:	0
Octets	:	3331342	Collisions	:	0
Pkts	:	33150	Pkts64Octets	:	15428
BroadcastPkts	:	18579	Pkts65to127Octets	:	13300
MulticastPkts	:	14164	Pkts128to255Octets	:	3992
CRCAlignErrors	:	22	Pkts256to511Octets	:	206
UndesizePkts	:	0	Pkts512to1023Octets	:	398
OversizePkts	:	0	Pkts1024to1518Octets	:	92
Fragments	:	0			

QoS and Packet Filtering

P8824XG performs the following functions for QoS and packet filtering.



- **MFC (Multi-Field Classifier)**
  Specific action execution or marking of specific field for QoS after selecting the flow-rule by classifying the value of protocol, src/dest IP, UDP/TCP Port, dscp, Tcp syn. And it is used for various filtering functions.

- **TC (Traffic Conditioner)**
  Make statistics bound with the special flow-rule, limit bandwidth, or remark QoS fileds. Various statistics and bandwitdh limit is possible because many flow-rule can be bound in on TC.

- **Scheduling**

  Differentiate traffic oveload process with scheduling algorithm as the following traffic condition.

  - SPQ (Strict Priority Queuing Method)

  SPQ is used to process data priority. This algorithm processes the data by priority so that data with low priority cannot outgo and the bandwidth is full with the data with high priority.

  - WRR (Weighted Round Robin Method), WFQ (Weighted Fair Queuing Method)

  WRP processes data with the certain rate and covers the disadvantages of SPQ. It allots bandwidth to queue and user can set certain process rate for the environment..

MFC (Multi-Field Classifier)

Setting/Clearing Flow-Rule

Flow-rule can be classified based on the specific value such as src/dest IP, UDP/TCP Port, dscp, and Tcp sync. And it supports classification such as netbios-filter, nbt-filter, dhcp-filter only for the special filtering (drop).

Table 63. Command for Flow-rule Classification

Command	Description	Mode
flow-rule NAME **classify** { <0-255> | icmp | igmp | ip | ospf | pim | tcp | udp } { SRCIP SRCMASK | SRCIP/M | any } { DSTIP DSTMASK | DSTIP/M | any }	Apply to all or specific SRC/DEST IP of the specific protocol of port that flow-rule is applied.	Config
flow-rule *NAME* **classify** { *<0-255>* | **icmp | igmp | ip | ospf | pim | tcp | udp** } { *SRCIP SRCMASK* | *SRCIP/M* | **any** } { *DSTIP DSTMASK* | *DSTIP/M* | **any** } **dscp** *VALUE*	Apply to all or specific SRC/DEST IP and the specific DSCP of the specific protocol of port that flow- rule is applied.	Config
flow-rule *NAME* **classify** { **tcp | udp** } { *SRCIP SRCMASK* | *SRCIP/M* | **any** } { *DSTIP DSTMASK* | *DSTIP/M* | **any** } { *<0-255>* | *SRCPORT* } { *<0-255>* | *DSTPORT*}	Apply to all or specific SRC/DEST IP and all or specific SRC/DEST port of the UDP/TCP protocol of port that flow-rule is applied.	Config
flow-rule *NAME* **classify** { **tcp | udp** } { *SRCIP SRCMASK* | *SRCIP/M* | **any** } { *DSTIP DSTMASK* | *DSTIP/M* | **any** } { *<0-255>* | *SRCPORT* } { *<0-255>* | *DSTPORT*} **dscp** *VALUE*	Apply to all or specific SRC/DEST IP, all or specific SRC/DEST port, and the specific DSCP of the UDP/TCP protocol of port that flow-rule is applied.	Config
flow-rule *NAME* **classify** { **tcp | udp** } { *SRCIP SRCMASK* | *SRCIP/M* | **any** } { *DSTIP DSTMASK* | *DSTIP/M* | **any** } { *<0-255>* | *SRCPORT* } { *<0-255>* | *DSTPORT*} **cos** *VALUE*	Apply to all or specific SRC/DEST IP, all or specific SRC/DEST port, and the specific COS of the UDP/TCP protocol of port that flow-rule is applied.	Config
flow-rule *NAME* **classify** { **tcp | udp** } { *SRCIP SRCMASK* | *SRCIP/M* | **any** } { *DSTIP DSTMASK* | *DSTIP/M* | **any** } { *<0-255>* | *SRCPORT* } { *<0-255>* | *DSTPORT*} **tos** *VALUE*	Apply to all or specific SRC/DEST IP, all or specific SRC/DEST port, and the specific TOS(ip-precedence) of the UDP/TCP protocol of port that flow-rule is applied.	Config
flow-rule *NAME* **classify tcp** { *SRCIP SRCMASK* | *SRCIP/M* | **any** } { *DSTIP DSTMASK* | *DSTIP/M* | **any** } { *<0-255>* | *SRCPORT* } { *<0-255>* | *DSTPORT*} **sync**	Apply to all or specific SRC/DEST IP, all or specific SRC/DEST port and SYNC of the TCP protocol of port that flow-rule is applied.	Config
flow-rule *NAME* **classify** { *H.H.H* | **any** } { *H.H.H* | **any** }	Apply to all or specific SRC/DEST MAC address of the port that flow-rule is applied.	Config

flow-rule *NAME* **classify** { *H.H.H* | **any** } { *H.H.H* | **any** } **cos** *VALUE*	Apply to all or specific SRC/DEST MAC address and the specific COS of the port that flow-rule is applied.	Config
flow-rule *NAME* **classify dhcp-filter**	Apply filter for DHCP protocol of the port that flow-rule is applied.	Config
flow-rule *NAME* **classify nbt-filter**	Apply filter for NBT protocol of the port that flow-rule is applied.	Config
flow-rule *NAME* **classify netbios-filter**	Apply filter for NETBIOS protocol of the port that flow-rule is applied.	Config

It can apply special action to the flow-rule classified by each condition, mark CoS, DP (Drop precedence), Dscp, Tos(Ip Precedence), Queue field for QoS, and apply action such as Redirect, Mirror, Traptocp, and Rate-limit.
And, it performs Remark, Rate-limit, and statistics of QoS field bounded with TC (Traffic Conditioner).

Notice The special Flow-rule such as DHCP-filter, NBT-filter, and NETBIOS-filter cannot match with other actions.

Notice The flow rule assigned SRC/DEST MAC Address is included only in policy-map having l2-default profiles. And the flow- rule assigned COS among flow-rule related to l3 is included policy-map having 13 COS profile.

Table 64. Command for Flow-rule Policy

Command	Description	Mode
flow-rule NAME match { permit | drop }	Permit/Deny packet mateced with the policy.	Config
flow-rule *NAME* **match** { **cos | droppreceden**ce **| dscp | queue-parameter** } *VALUE*	Mark packet qos value matched with the policy .	Config
flow-rule *NAME* **match mirror**	Transmit the packet copy matched with the policy to Mirror port.	Config
flow-rule *NAME* **match redirect** VNAME *IFNAME*	Transmit the packet matched with the policy to VLAN port.	Config
flow-rule *NAME* **match rate-limit** *<1-100000>*	Limit packet rate matched with the policy	Config
flow-rule *NAME* **match tc-table** *TBLNAME*	Bind the packet mateched with the policy to TC-table.	Config
flow-rule name **match trapcpu**	Trap the packet matched with the policy to CPU.	Config

Notice A flow-rule can match only one action except Marking.

To cancel the policy applied to the specific Flow-rule, use the following command.

Table 65. Command for Flow-rule

Command	Description	Mode
no flow-rule NAME match { permit | drop }	Cancel flow-rule match.	Config
no flow-rule *NAME* **match** { **cos | dropprecedence | dscp | queue-parameter** }		
no flow-rule *NAME* **match mirror**		
no flow-rule *NAME* **match redirect**		
no flow-rule *NAME* **match rate-limit**		
no flow-rule *NAME* **match tc-table**		
no flow-rule *NAME* **match trapcpu**		

The following command is to cancel the specific flow-rule.

Table 66. Command for Flow-rule Cancel

Command	Descriptoin	Mode
no flow-rule NAME	Delete Flow-rule of NAME.	Config

Policy-map Create/Add

To apply flow-rule to interface, create policy-map that can include various flow-rules, and various policies are applied to one interface. The sequence is important because flow-rule is applied by add sequence to policy-map. You can check the sequence from **Show Flow-rule**.

Table 67. Command for Policy-map Creat/Add

Command	Description	Mode
policy-map PNAME flow-rule FNAME	Generate new PNAME or add FNAME flow lastly when there is PNAME policy;.	Config
policy-map *PNAME* **flow-rule** *FNAME1* **above flow-rule** *FNAME2*	Add flow of FNAME 1 above the FNAME2.	Config
policy-map *PNAME* **flow-rule** *FNAME1* **below flow-rule** *FNAME2*	Add flow of FNAME 1 below the FNAME2.	Config

And, this system supports three profiles for Flow-rule classficiation, and classficiation fild that each profile supports is as follows.

- **l3deafult** : protocol type, src/dst ip, src/dst port, dscp, tos, tcp flag
- **l3cos** : protocol type, src/dst ip, src/dst port, dscp, tos, cos
- **l2default** : src/dest mac, cos

The Policy-map should include flow-rule with the same condition, and whole system can include two profiles.

Table 68. Policy-map Create and Profile Modification

Command	Description	Mode
policy-map PNAME profile { l3default | l3cos | l2default }	Create new PNAME or modify policy-map profile to the following value.	Config

Notice When flow-rule of policy-map is created with insering directly, profile is decfided by the first inserted flow-rule. For example, when policy-map is created by flow-rule having SRC/DEST Mac classification, policy-map of l2-default profile is created.

To cancel whole policy-map or one applied flow-rule, use the following command.

Table 69. Command for Policy-map Cancel and Specific Flow-rule Cancel

Command	Description	Mode
no policy-map PNAME	Cancel policy-map of PNAME	Config
no policy-map *PNAME* **flow-rule** *FNAME*	Cancel the specific flow-rule in the policy-map of FNAME.	Config

The following shows the command to apply/cancel created policy-map to VLAN.

Table 70. Command for Policy-map Apply/Cancel

Command	Description	Mode
service-policy PNAME	Apply PNAME policy-map to the special VLAN interface.	Interface
no service-policy	Cancel applied policy-map.	Interface

Notice One VLAN interface has only one policy-map so create applicable policy-map to flow-rule with proper sequence.

The following shows the command to inqure flow-rule setting.

Table 71. Command for Flow-rule Inquriy

Command	Description	Mode
show flow-rule	Display detail of flow-rule and policy-map.	Config
show service-policy	Display current policy-map with VLAN interface.	Config

The following shows the example to meet conditions.

Example 1)
Condition : vlan3
Drop except Telnet among srcip : 210.222.57.0/24
Setting netbios filter

```
Switch#configure terminal
Switch(config)# flow-rule telnet23 classify ip 210.222.57.0/24 any
Switch(config)# flow-rule telnet23 match permit
Switch(config)# flow-rule droprule classify ip 210.222.57.0/24 any
Switch(config)# flow-rule droprule match drop
Switch(config)# flow-rule netbiosfilter classify netbios-filter
Switch(config)#
Switch(config)# policy-map example1 flow-rule telnet23
Switch(config)# policy-map example1 flow-rule droprule
Switch(config)# policy-map example1 flow-rule netbiosfilter
Switch(config)#
Switch(config)# int vlan3
Switch(config-if-vlan3)#
Switch(config-if-vlan3)# service-policy example1
Switch(config-if-vlan3)# end
Switch# show flow-rule

    < flow table >
flow-rule telnet23 classify ip 210.222.57.0/24 any
telnet23 mode keep-l2-cos
telnet23 match permit
flow-rule droprule classify ip 210.222.57.0/24 any
droprule mode keep-l2-cos
droprule match drop
flow-rule netbiosfilter classify netbios-filter

    < policy table >
policy-map   example1 profile l3default
                 example1 flow-rule telnet23
  example1 flow-rule droprule
  example1 flow-rule netbiosfilter

Switch#
Switch# show service-policy
<vlan3>
  service-policy example1
Switch#
```

Example 2)
Condition : vlan2
Mark DSCP value for ICMP packet as “3”.

Redirect Pop3 packet as gi1 in VLAN 3.

```
Switch# conf t
Switch(config)# flow-rule dscpmark classify icmp any any dscp 3
Switch(config)# flow-rule dscpmark match dscp 5
Switch(config)# flow-rule dscpmark mode map-to-entry-dscp
Switch(config)# flow-rule pop3 classify tcp any any any 110
Switch(config)# flow-rule pop3 match redirect vlan3 gi1
Switch(config)#
Switch(config)# policy-map pol1 flow-rule dscpmark
Switch(config)# policy-map pol1 flow-rule pop3
Switch(config)#
Switch(config)# int vlan2
Switch(config-if-vlan2)# service-policy pol1
Switch(config-if-vlan2)#
Switch(config-if-vlan2)# end
Switch# show flow-rule

    < flow table >
flow-rule dscpmark classify icmp any any dscp 3
dscpmark mode map-to-entry-dscp
dscpmark match dscp 5
flow-rule pop3 classify tcp any any any 110
pop3 mode keep-l2-cos
pop3 match redirect vlan3 gi1

    < policy table >
policy-map    pol1 profile l3default
                  pol1 flow-rule dscpmark
   pol1 flow-rule pop3

Switch#
Switch# show service-policy
<vlan2>
   service-policy pol1
Switch#
```

TC (Traffic Conditioner)

As mentioned above, P8824XG switch remarks QoS field of the bound flow-rule with TC (Traffic Conditioner), limit bandwidth, or provide statistics function.

Notice The various flow-rules can be applied to one TC but one flow-rule cannot be bound to the various TC.

TC Creat/Cancel

Table 72. Command for Traffic Conditioner Creat

Command	Description	Mode
tc-table TNAME noratelimit	Create Traffic-conditioner that does not limit rate.	Config
tc-table *TNAME* <1-100000> { **drop** | **nodrop** } **remarkqos**	Creat Traffic-conditioner for the special Ratelimit and QoS (CoS, Queue, DP) remarking.	Config
tc-table *TNAME* <1-100000> { **drop** | **nodrop** } **remarkcos**	Create Traffic-conditioner for the special Ratelimit and Cos remarking.	Config
tc-table *TNAME* <1-100000> { **drop** | **nodrop** } **remarkdp**	Create Traffic-conditioner for the special Ratelimit and Drop precedence remarking.	Config
tc-table *TNAME* <1-100000> { **drop** | **nodrop** } **remarkdp_cos**	Create Traffic-conditioner for the special Ratelimit and Drop precedence/Cos remarking.	Config

Notice In case of Drop/Nodrop option, DP (Drop Precedence) decides RED packet drop among green, yellow, red packet.

To cancel the created TC, use the following command, and TC that flow-rule is not bound is not canceled.

Table 73. Command for Traffic Conditioner Cancel

Command	Description	Mode
no tc-table TNAME	Cancel the special Traffic-conditioner in case of no bound flow.	Config

TC Inquiry with statistics

The following shows the command to inqure created TC_table and bound flow-rule information.

Table 74. Command for Traffic Conditioner Table Inquriy

Command	Description	Mode
show tc-table	Display Traffic-conditioner Information and bound flow-rule.	Config

The following shows the command to inqure current, one min, and 5 min statistics of the special TC.

Table 75. Command for Traffic Conditioner Statistics Inquiry

Command	Description	Mode
show tc-table count TNAME	Display the current, one min, and 5 min statistics of TNAME TC.	Config
show tc-table count all	Display statistics of the current Traffic conditioner and flow-rule.	Config
show tc-table clear-and-count *TNAME*	Display the current, one min, and 5 min statistics of TNAME TC and initialize counter.	Config

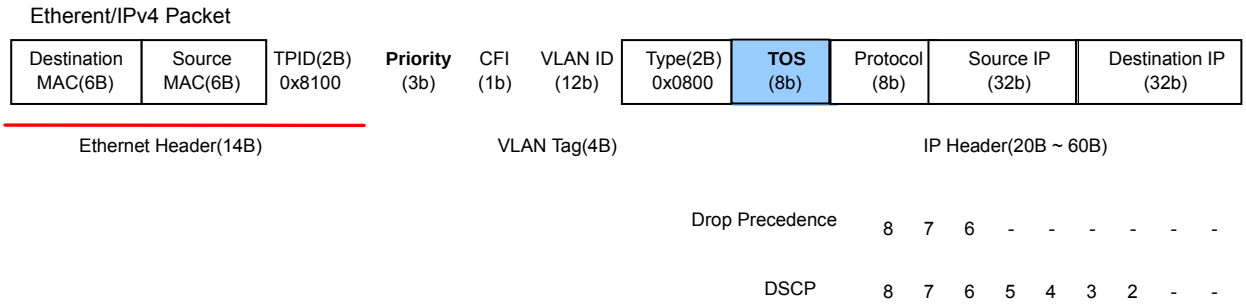
The following shows the example that SRC bandwidth binds flow-rule with DEST 20.1.1.0/24 in 10.1.1.0/24 and limits bandwidth to 1M. You can check TC statistics as follows.

```
Switch(config)# tc-table tc1 1000 nodrop
Switch(config)# flow-rule fa classify ip 10.1.1.0/24 20.1.1.0/24
Switch(config)# flow-rule fa match tc-table tc1
Switch(config)#
Switch(config)# policy-map ra flow-rule fa
Switch(config)#
Switch(config)# int vlan2
Switch(config-if-vlan2)# service-policy ra
Switch(config-if-vlan2)#
Switch(config-if-vlan2)# end
Switch# sh flow-rule

    < flow table >
flow-rule fa classify ip 10.1.1.0/24 20.1.1.0/24
fa mode keep-l2-cos
fa match tc-table tc1

    < policy table >
policy-map ra flow-rule fa

Switch# sh service-policy
```

```
<vlan2>
   service-policy ra
Switch# sh tc-table

     < tc table >
tc-table tc1    1000    nodrop
       flow-rule fa applied

Switch# sh tc-table count all

TC-NAMEFlowCnt(bps)     PktCnt(pps) FLOW-RULE
--------------------------------------------------------------------------------
tc10     0    ip 10.1.1.0/24 20.1.1.0/24

Switch#
Switch# show tc-table count tc1

       current count

     FlowAggCount    :     0 Bytes
     PktAggCounter :     0 Pkts
     GreenCounter    :     0 Bytes
     Yellowcounter :     0 Bytes
     RedCounter      :     0 Bytes

       1 minute avg. count

     FlowAggCount    :     0 Bytes
     PktAggCounter :     0 Pkts
     GreenCounter    :     0 Bytes
     Yellowcounter :     0 Bytes
     RedCounter      :     0 Bytes

       5 minute avg. count

     FlowAggCount    :     0 Bytes
     PktAggCounter :     0 Pkts
     GreenCounter    :     0 Bytes
     Yellowcounter :     0 Bytes
     RedCounter      :     0 Bytes
```

QoS Parameter

The following shows the fields in Ethernet Packet for QoS in P8824XG switch.



Mark/Remark the following fields for QoS. Marking is to modify field with the condition in MFC or L2 level by force and remarking is to remodify the field with TC. The following shows the commands.

QoS-related Parameter Inquire

Table 76. Command for QoS-related Marking/Remarking Table Inquiry

Command	Description	Mode
Show qos cos	Display mapping/remaking table by packet CoS.	Privileged
Show qos dscp-marking	Display QoS (CoS, DP, Queue) field value marked by packet DSCP value. Mark-DSCP option of flow-rule refers this.	Privileged
Show qos dscp-remarking	Display QoS (CoS, DP, Queue) field value marked by packet DSCP value. Mark-DSCP option of TC (Traffic Conditioner) refers this.	Privileged
Show qos tc-cos-remarking	Display CoS value marked by Queue, DP. Remark-CoS option of TC (Traffic Conditioner) refers this.	Privileged

Qos-related Parameter Modification

The following table shows that the following command modifies value to be marked / remarked.

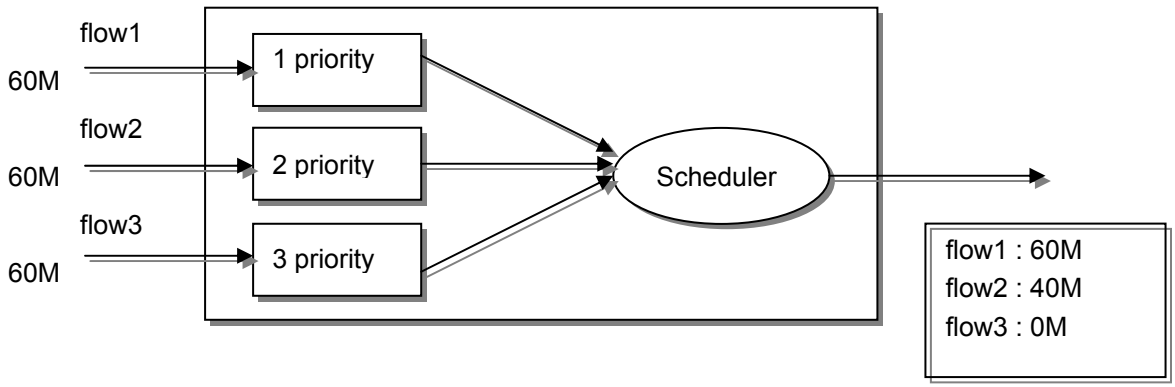
Table 77. Command for Qos-related Marking/Remarking Table Setting

Command	Description	Mode
qos cos-dp-map <0-7> <0-2>	Set new DP (Drop Precedence) value mapped by packet CoS. You can check this with **Show Qos Cos.**	Config
qos cos-queue-map *<0-7> <0-7>*	Set new Queue value mapped by packet CoS. You can check this with **Show Qos Cos.**	Config
qos dscp-marking *<0-63> <0-7 <0-2> <0-7>*	Set new Qos(Cos, Dp, Queue) field value marked by packet DSCP. You can check this with **Show Qos DSCP-Marking.**	Config
qos dscp-remarking *<0-63> <0-7 <0-2> <0-7>*	Set new Qos(Cos, Dp, Queue) field value remarked by packet DSCP. You can check this with **Show Qos DSCP-Remarking.**	Config
qos tc-cos-remarking *<0-7> <0-7>*	Set new Cos value remarked by packet Queue and DP. You can check this with S**how Qos TC-COS-Remarking.**	Config

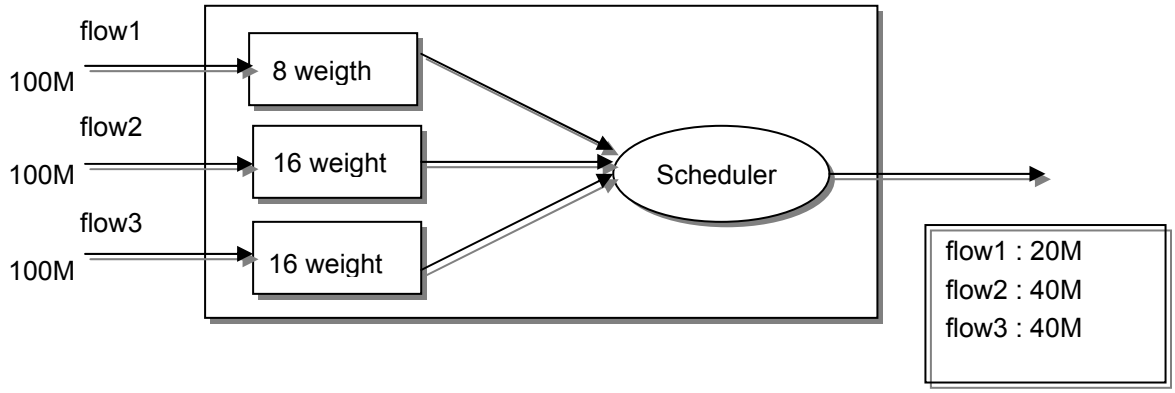
Scheduling

P8824XG switch support SPQ (Strict Priority Queue) Method and WRR (Weighted Round Robin) mothod for Schedulingand the default is SPQ.

The follwoing diagrams show the difference between SPQ and WRP.



SPQ (Strict Priority Queue) method processes the prior packet. All packets are transmitted in “Flow 1” but packets in “Flow 3” of the low rank cannot be tranmitted at all.



- **WRR (Weighted Round Robin) Method**

The above diagram is an example of using WRR (Weighted Round Robin) Method transmitting to port by certain rate.

P8824XG switch suprots Queue for 8 scheduling of 0~7 and the following shows the command to decide Queue method of the specific interface.

Table 78. Command for Queue-method Modification

Command	Description	Mode
queue-method <0-7> { strict | wrr 1| wrr2 }	Modify Queue-method of the interface to Strcint method or WRR (Weight-Round-Robin) mothod.	Interface

Notice Queue with the small number has the priority among 8 Queues of 0~7 in SPQ.

The following shows the command to modify Queue Weight with WRR (Weighted Round Robin) Method.

Table 79. Command for Wrr-method Queue Weight Modification

Command	Description	Mode
wrr-profile <0-7> <8-255>	Modyify Queue Weight of the interface with WRR (Weighted Round Robin) Method. After modifying, you can check with S**how Port QoS.** The default is 8.	Interface

The following shows the scheduling status of each port.

Table 80. Command for Queue-method of the Whole Interfaces and Wegith Inquriy

Command	Description	Mode
show port qos	Display Weight with Queue-method of the whole system Interface and WRR method.	Interface

The following shows the procedures to get result with 1, 2 and 3 Queue among 8 Queues when input ports are gi1, gi2, gi3 and outport are gi4. Port-priority command is to mark packetsas specific queue.

```
Switch(config)# int gi4
Switch(config-if-gi4)# queueing-method 1 wrr1
Switch(config-if-gi4)# queueing-method 2 wrr1
Switch(config-if-gi4)# queueing-method 3 wrr1
Switch(config-if-gi4)# wrr-profile 1 8
Switch(config-if-gi4)# wrr-profile 2 16
Switch(config-if-gi4)# wrr-profile 3 16
Switch(config-if-gi4)#
Switch(config-if-gi4)# int gi1
Switch(config-if-gi1)# port-priority 1
Switch(config-if-gi1)# int gi2
Switch(config-if-gi2)# port-priority 2
Switch(config-if-gi2)# int gi3
Switch(config-if-gi3)# port-priority 3
Switch(config-if-gi3)# end
Switch# show port qos
 IFNAME     Pri WRED     Q0Q1Q2Q3Q4Q5Q6Q7
-----------------------------------------------------------------------
  gi1     P-1    .  st-    st-    st-    st-    st-    st-    st-    st-
  gi2     P-2    .  st-    st-    st-    st-    st-    st-    st-    st-
```

gi3	P-3 .	st-	st-	st-	st-	st-	st-	st-	st-
gi4.	.	st-	w1-	8 w1-	16 w1-	16 st-	st-	st-	st-
gi5.	.	st-	st-	st-	st-	st-	st-	st-	st-
gi6.	.	st-	st-	st-	st-	st-	st-	st-	st-
gi7.	.	st-	st-	st-	st-	st-	st-	st-	st-
gi8.	.	st-	st-	st-	st-	st-	st-	st-	st-
gi9.	.	st-	st-	st-	st-	st-	st-	st-	st-
gi10.	.	st-	st-	st-	st-	st-	st-	st-	st-
gi11.	.	st-	st-	st-	st-	st-	st-	st-	st-
gi12.	.	st-	st-	st-	st-	st-	st-	st-	st-

Extra Filtering

The following shows the command for Source-ip, IPX-NETBIOS filtering.

Table 81. Command for Other Filtering

Command	Description	Mode
source-ip-filter	Set Source-IP Filtering to the specific interface.	Interface
no source-ip-filter	Candel Source-IP Filtering to the specific interface.	Interface
ipx_netbios	Set IPX_NETBIPS Filteringto the specific interface.	Interface
no ipx_netbios	Candel IPX_NETBIPS Filtering to the specific interface.	Interface

sFlow

The system supports sFlow in order to monitor the Traffic flow and collect statistics of individual interface. The objects scope of interface that sFlow takes care confine to physical port in Ubiquoss 9200 Series. sFlow consists of sFlow agent and sFlow collector; sFlow agent collects the status and statistics information of its switch or router while sFlow collector sorts out the collected information and reports to administrator. The following figure shows the basic operation of sFlow.

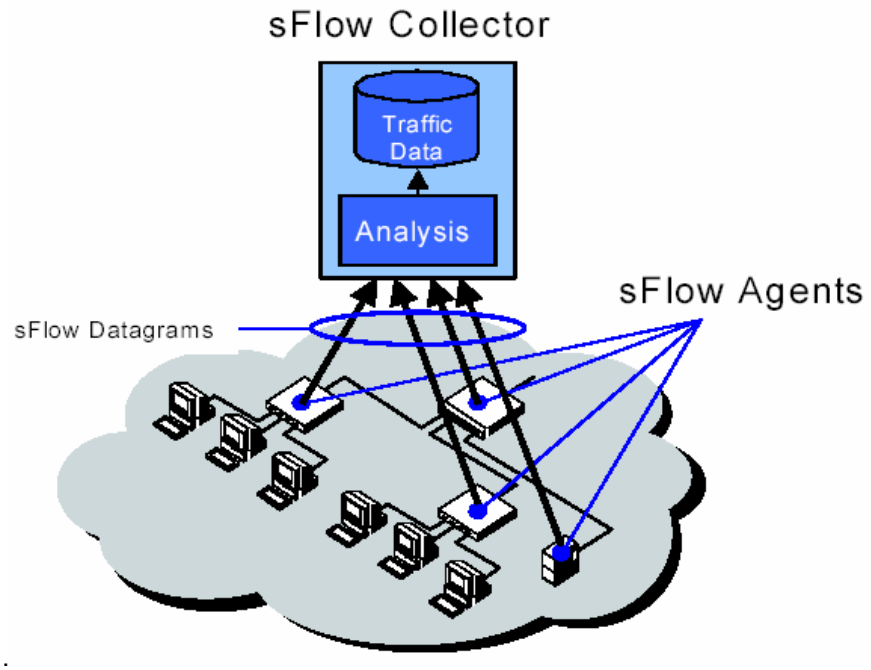


Figure1 Key Map of sFlow (sFlow agent and collector)

sFlow Agent

This section introduces the function and commands for sFlow agent. They have the command for setting IP address of agent and collector, flow sampling rate, counter (statistics) polling interval, sflow forward, and service sflow. The Agent IP is to be inserted into the sampling packet when sFlow agent sends out the sampling packet to sFlow collector, and sFlow collector must specify the Agent IP which is inserted to the sampling packet. sFlow is classified into two categories; one is Flow sampling which is packet based and the other is counter(statistics) sampling which is time based. Flow sampling rate determines the number of packets which come through the interface before system does sampling whereas counter polling interval determines the period in terms of seconds as to when the system does sampling the Interface statistics. By use of ‘sflow forward’ command, you can configure the physical interface (ex, gi1) for sampling upto maximum 4 interfaces. With ‘service sflow’ command you can initiate sflow service.

Table 82. sFlow Command

Command	Description	Mode
show sflow	Shows the commands that you can use to set sflow.	Privileged
service sflow	Makes the system start flow sampling and statistics sampling for the enabled interface. When you want to clear the command, use 'no' preposition.	Config
sflow forwarding	Sets to do sampling with respect to the packets which come through the interface. When you want to clear the command, use 'no' preposition.	Interface
sflow sample *<10-65530>*	Sets the sampling rate in terms of the number of packets which come through the interface. When you use 'no' preposition with this command, it sets to Default value.	Interfac, Config
sflow polling-interval *<20-120>*	Sets the sampling rate in terms of seconds.	Config
sflow agent *A.B.C.D*	Sets the ip address of sflow agent. When you use 'no' preposition with this command, it sets to Default value.	Config
sflow destination *A.B.C.D*	Sets the ip address of sflow collector. When you use 'no' preposition with this command, it sets to Default value.	Config

sFlow Collector

This section describes sFlow collector. It shows statistics values to administrator after analyzing sampling packet. It consists of sflowtool, sFlowTrend, and Inmon Traffic Server. Sflowtool and sFlowTrend are open version. You can download from inmon corporation hompage http://www.inmon.com/index.htm. The following describes sfllowtool and sFlowTrend setting.

sflowtool Configuration

1. You can show sFlow sampling packet in port 6343.with the following command.

```
[lns:/home/lns] sflowtool -p 6343
startDatagram =================================
datagramSourceIP 192.168.0.212
datagramSize 144
unixSecondsUTC 1136381882
datagramVersion 5
agentSubId 0
agent 192.168.0.212
packetSequenceNo 9512
sysUpTime 190157000
samplesInPacket 1
startSample ----------------------
sampleType_tag 0:2
sampleType COUNTERSSAMPLE
endSample   ----------------------
endDatagram   =================================
```

2. You can show sFlow sampling packet by line unit with the following command.

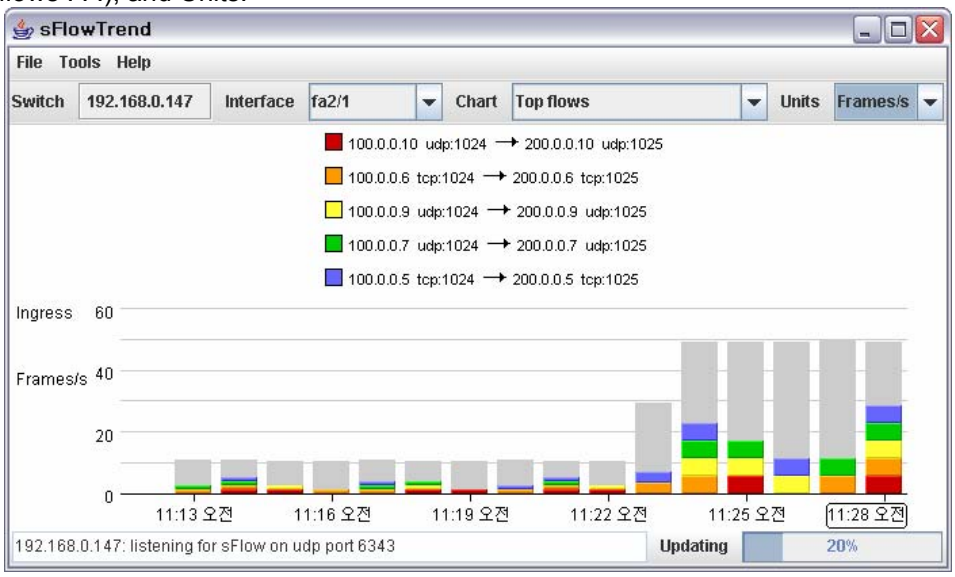
```
[lns:/home/lns] sflowtool -l
CNTR,10.0.0.254,17,6,100000000,0,2147483648,175283006,136405187,257
8019,297011,0,3,0,0,0,0,0
,0,0,1
FLOW,10.0.0.254,0,0,00902773db08,001083265e00,0x0800,0,0,10.0.0.1,10.0
.0.254,17,0x00,64,3569
0,161,0x00,143,125,80
```

sFlowTrend Configuration

1. After executing sFlowTrend program, click the “Click to select” button at upper-left corner.

2. Type in the IP Address of sFlow Agent at the 'Select switch/router to monitor' dialog box.

3. Once sFlowTrend has acquired sampling information, select the relevant option within the scroll donw menu of Interface, Chart (Utilization, Counters, Top flows . . .), and Units.



sFlow Network Configuariton

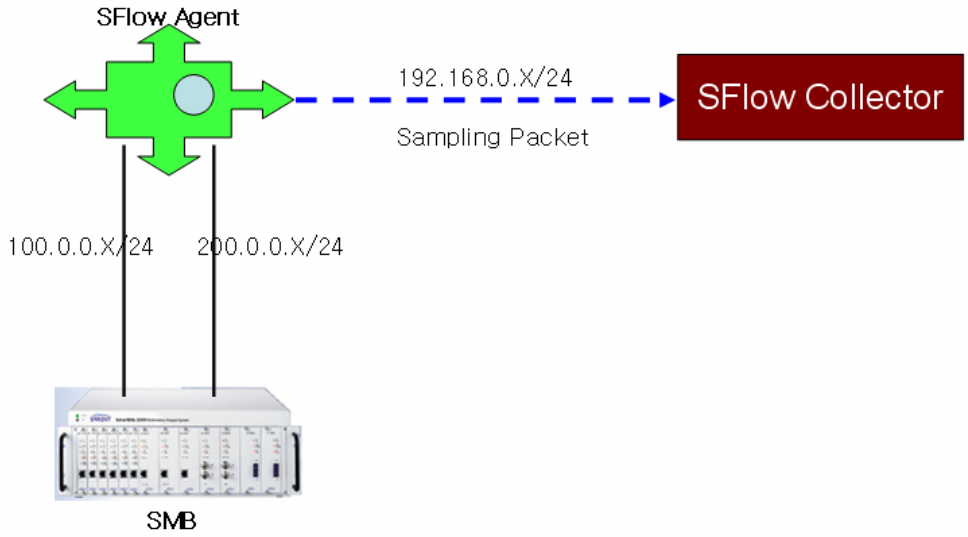


Figure2. sFlow Network Configuration

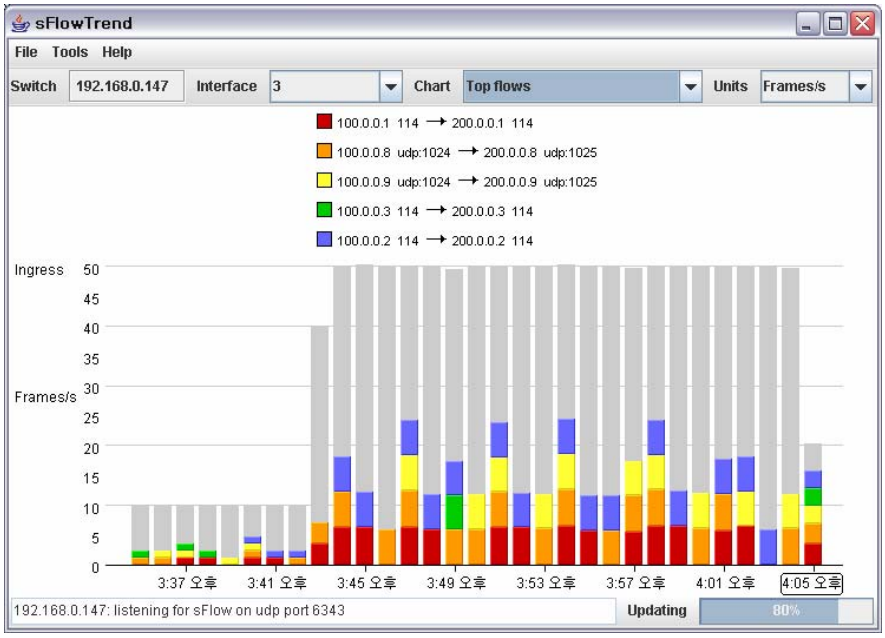
sFlow Sampling Test

sFlow sampling has traffic flow sampling and interface staticstics sampling. You can make sure sampling result via sFlow collector in the above figure.

1. Make traffic per various flows with using SMB and send to Sflow Agent.
2. Do the sampling traffic of port connected with SMB in Sflow Agent.
3. To send this traffic to SFlow collector, set IP Address of SFlow Collector and SFlow Agent.
4. Enable SFlow Service.

```
Switch(config)# interface gi1
Switch(config-if-gi1)# sflow forwarding
 Switch(config-if-gi1)# exit
Switch(config)# sflow agent 192.168.0.147
Switch(config)# sflow destination 192.168.0.200
Switch(config)# service sflow
```

5. To use sFlow Collector, make sure Traffic flow sampling and Interface statistics sampling.



Traffic flow sampling

Interface statistics sampling

Chapter 12. STP and SLD

This chapter explains how to configure the Spanning Tree Protocol (STP) and Rapid Spanning Tree Protocol (RSTP) on the switch.

This chapter includes 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 switch 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 83. 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 84. 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).

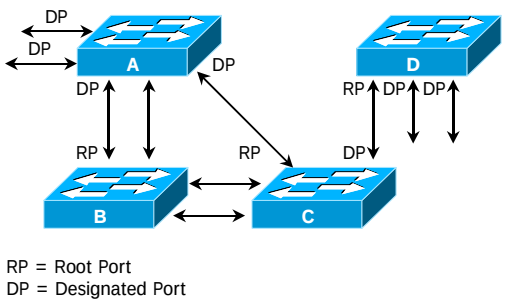


Figure 20. Spanning-Tree Topology

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.

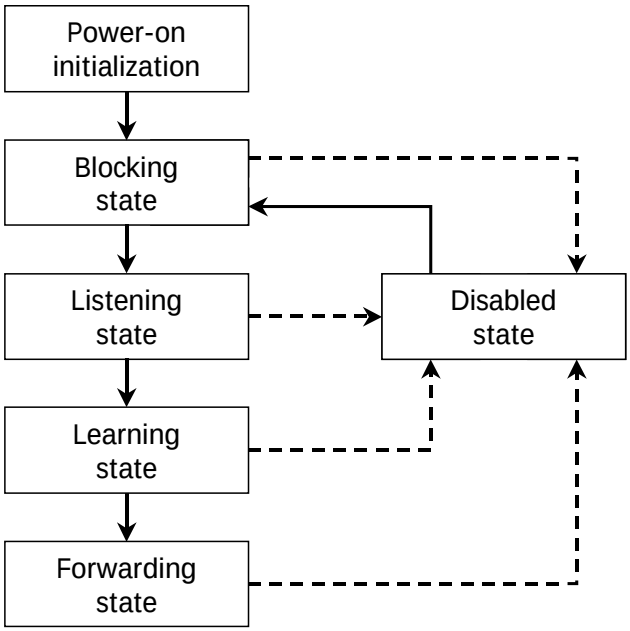


Figure 21. Spanning-Tree Interface States

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

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

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

Blocking State

A Layer 2 interface in blocking state does not forward frames. The switch transfers BPDUs to each interface after initialization. The switch acts as a root switch until it exchanges BPDUs with other switches. One switch of the network is elected as root switch through BPDU exchange. If only one switch is included in the network, BPDU exchange between switches does not occur and the interface goes into listening state after forward-delay timer out. The interface is always set to blocking state after switch initialization.

An interface acts as following in blocking state:

- Drops the frames received through the port
- Drops the frames switched from other interfaces
- Does not perform address learning
- Receives BPDUs

Listening State

Listening state comes after the blocking state. If an interface decides to forward the frames, it goes into listening state.

An interface acts as following in listening state:

- Drops the frames received through the port
- Drops the frames switched from other interfaces
- Does not perform address learning
- Receives BPDUs

Learning State

In learning state, a Layer 2 interface is ready to forward frames. The interface goes from listening state to learning state.

In learning state, an interface acts as follows:

- Drops the frames received through the port
- Drops the frames switched from other interfaces
- Performs address learning
- Receives BPDUs

Forwarding State

In forwarding state, a Layer 2 interface forwards frames. The interface goes from learning state to forwarding state.

In forwarding state, an interface acts as follows:

- Forwards the frames received through the port
- Forwards the frames switched from other interfaces
- Performs address learning
- Receives BPDUs

Disable State

In disabled state, a Layer 2 interface does not participate in frame forwarding or spanning tree.

A disabled interface acts as follows:

- Drops the frames received through the port
- Drops the frames switched from other interfaces
- Does not perform address learning
- Does not receive BPDUs

Understanding RSTP

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

This chapter gives an understanding of RSTP:

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

RSTP Overview

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

Port Roles and the Active Topology

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

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

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

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

Table 85. 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.

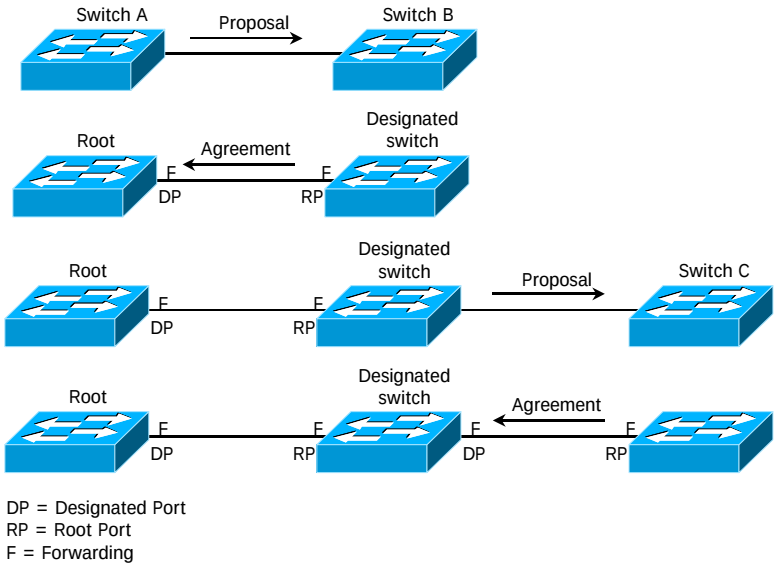


Figure 22. Proposal and Agreement Handshaking for Rapid Convergence

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 86. RSTP BPDU Flags

Bit	Function
0	Topology change (TC)
1	Proposal
2-3: 00 01 10 11	Port role: Unknown Alternate port Root port 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 87. 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 3600 Series switch supports IEEE 802.1w RSTP. As 802.1D STP is internally included in 802.1w, the P8800 Series switch 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:

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

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

Disable per VLAN STP

The P8800 Series switch 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:

		Command	Description
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:

		Command	Description
Step1		**configure terminal**	Enters the global configuration mode.
Stpe2		**interface** *interface-id*	Specifies an interface and enters interface configuration mode. Effective interfaces include physical interfaces and port groups.
Step3		**spanning-tree vlan** *vlan-id* **port-priority** *priority*	Sets a VLAN port priority of the interface. ● *vlan-id* ranges from 1 to 4094. ● *priority* is a multiple of 16 between 0 and 240. The default setting is 128. A smaller number indicates a higher priority. Effective numbers include 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224 and 240. Other values are rejected.
Step4		**end**	Changes to privileged EXEC mode.

Step5		**show spanning-tree interface** *interface-id* or **show spanning-tree vlan** *vlan-id*	Views the settings.
Step6		**copy running-config startup-config**	Stores the (option) settings in the configuration file.

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

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:

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

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

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:

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

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

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:

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

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

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:

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

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

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:

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

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

Configuring the Port as Edge Port

To enable STP in the P8800 Series, 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:

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

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

Configuring the RSTP Mode

You can set protocol mode for each spanning-tree instance of VLAN. In RSTP, a spanning-tree is configured using only RSTP BPDUs 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:

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

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

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:

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

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

Restarting the Protocol Migration Process

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

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

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

Displaying the Spanning-Tree Status

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

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

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

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.

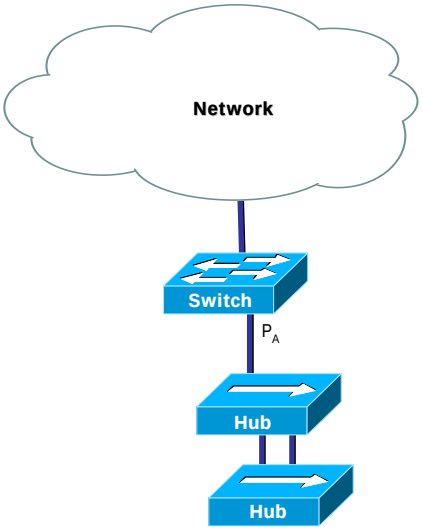


Figure 23. Environment Where a Self-loop is Formed

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.

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

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

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

The following shows an example of enabling self-loop detection for port gi1 with the default limit time:

```
Switch# configure terminal
Switch(config)# interface gi1
Switch(config-if-gi1)# self-loop-detection
Switch(config-if-gi1)# 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:

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

Disabling Self-loop Detection

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

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

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

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

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

```
Switch# configure terminal
Switch(config)# interface gi1
Switch(config-if-gi1)# no self-loop-detection
Switch(config-if-gi1)# 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 gi5. 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 gi5
  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
---------------------------------------------------------------------------
 gi1.    down .   . .    0 .
 gi2.     up   .   . .    0 .
 gi3.    down .   . .    0 .
 gi4.    down .   . .    0 .
 gi5     set    up set 5 min .      1   May 29 04:48:39 2006
 gi6.    down .   . .    0 .
 gi7.    down .   . .    0 .
 gi8.    down .   . .    0 .
Switch#
```

Chapter 13. Configuration saving & Software Upgrade

This chapter describes the procedure for upgrading the system software image. This chapter also discusses how to save booting image and configuration file on P8824XG switch.

Flash File System

This section provides the summary of flash file system, which is built by P8824XG switch to save OS image and configuration profiles in the flash memory.

OS image and configuration profiles are saved and used in our flash file system. A certain space of memory of flash file system is assigned to each file.

The commands are as follow;

Table 88. Command for the File Management

Command	Description	Mode
show flash	• Display Flash File Status and its Contents.	Privileged
erase *filename*	• Erase Flash File Contents.	Privileged
rename *filename1 filename2*	• Change FileName in Flash from FileNAME 1 to FileNAME 2.	Privileged

The following shows an example of results when show flash: command is used. Premier 8000 Series switch shows the file name, file size, and the current (B) and next booting mode (*) information and the type of file as Flash File System information.

```
Switch# show flash:
-length- ----------type/info---------- CN path
8823882 1.4.4 B- p70x.r144
8904920 1.4.5 -* p70x.r145
4164 text file B* default.cfg
3212 Kbytes available (29556 Kbytes used)
```

Configuration Saving

The configuration is the customized set of commands that you have selected to run on the P8824XG switch. Configuration of P8824XG switch consists of Startup-config type and running-config type. The configuration that is saved in the flash memory and loaded when the switch is first started is called startup-config. The configuration running in DRAM is called running-config.

As you make configuration changes, the new settings are stored in DRAM memory. Settings that are stored in DRAM memory are not retained when the switch is rebooted. To retain the settings, and have them be loaded when you reboot the switch, you must save the configuration to the flash memory.

Table 89. Command for Configuration Saving

Command	Description	Mode
show startup-config	• Show the configuration of Booting config File saved in the flash memory	Privileged
show running-config	• Show the current configuration.	Privileged
copy running-config startup-config	• Save running-config as startup-config in the flash memory.	Privileged
copy running-config *filename*	• Save Running-config as Filenam in the flash memory.	Privileged
erase startup-config	• Delete startup configuration file saved in the flash memory.	Privileged
boot config *filename*	• Set filename as Start-up configuration file.	Privileged
rename *filename1 filename2*	• Change file name from filename1 to filename2	Privileged

P8824XG switch saves running configuration with startup or backup configuration File. The following shows an example of saving running-config in the flash memory.

```
P8800SERIES# copy running-config startup-config
Overwrite 'start.cfg'? [yes/no] yes
P8800SERIES#
P8800SERIES#
```

Deleting Configuration File

P8824XG switch reloads the Startup-config in the Flash memory when it is rebooted. If you want to ignore the current Configuration file and use the different file in the system, delete the startup-config as shown in the following example and set the different fiel as startup-config and then, reboot the system.

```
P8800SERIES# erase System1.cfg
Warning: System1.cfg is booting config file
Do you want to erase it [yes/no]? y
P8800SERIES# boot config System2.cfg
P8800SERIES# reload
```

Configuration Backup

P8824XG switch supports backup of system configuration files to TFTP/FTP server on your network. The uploaded configuration file is saved in the format of command-line interface. System Operator can modify the configuration using a text editor, and later download a copy of the file to the same system, or to one or more different systems. For configuration backup, copy running-config command is used.

Table 90. Command for Configuration Backup

Command	Description	Mode
copy running-config tftp/ftp	Upload Running-config from TFTP/FTP server.	Privileged

```
P8800SERIES# copy running-config tftp
IP address of remote host? 192.168.0.3
Name of configuration file to write ? conf.bak

TFTP send: running-config -> 192.168.0.3//conf.bak
continue [yes/no]? yes
Sent 3222 bytes in 0.1 seconds

Successful tftp write
P8800SERIES #
```

Configuration Download

You can download the previously saved configuration from a TFTP or FTP server on your network.

Warning The downloaded configuration is added to the current configuration or replaced with the current configuration on the system. That is, the current system configuration is not totally removed or replaced by the downloaded configuration.

Table 91. Command for Configuration Download

Command	Description	Mode
copy tftp/ftp running-config	Download Running-config file from TFTP/FTP server.	Privileged

```
P8800SERIES# copy tftp running-config
IP address of remote host ? 192.168.0.3
Name of configuration file ? conf.new

TFTP receive: 192.168.0.3//conf.new --> running-config
Continue [yes/no]? yes

Receivecd 3133 bytes in 0.1 seconds

Configuration File Received well
Applying to current configuration from received Configuration File
……
P8800SERIES #
```

Image Upgrade

The System Image File contains the executable file that runs on P8824XG switch. It is pre-installed from the factory. As new versions of the image are released, you should upgrade the software running on your system.

The image is downloaded from either a Trivial File Transfer Protocol (TFTP) or File Transfer Protocol (FTP) server on the network. To start up the system with a new version image after the image upgrade, you have to restart the system.

P8824XG switch can store more than two OS images in Flash memory. System operator chooses Image to update and save it in our flah memory as wanted name. And, choose iamge as booting file and restart.

Warning You have to be very careful when you select the image to upgrade. So follow the directions of our company, since it is very sensitive and dependant on the system model and its version.

Table 92. Command for Image Download

Command	Description	Mode
copy tftp/ftp flash *filename*	Download an image from TFTP/FTP server and save it in the flash memory.	Privileged
boot image *filename*	Set OS Image to load when system is rebooted.	Privileged
rename *source_name destination_name*	Rename from source_name to destination_name	Privileged

```
P8800SERIES# copy tftp flash

IP address of remote host ? 192.168.0.3
Source filename ? P8800_1.img
Destination file name ? first.img
TFTP::192.168.0.3//P8800_1.img --> image file[first.img]
Proceed [yes/no]? yes
Receivecd 501133 bytes in 7.2 seconds
Verify image…
Header..OK
Image Data.. OK
Successful Image verification

Saving image to flash memory
```

```
Image download completed
```

```
P8800SERIES# boot image first.img
P8800SERIES# reload
```

Image/Configuration File Backup

You can save the current OS image/Configuraion File of the system in your server by using Copy command.

Table 93. Image Backup Command

Command	Dscription	Mode
copy flash tftp/ftp	Upload OS image to TFTP/FTP server	Privileged

```
P8800SERIES# copy flash tftp
IP address of remote host ? 192.168.0.3
filename to write on tftp host? first.img
first.img -> TFTP::192.168.0.3//first.img
Proceed [yes/no]? yes
Sent 5218411 bytes in 1.2 seconds

Successful tftp write

P8800SERIES#
```

System Restart

You can restart the system using a command on the consol or turning on/off the power of P8824XG switch.

Warning Before you restart the system, you have to save the current configuration in the flash memory.

```
P8800SERIES# reload
WARNING !!!
  You must save current configuration or you will lose it..

"continue to reboot [yes/no]? yes
P8800SERIES#
```

Chapter 14. IP Account and Snoop Device

This chapter describes the IP Account functions of 8700 Series switch and the snoop devices.

Overview of IP account

The IP account function enables you to observe the performance data by IP information with the commercial S/W program NTOP, through the console and web. You may group the devices to be observed as the Snoop Device.

Commands for IP account

You may observe IP account through console and web. For the latter method, you need to install NTOP.

Show ip account

You may use Show ip account IFNAME to check the IP account on the console.

Table 94. Show ip account

Command	Description	Mode
Show ip account IFNAME	The devices such as gi1, vlan1 and snoop may be used for **IFNAME**.	privileged

```
                        lns ntop v.0.1 [p8k] listening on eth0
210 Pkts/27.9 Kb [IP 21.4 Kb/Other 6.5 Kb]     Thpt: 0.0 Kbps/0.0 Kbps
  Host Act     -Rcvd- Sent    TCP    UDPICMP
  192.168.0.197      B       9.9 Kb     11.5 Kb    727       9.0 Kb 212
  192.168.0.51       B       9.6 Kb      9.8 Kb      0       9.4 Kb 212
  192.168.0.1B       1.9 Kb    727       1.9 Kb      0      0
  00:07:70:42:00:00        S       0       3.9 Kb      0       0      0
  00:07:70:80:01:1B        S       0    414        0       0      0
  00:50:DA:92:A8:0E        S       0     98        0       0      0
```

```
'q' - quit ntop
'r' - reset statistics
'n' - toggle address format (num <-> sym <-> MAC <-> Nw Board Manufact.)
'p' - toggle traffic values (bytes <-> % <-> thpt)
'l' - toggle hosts display (local subnet <-> all)
'd' - toggle idle (idle <-> send/receive)
't' - toggle sort (sent <-> received)
'y' - toggle columns sort
'h' - show this help
' ' - toggle protocol
```

Installing and executing NTOP

To check the IP account on the web, you must download and execute ntop.conf first.

Notice NTOP provides a short-term traffic monitoring. All data are reset after a determined time. .

Downloading ntop.conf

You should download ntop.conf with the command copy tftp config-file or copy ftp config-file.

```
Switch# copy tftp config-file
IP address of remote host ? 192.168.0.1
Source configuration file name ? ntop.conf
Destination configuration file name ? ntop.conf
```

Registering service key

You must register the service key with the command **license.** (See license.)

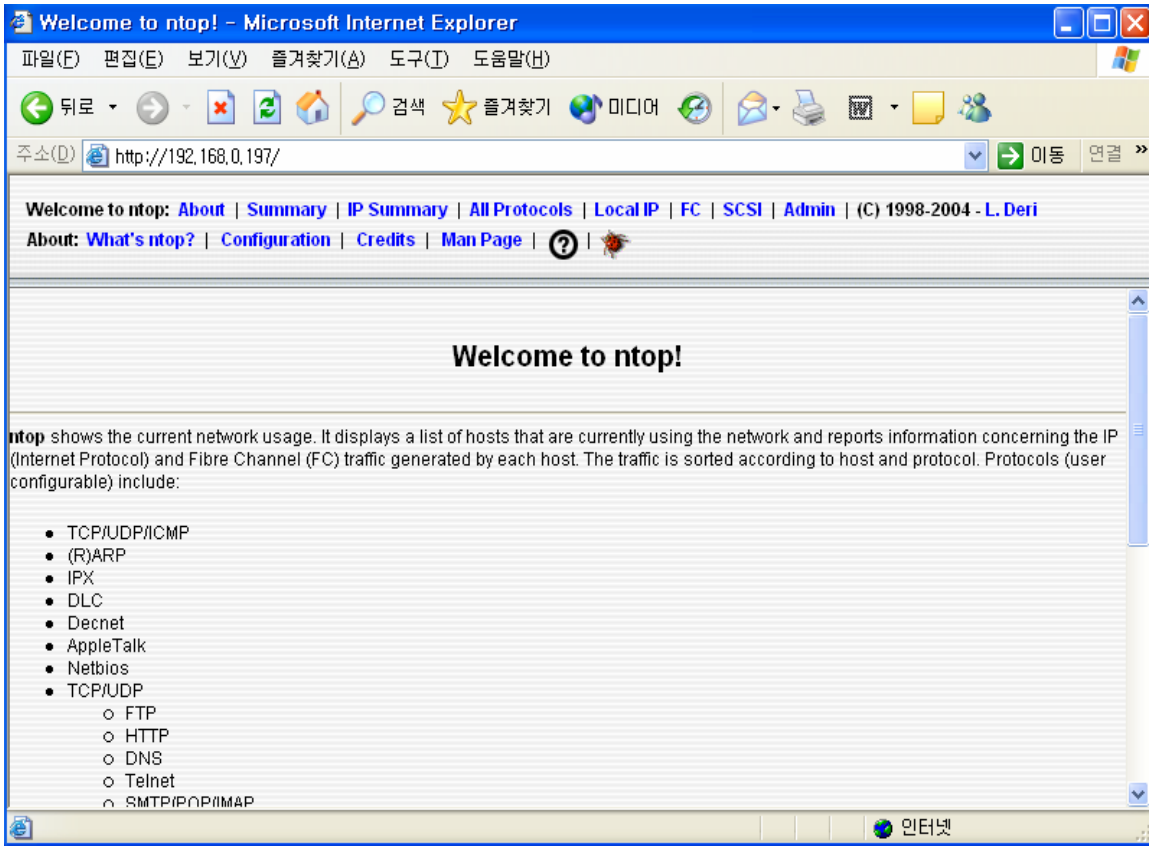
```
Switch # show license

Software is licensed for the following features.

  RIP is enabled
  OSPF is enabled
  BGP is enabled
  PIM-SM is enabled
  IPACC is enabled

Switch #
```

Executing NTOP

Start the ntop service with the command **Service ntop IFNAME**. After executing the service, access the system through the web browser and read the performance data. The follwing figure shows the main screen of ntop.

Table 95. ntop execution/stop commands

Command	Description	Mode
Service ntop IFNAME	The command used to start the Ntop service. The devices such as gi1, vlan1 and snoop may be used for **IFNAME**.	Config
Service ntop IFNAME local A.B.C.D/M	The command used to start the Ntop service including the range of the local network.	Config
No service ntop	The command used to stop the Ntop service.	Config



ntop main screen

Creating protocol list

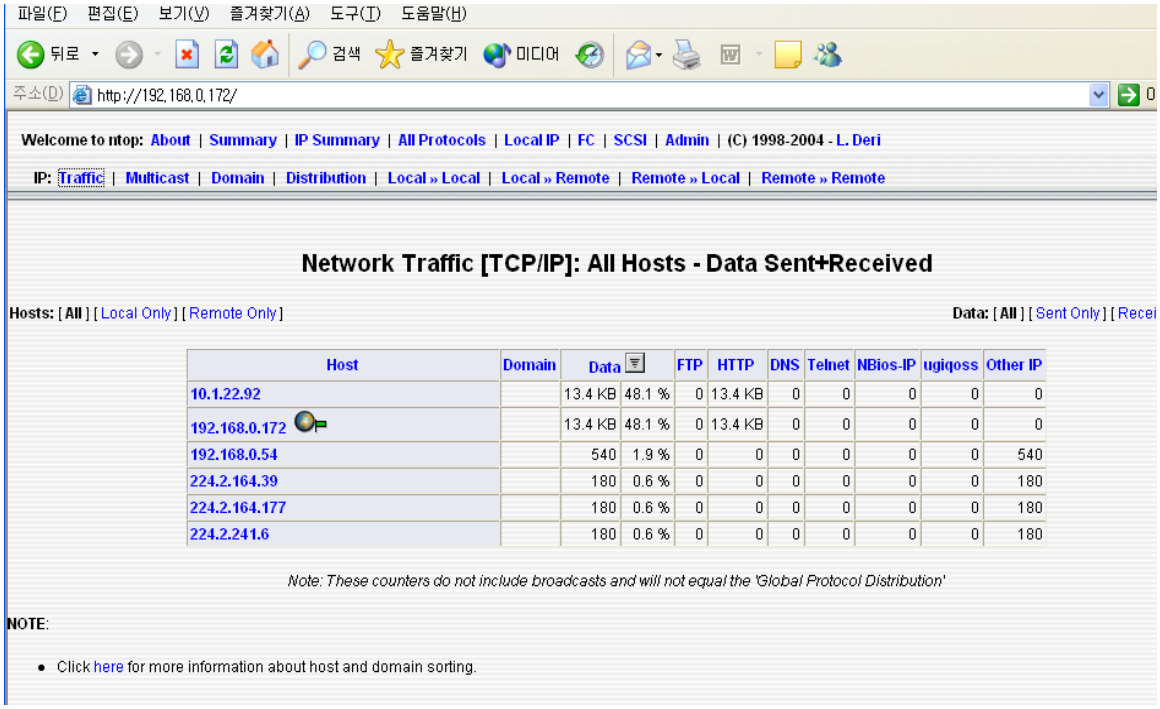
The protocol list function enables you to create/delete the protocol you wish to monitor on NTOP. If you select a protocol list with **ntop protocol-list PROTO_ID_LIST**, it is automatically reflected in the NTOP service.

Table 96. Protocol list commands

Command	Description	Mode
show ntop protocol-list	This command shows the protocol list available for use in Ntop.	privileged
ntop protocol-list PROTO_ID_LIST	This command enables you to select the protocols you wish to observe by referring to **show ntop protocol-list**.	Config
No ntop protocol-list PROTO_ID_LIST	This command releases the protocols you have selected.	
ntop protocol-list create PROTO_NAME	This command creates new protocol lists. (The protocol list is reflected in **show ntop protocol-list.**)	Config
ntop protocol-list delete PROTO_NAME	This command deletes the existing protocol list.	Config

```
Switch (config)# ntop protocol-list create ubiquoss
Switch (config)#exit
```

```
Switch # show ntop protocol-list
  1.FTP=ftp|ftp-data
  2.HTTP=http|www|https|3128
  3.DNS=name|domain
  4.Telnet=telnet|login
  5.NBios-IP=netbios-ns|netbios-dgm|netbios-ssn
  6.Mail=pop-2|pop-3|pop3|kpop|smtp|imap|imap2
  7.DHCP-BOOTP=67-68
  8.SNMP=snmp|snmp-trap
  9.NNTP=nntp
  10.NFS=mount|pcnfs|bwnfs|nfsd|nfsd-status
  11.X11=6000-6010
  12.SSH=22
  13.Gnutella=6346|6347|6348
  14.Kazaa=1214
  15.WinMX=6699|7730
  16.eDonkey=4661-4665
  17.Messenger=1863|5000|5001|5190-5193
  18.ubiquoss=4000-4001|5000
Switch #con t
Switch (config)# ntop protocol-list 1-5,19
Switch (config)# service ntop snoop1 local 192.168.0.0/24
```



Protocol items for creation of protocol list

Snoop device

Snoop device commands are used to monitor a specific device or multiple devices with the IP account function.

Table 97. Snoop device commands

Command	Description	Mode
Snoop device <1-100>	This command creates a snoop device. Snoop device id 1 has the device name 'snoop1'.	Config
No snoop device <1-100>	This command deletes the snoop device.	Config
Snoop device <1-100> add IFNAME	This command adds an interface to the snoop device. gi1 or vlan1 may be used for IFNAME.	Config
Snoop device <1-100> delete IFNAME	This command deletes the interface from the snoop device.	Config

Chapter 15. CPU-FILTER & IP-OPTION

This chapter describes how to set CPU-Filter and IP-OPTION

CPU Filtering

P8824XG provides the filtering function for the traffic incoming to the switch or being forwarded through CPU of the switch. With the following commands, you may set the filtering function by IP address, protocol or port.

Establishing/unestablishing CPU-filtering rule

In order to filter packets, you should establish the appropriate rule. The CPU-filtering rule may be applied via various methods including protocol, src/dest IP and UDP/TCP Port. In order to apply the CPU-filtering rule, you should run the following commands in the global mode.

Table 98. CPU-filtering rule

Command	Description
cpu-filter rule *NAME* **ip { *srcIP* | *srcIP/M* | any } { *dstIP* | *dstIP/M* | any } match { permit | deny }**	■ CPU-filter for IP protocols ■ CPU-filter is applied based on the source address and the destination address. ■ The match command is used to determine whether to allow the classified packets.
cpu-filter rule *NAME* **tcp { *srcIP* | *srcIP/M* | any } { *dstIP* | *dstIP/M* | any } { *srcPort* | any } { *dstPort* | any } match { permit | deny }**	■ CPU-filter for TCP protocols ■ CPU-filter is applied based on the source / destination address and the source / destination port number. ■ The match command is used to determine whether to allow the classified packets.
cpu-filter rule *NAME* **udp { *srcIP* | *srcIP/M* | any } { *dstIP* | *dstIP/M* | any } { *srcPort* | any } { *dstPort* | any } match { permit | deny }**	■ CPU-filter for UDP protocols ■ CPU-filter is applied based on the source / destination address and the source / destination port number. ■ The match command is used to determine whether to allow the classified packets.

To unestablish the above CPU-filter rules, you should use the following command in the configure mode.

Table 99. Unestablishing cpu-filter rule

Command	Description
no cpu-filter rule *NAME*	■ NAME : Name of the established CPU-filter.

Establishing CPU-FILTER group

To apply the CPU-Filter to the system, you should add the CPU-Filter rule to the CPU-Filter group. In the P8824XG switche, you may establish two groups: Input group and Output group. Input group

is a filter group for the traffic incoming to the system, and forward group is the filter group for the traffic being routed through the CPU of the switch. Numbers of rules may be applied to CPU-Filter groups, and the rules are applied in the order of rules added to the group. Therefore, the sequence of rules applied to the group is important. Two types of CPU-Filter group are supported, and the sequence of application can be found with show cpu-filter group.

Establishing/unestablishing INPUT group

To apply Input CPU-Filtering Group, you should use the following commands in the global mode.

Table 100. CPU filter group

Command	Description
cpu-filter group input add *NAME*	■ NAME : Name of the rule to be added
cpu-filter group input add *NAME1* **{ above | below }** *NAME2*	■ This command inserts a new rule to the relative position of the existing rules in the group. ■ NAME1 : Name of the new rule to be added to the group. ■ NAME2 : Name of the existing rule in the group. ■ above : Insert NAME1 above NAME2. ■ below : Insert NAME1 below NAME2.

To delete a rule from the Input CPU-Filtering group, you should run the following command in the global mode.

Table 101. cpu-filter group

Command	Description
cpu-filter group input delete *NAME*	■ NAME : Name of the rule to be deleted from the group.
cpu-filter group input delete all	■ Deletes all rules from the group.

Establishing/unestablishing FORWARD group

To apply Forward CPU-Filtering Group, you should run the following commands in the global mode.

Table 102. cpu-filter group forward

Command	Description
cpu-filter group forward add *NAME*	■ NAME : Name of the rule to be added to the forward group
cpu-filter group forward add *NAME1* **{ above | below }** *NAME2*	■ This command inserts a new rule to the relative position of the existing rules in the group. ■ NAME1 : Name of the new rule to be

	added to the group. ■ NAME2 : Name of the existing rule in the group. ■ above : Insert NAME1 above NAME2. ■ below : Insert NAME1 below NAME2.

Activating CPU-FILTER service

After establishing a CPU-Filtering group, to apply the rules to the system, you should run the following commands in the global mode.

Table 103. Service cpu-filter

Command	Description
service cpu-filter	■ Activate CPU-FILTER
no service cpu-filter	■ Deactivate CPU-FILTER

Example of establishing CPU-FILTER

The following example shows how to disallow all TELNET packets incoming to the switch.

Table 104. Example of cpu-filter

```
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 example shows how to disallow FTP traffic routed by CPU of the switch.

Table 105. How to disallow FTP traffic

```
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 example shows how to view the CPU-FILTER group established for the switch.

Table 106. show cpu-filter group

```
Switch# show cpu-filter group
----------------------
INPUT   GROUP-LIST      :
----------------------
telnet
----------------------
```

```
FOWARD GROUP-LIST       :
----------------------
ftp
----------------------
total 2group-list found
```

The following example shows how to view the CPU-FILTER rule established for the switch.

Table 107. show cpu-filter

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

Overview of IP Option

The IP option enables you to establish/unestablish the attack-preventive parameters under /proc/sys/net/ipv4 of linux kernel.

IP option commands

The following parameters are available for establishment with the IP option commands.

Table 108. IP option commands

Command	Description	Mode
ip option secure_redirect INTERFACE (default|disable|enable)	Enable/disable delivery of the ICMP redirect messages to the gateways on the default gateways list only. **Default) enable**	config
ip option send_redirects *INTERFACE* **(***default|disable|enable***)**	Enable/disable delivery of ICMP redirect messages to other hosts when the router works. **Default) enable**	config
ip option icmp_port_unreach *INTERFACE* **(***default|disable|enable***)**	Enable/disable Icmp port unreachable **Default) disable**	config
ip option icmp_host_unreach *INTERFACE* **(***default|disable|enable***)**	Enable/disable Icmp host unreachable **Default) disable**	config
ip option icmp_net_unreach *INTERFACE* **(***default|disable|enable***)**	Enable/disable Icmp net unreachable **Default) disable**	config
ip option icmp_prot_unreach *INTERFACE* **(***default|disable|enable***)**	Enable/disable Icmp prot unreachable **Default) disable**	config
ip option tcp_max_syn_backlog VALUE	Max. value of the Tcp syn backlog queue. **Default) 1024**	config
ip option ip_default_ttl *VALUE*	Default TTL size. **Default) 64**	config
ip option ipfrag_time VALUE	The time the fragmented IP data is in the memory. **Default) 30**	config
ip option tcp_syn_retries VALUE	The time for retry for activated TCP connection before sending the reset SYN packet. **Default) 5**	config
ip option tcp_retries1 VALUE	Number of retries for doubtful tcp session. **Default) 3**	config
ip option tcp_retries2 VALUE	Number of retries before termination. **Default)15**	config
ip option tcp_keepalive_time *VALUE*	Activated keepalive time. **Default) 7200**	config
ip option tcp_fin_timeout *VALUE*	FIN-WAIT-2 socket timeout. **Default) 60**	config
ip option tcp_max_tw_buckets *VALUE*	Timewait socket count. **Default) 18700**	config
ip option tcp_keepalive_probes VALUE	Keepalive probe messages to be generated until the disconnection is considered. **Default) 9**	config
ip option tcp_syncookies	Enable/disable protection against syn	config

(*default*|*disable*|*enable***)**	flood attack. **Default) enable**	
ip option tcp_send_reset (*default*|*disable*|*enable***)**	Enable/disable Tcp send reset flag **Default) enable**	config
(no) ip option icmp-ttl-exceed-send	Send TTL Exceed ICMP **Default) send**	config

Chapter 16. VRRP

This chapter describes the VRRP configuration of system.

Virtual Router Redundancy Protocol (VRRP) is a protocol that allows two or more routers to have same virtual IP address to provide multiple access routes in the LAN, with one of the routers elected as a virtual router. VRRP router uses VRRP protocol to communicate with other routers connected to the LAN. If a router is elected as a master virtual router in VRRP configuration, the other routers will stand by as backup in case of any failure in the master virtual router.

Information about VRRP

VRRP Operation

There are several ways that a LAN client may choose to elect the first hop router for any specific destination. The client can use dynamic or static setting methods. The following example shows a dynamic election of router:

- Proxy ARP – The client uses Address Resolution Protocol (ARP) to get its own destination and the router will reply to the ARP request using its own MAC address.
- Routing protocol – The client creates its own routing table using update information in the dynamic routing protocol.
- IRDP (ICMP Router Discovery Protocol) client – The client runs Internet Control Message Protocol (ICMP) router discover client.

The headache in configuration of LAN clients and operations of protocol is one of major demerits of dynamic protocol. Moreover it can be slower to switch to other routers when there is a failure in the router.

One of alternatives to the dynamic protocol is to set a default router for the clients. This method is very simple in terms of client configuration and operation. But if there is any failure in the default gateway, the LAN client will be disconnected from the external network.

VRRP can solve static configuration problems. VRRP allows router groups to form a virtual router. LAN client elects the virtual router as its own default gateway. The virtual router standing for the router group is also called VRRP group.

Figure 1 illustrates the topology of LAN with VRRP set. In this example, the router A, B and C are the VRRP routers (VRRP running routers) that consists virtual routers. The IP address of the virtual router is set to the IP address same as that of the router A (10.0.0.1).

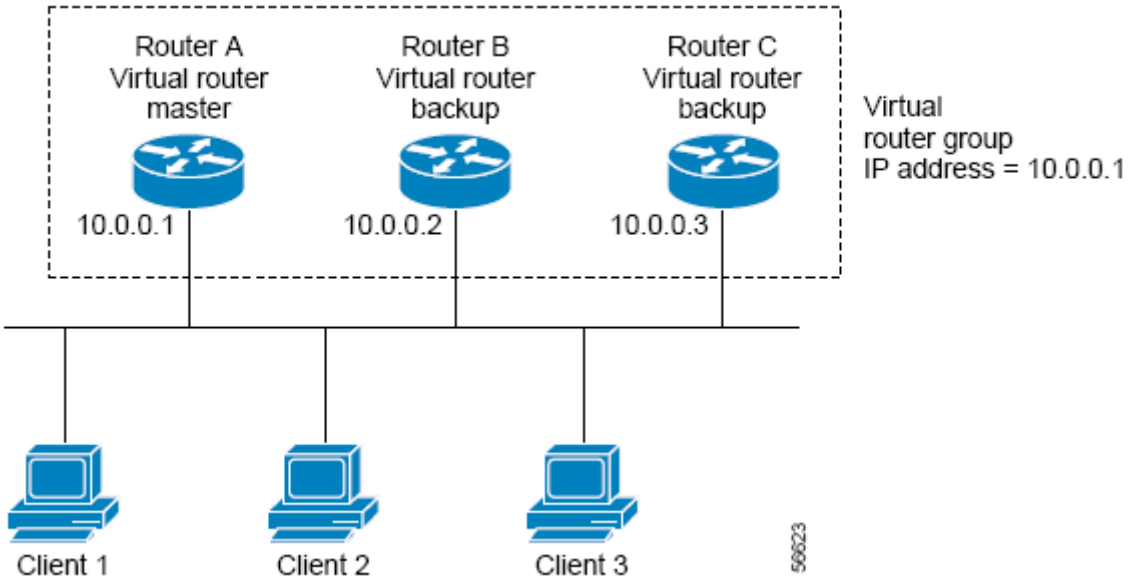


Figure 24. Basic VRRP Topology

Because the virtual router uses the physical address of the router A, router A takes the role of master virtual router and is called IP address owner. The router A, as the master virtual router, controls the IP address of the virtual router, and takes in charge of forwarding of packets forwarded to this IP address. Set the IP address of the default gateway to 10.0.0.1 for Client 1 through 3.

The router B and C work as backup virtual routers. If there is a failure in the master virtual router, the router with higher priority becomes the master virtual router to continue provision of services to the LAN hosts. If the router A is recovered from the failure, it becomes the master virtual router again.

The following figure shows the example in which the VRRP is set to make the router A and the router B share the traffic. The router A and the router B work as backup virtual routers for each other.

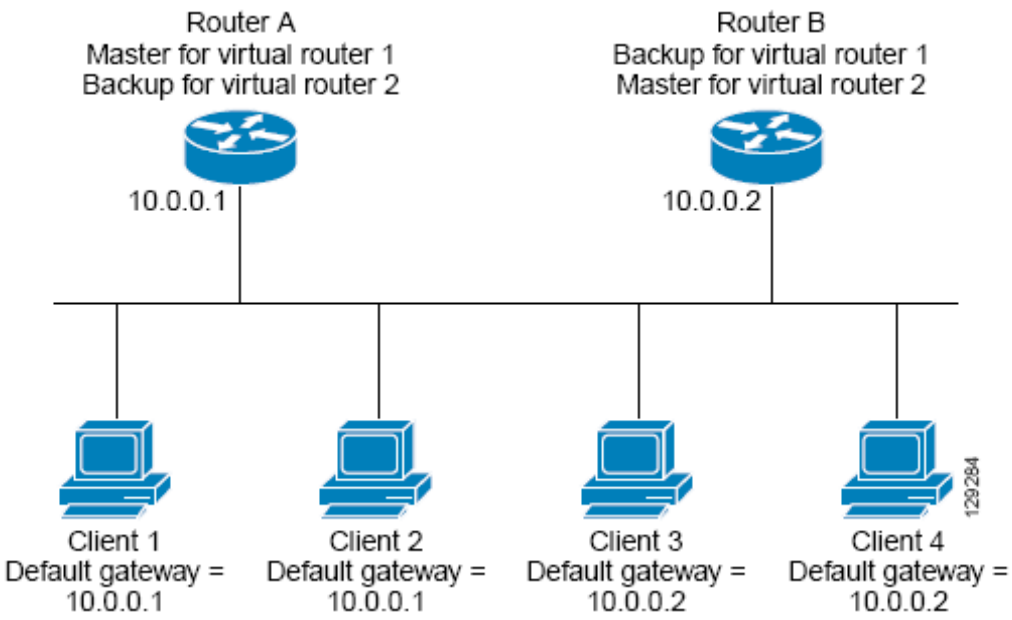


Figure 25. Load Sharing and Redundancy VRRP Topology

In this topology, two virtual routers are configured. In the virtual router 1, the router A is the host of IP address 10.0.0.1 and the master virtual router, while router B is the backup virtual router for the router A. Client 1 and 2 use 10.0.0.1 for the IP address of the default gateway.

In the virtual router 2, the router B is the owner of IP address 10.0.0.2 and the master virtual router, and the router A is a backup virtual router for the router B. The client 3 and the client 4 use 10.0.0.2 for the IP address of the default gateway.

VRRP Benefits

Redundancy

VRRP enables you to set two or more routers as default gateway router. This decreases the risk of single point of failure in the network.

Load Sharing

VRRP can be set to make the traffic from LAN clients to be distributred to multiple routers. In this way, the load of traffics can be distributed to several routers.

Multiple Virtual Routers

VRRP supports up to 255 virtual routers (VRRP group). By supporting several virtual routers, it is possible to support redundancy and load sharing in the LAN configuration.

Preemption

The redundancy scheme of VRRP allows the router with higher priority, when it becomes available, to be elected as the master virtual router on behalf of other backup virtual routers.

Advertisement Protocol

VRRP uses exclusive Internet Assigned Numbers Authority (IANA) standard multicast address

(224.0.0.18) for VRRP advertisement. IANA assigns the IP protocol No. 112 to VRRP.

VRRP Object Tracking

VRRP object tracking allows the best VRRP router to be the master virtual router by changing VRRP priority depending on the state of interface or IP route.

Multiple Virtual Router Support

For single physical interface of a router, maximum 255 virtual routers can be set. The number of actual virtual routers that a router can support is affected by the following factors:

- Process capability of the router
- Memory capacity of the router
- Maximum number of MAC addresses that the interface of router can provide

VRRP Router Priority and Preemption

One of important factors in VRRP redundance function is VRRP router priority. If there is a failure in the master virtual router, the role of VRRP router is determined according to the priority.

If a VRRP router has the IP address of the virtual router as the IP address of its own physical interface, this router works as the master virtual router.

The priority becomes the basis for electing the master virtual router among the VRRP routers working as back virtual routers when there is a failure in the master virtual router. *vrrp priority* command can be used to set the priority of backup virtual routers in the range of 1 ~ 254.

For example, if there is a failure in the router A, that is, the master virtual router in the LAN, alternative master virtual router should be elected among the backup virtual router B and C according to the election procedure. If the priority of the router B and the router C is set to 101 and 100 respectively, the router B becomes the master virtual router since its priority is higher. If the priority of both router B and router C is set to 100, the backup virtual router with higher IP address will be elected as the master virtual router.

The preemptive scheme will be applied to allow the backup virtual router with higher priority to become the master virtual router. ***no vrrp preempt*** command can be used to bring preemptive scheme to an end. If Preemption is inactivated, the backup virtual router that has become the master virtual router continues to carry out the role of the master till the original master virtual router is recovered to become the master again.

VRRP Advetisements

The master virtual router transmits the VRRP advertisement to other VRRP routers in the same group. In this Advertisement, the priority and status information of the master virtual router are included. VRRP advertisement is made in IP packet and transmited to the IPv4 multicast address assigned to the VRRP group. The advertisement is transmitted every second by Default, and the transmission interval can also be set.

VRRP Object Tracking

Object tracking is an independent process that generates and monitors objects such as line-protocol status of the interface etc, and manages their removal. The clients like VRRPs register the

objects to track their change status.

The object to be tracked has a unique number assigned by the tracking comman-line-interface (CLI). The client processes such as VRRP specify the object to track using this number.

In the Tracking process, the status of objects is checked periodically and any change in the status value is notified to the clients. The status value of objects is expressed either in up or down.

Throughout the tracking process, VRRP can track the status change of all the objects. Tracking process provides the function to track the status of each object such as line protocol status of the interface and reachability of the route etc.

Each VRRP group can track several objects affecting the priority of VRRP routers. If the number of object to track is specified, VRRP can detect the change status of the object. VRRP increases or decreases the priority value of the virtual router according to the status of object to track.

How to Configure VRRP

This section covers the following procedures:

- Enabling VRRP
- Disabling VRRP on an Interface
- Configuring VRRP Object Tracking

Enabling VRRP

To enable VRRP, do the following steps.

	Command or Action	Description
Step 1	**configure terminal** **Example:** Switch# **configure terminal**	To enter into Global configure mode
Step 2	**interface** *interface-name* **Example:** Switch(config)# **interface vlan1**	To enter into Interface configuration mode.
Step 3	**ip address** *ip-address/prefix-length* **Example:** Switch(config-if-vlan1)# **ip address 172.16.6.5/24**	To set the IP address of the interface.
Step 4	**vrrp** *group* **ip address** *ip-address* **Example:** Switch(config-if-vlan1)# **vrrp 10 ip 172.16.6.5**	To enables VRRP on the interface. **Note:** All the routers in the VRRP group should be set to the same IP address. If other IP address is to be set, the routers in the VRRP group can't communicate with each other, and the router with wrong configuration will work as the master by itself.
Step 5	**end** **Example:** Switch(config-if-vlan1)# **end**	To returns to the privileged EXEC mode
Step 6	**show vrrp** [**brief**	*group*] **Example:** Switch# **show vrrp 10**	(option) To checks the status info of VRRP group of the router.
Step 7	**show vrrp interface** *interface-name* [**brief**] **Example:** Switch# **show vrrp interface vlan1**	(option) To check the information of VRRP group set in the specific interface.

Disabling VRRP on an Interface

It's possible to disable only the protocol operation while keeping VRRP settings, by disabling VRRP on the interface.

show running-config command can be used to check the settings of the VRRP group and whether the VRRP is working or is disabled.

	Command or Action	Description
Step 1	**configure terminal** **Example:** Switch**# configure terminal**	To enter into Global configure mode
Step 2	**interface** *interface-name* **Example:** Switch(config)**# interface *vlan1***	To enter into Interface configuration mode.
Step 3	**ip address** *ip-address/prefix-length* **Example:** Switch(config-if-vlan1)**# ip address 172.16.6.5/24**	To set the IP address of the interface.
Step 4	**vrrp** *group* **shutdown** **Example:** Switch(config-if-vlan1)**# vrrp 10 shutdown**	To shutdown VRRP on the interface. **Note:** The VRRP can be shutdown while VRRP settings are kept.

Configuring VRRP Object Tracking

To set VRRP object tracking, please follow the following steps.

If the VRRP group is the host of the IP address, the priority of the VRRP group will be fixed to 255, and the priority will not be changed through object tracking.

	Command or Action	Description
Step 1	**configure terminal** **Example:** Switch**# configure terminal**	To enter into Global configure mode
Step 2	**track** *object-number* **interface** *interface-name* { **line-protocol	ip routing** } **Example:** Switch(config)**# track 2 interface vlan1 line-protocol**	To set the interface that affects the priority of VRRP group. - Use this command to set the interface. For ***vrrp track*** command, the corresponding object number is used. - ***line-protocol*** key word is to track whether the status of the interface is 'up' or not. ***ip routing*** key word

		is to track whether an IP address is set and the status of the interface is 'up'. - ***track ip route*** command can be used to check the reachability of specific IP route.
Step 3	**interface** *interface-name* **Example:** Switch(config)**# interface vlan10**	To enter into Interface configuration mode.
Step 4	**ip address** *ip-address/prefix-length* **Example:** Switch(config-if-vlan10)# **ip address 10.0.1.1/24**	To set an IP address of interface.
Step 5	**vrrp** *group* **ip address** *ip-address* **Example:** Switch(config-if-vlan10)# **vrrp 10 ip 10.0.1.20**	To enable VRRP on the interface and set the IP address of the virtual router.
Step 6	**vrrp** *group* **priority** *leve* **Example:** Switch(config-if-vlan10)# **vrrp 10 priority 120**	To set the priority of VRRP router.
Step 7	**vrrp** *group* **track** *object-number* [**decrement** *priority*] **Example:** Switch(config-if-vlan10)# **vrrp 10 track 2 decrement 15**	To set VRRP to track the status of the objects.

Configuration Examples for VRRP

Configuring VRRP: Example

In the following examples, the switch A and the switch B belong to 3 VRRP groups.

The configuration of each group is as follows:

- Group 1:
  - The virtual IP address is 10.1.0.10.
  - The switch A becomes the master of this group, since its priority value is 120.
  - Advertising interval is 3 seconds.
  - Preemption is activated.
- Group 5:
  - The switch B becomes the master of this group, since its priority value is 200.
  - Advertising interval is 30 seconds.
  - Perrmption is inactivated.
- Group 100:
  - The switch A becomes the master of this group, since it has highest IP address (10.1.0.2).
  - The Advertising interval is 1 second by default.
  - Preemption is inactivated.

Router A

```
interface vlan1
  ip address 10.1.0.2/8
  vrrp 1 priority 120
  vrrp 1 timers advertise 3
  vrrp 1 ip 10.1.0.10
  vrrp 5 timer advertise 30
  vrrp 5 ip 10.1.0.50
  no vrrp 100 preempt
  vrrp 100 ip 10.1.0.100
```

Router B

```
interface vlan1
  ip address 10.1.0.1/8
  vrrp 1 timers advertise 3
  vrrp 1 ip 10.1.0.10
  vrrp 5 priority 200
  vrrp 5 timer advertise 30
  vrrp 5 ip 10.1.0.50
  no vrrp 100 preempt
  vrrp 100 ip 10.1.0.100
```

VRRP Object Tracking: Example

In the following examples, the tracking process is set to track the line protocol status of interface vlan10. VRRP on the interface vlan1 is registered to the tracking process to be able to get the information on changes of protocol status in the interface vlan10. If the line protocol status of interface vlan10 turns to down, the priority value of VRRP group decreases by 15.

```
track 1 interface vlan10 line-protocol
!
interface vlan1
   ip address 10.0.0.2/8
   vrrp 1 ip 10.0.0.3
   vrrp 1 priority 120
   vrrp 1 track 1 decrement 15
```

VRRP Object Tracking Verification: Example

The following example is to track the settings made in “VRRP Object Tracking: Example” section:

```
Switch# show vrrp
vlan1 – Group 1
   State is Master
   Virtual IP address is 10.0.0.3
   Virtual MAC address is 0000.5e00.0101
   Advertisement interval is 1 sec
   Preemption is enabled
   Priority is 105
     Track object 1 state Down decrement 15
   Master Router is 10.0.0.2 (local) priority is 105
   Master Advertisement interval is 1 sec
   Master Down interval is 3.531 sec

Switch# show track

Track 1
   Interface vlan10 line-protocol
   Line protocol is Down (hw down)
     1 change, lasst change 00:06:53
   Tracked by:
     VRRP vlan1 1
```

Disabling a VRRP Group on an Interface: Example

The following example explains how to shutdown the VRRP group on interface vlan1 while keeping the settings of interface VRRP group:

```
interface vlan1
   ip address 10.24.1.1/24
   vrrp1 ip 10.24.1.254
   vrrp 1 shutdown
```

Chapter 17. Utilities

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

Status dump command

Command

“show tech” is used to dump the system logging messages of each module (system configuration, multicast, routing, driver, etc.).

```
# show tech
```

If a problem occurs in system operation, you need to enter various commands to check the behavior of the modules. This command makes predefined critical commands run for the modules, and shows the result message, enabling the module admins to check the fault immediately.

Because the output messages are not paged, the output of messages continue until running of the command is finished. In order to stop the output during the running of the command, you should enter Ctrl+C.

See the following example.
Show tech command provides considerable amount of load to CPU, and it takes a long time to process the command.
As CPU continues to run at 100%, there can be a routing interruption. Therefore, the program requests the operator to confirm whether to run the command.

Table 109. show tech

```
Switch# show tech

NOTICE !!!
  This may take a few minutes and may take up the CPU resources!!
continue to process [yes/no]?y

=========================================================================
  Display the system information
=========================================================================
Model Name      : P8824XG
Main Memory Size    : 256 MB
Flash Memory Size : 32 MB
H/W Revision : Rev 9.1
H/W Address    : 00:07:70:a4:36:a9
RTC Information      : Installed
Serial Number: P25M05171234

=========================================================================
     Display the system version
=========================================================================
```

```
P8624XGB Software Version 1.4.1h
Copyright (c) 2001-2008 by Ubiquoss Inc.
...
================================================================================
   CPU information
================================================================================
----------------------------------------
   Average CPU load
----------------------------------------
   5 sec :     1.20%
   1 min :    10.36%
   5 min :     3.50%
----------------------------------------
   cpuload threshold (high) :     0%
   cpuload threshold ( low) :     0%
   cpuload time period : 1 Minutes
----------------------------------------

================================================================================
      Current operating configuration
================================================================================
!
vlan 33
vlan 44
vlan 2000
!
interface gi1/2
 shutdown
 switchport access vlan 33
!
interface gi2/1
 switchport access vlan 44
!
interface vlan33
 ip address 33.33.33.2/24
!
interface vlan44
 ip address 44.44.44.2/24
!
interface vlan2000
 ip address 198.19.1.250/24
!
interface eth0
 ip address 192.168.0.144/24
!
interface lo0
```

```
  ip address 58.229.2.143/32
!
!
ip igmp snooping
ip igmp snooping vlan 2000
!
```

Command history

This function shows the commands performed by the operator with the operator id, ip and time data. This function only provides the data on the normally executed commands only, and the commands which can be anticipated (e.g., exit, end, etc.) are excluded.

Table 110. Command history view and setting commands

Command	Description	Mode
show history	■ Show the executed commands.	Privileged
show history back	■ Show the executed commands in the reverse time order.	Privileged
show history flash	■ Show the executed commands stored in the Flash memory. You can view the commands which had been executed before the system rebooting.	Privileged
show history flash back	■ Show the executed commands stored in the Flash memory in the reverse time order. You can view the commands which had been executed before the system rebooting.	Privileged
clear history	■ Clear the commands history.	Privileged
clear history flash	■ Clear the commands history in the Flash memory.	Privileged
history flash {enable|disable}	■ Determine saving of commands in the Flash memory. Default is ‘enable.’	Config

To increase efficiency of commands, the system is designed to store the command history in the flash memory so that the operator can view the commands even if the system is down or rebooted. Because this function is enabled in default, the commands are stored in the flash memory unless you disable it.

This function shows the history of commands performed by the operator, facilitating analysis and clearance of system fault.

The repeated command is saved once.

Output Post Processing

Overview of output post processing

Most of the commands that show the current status or setting of a system begins with ‘show’. The show commands generally show the results on a page, but there are cases that the result is very long.

For example, show mac-address-table may result in thousands of lines, and show interface also provide considerable amount of result. If the result is very long, it is difficult to find the desired part. In this case, you may use the output post processing function provided by this system.

This function is similar with the Unix pipe function. This system provides 3 predefined output post processing functions. In order to use the output post processing function, you should attach a bar (|) after the show command, and then, use the following commands.

Table 111. output post processing

Command	Description
| include WORD	■ Show the string containing a specific word.
| exclude WORD	■ Show the string without a specific word.
| begin WORD	■ Show the lines after a string containing a specific word.

Example of output post processing

‘show mac-address-table’ outputs a large amount of results. You should use ‘include’ to get the mac addresses containing the desired part only.

Table 112. output post processing

```
Switch#
Switch# show mac-address-table | include 0007.70
     2      gi1   0007.7089.1123 0-0   F-F   UD.
     3      gi2   0007.709e.000b 0-0   F-F   UD.
    13     gi3   0007.701e.4dac 0-0   F-F   UD.
    13     gi4   0007.7089.1123 0-0   F-F   UD.
    13     gi5   0007.7092.40f6 0-0   F-F   UD.
    13     gi6   0007.7093.cca2 0-0   F-F   UD.
    13     gi7   0007.709e.1000 0-0   F-F   UD.
    13     gi8   0007.709f.5934 0-0   F-F   UD.
    20     gi9   0007.7042.0001 0-0   F-F   UD.
Switch #
```

‘show ip interface’ outputs a large amount of results. You should use ‘begin’ to get the result after a specific vlan interface.

Table 113. show ip interface

```
Switch#
Switch# show ip interface | begin vlan10
vlan10 is up
  type: vlan interface
  ip address: 10.1.10.1/24 broadcast address 10.1.10.254

  Cpu packet counters since creation
     4 packets input, 208 bytes
     Received 4 unicasts, 0 non-unicasts
     0 dropped, 0 errors
     6 packets output, 309 bytes

vlan11 is up
  type: vlan interface
  ip address: 10.1.11.1/24 broadcast address 10.1.11.255

  Cpu packet counters since creation
     1,057,364 packets input, 54,984,438 bytes
     Received 1,160 unicasts, 1,056,204 non-unicasts
     156 dropped, 0 errors
     6,560 packets output, 311,183 bytes
(omitted)

Switch #
```

DDM (Digital Diagnostic Monitoring)

P8824XG provides the command that shows detailed status of GBIC that supports DDM. You may set the threshold for the monitoring items of GBIC port, over which the system reports the incident to the user. The following table shows the items to be monitored.

Table 114. Digital Diagnostic Monitoring

Item	Description	Threshold range
Temperature	GBIC Port temperature	-128°C ~ 128°C
Voltage	GBIC Port voltage	0V ~ 6.55V
Current	GBIC Port current	0mA ~ 131mA
RxPower	GBIC Port optical input power	- 40dBm ~ 8.0dBm
TxPower	GBIC Port optical output power	- 40dBm ~ 8.0dBm

For each test item, 2 stage thresholds (alarm/warning) are provided. The switch monitors the GBIC port status at an interval of 5 minutes, and reports the threshold-crossed incidents to the user.

DDM Monitoring enable/disable (No command)

The DDM monitoring function of the P8K Switch is off in default. If you wish to log the GBIC status with the DDM function, you should activate the DDM monitoring function.

Table 115. DDM Monitoring enable/disable

Command	Mode	Description
gbic-ddm alarm enable	Config	Enable DDM Monitoring
gbic-ddm alarm disable	Config	Disable DDM Monitoring

Router**# configure terminal**
Router(config)**# gbic-ddm alarm enable**
Router(config)**# gbic-ddm alarm disable**

Even if the DDM monitoring function is disabled, you can set the threshold range, and view the current values of the GBIC monitoring items.

GBIC status check

With the following commands, you can view the current status of gbic that supports DDM.

Table 116. show port status gbic

Command	Mode	Description
show port status gbic-ddm	Privileged	Show the status of gbic that supports DDM.

Router**# show port status gbic-ddm**

```
 ifname gbic     ddm    TemperatureVoltage Bias CurrentTx Power    Rx Power
 (state)    (state)    (state)    (state)    (state)
 (warn)     high     lowhigh     lowhigh     lowhigh     lowhigh     low
(alarm)     high     lowhigh     lowhigh     lowhigh     lowhigh     low
-------------------------------------------------------------------------------------------
 gi1       gbic     ddm48.5'C       3.5 V       21.7 mA    -6.00 dBm-40.00 dBm
   Normal       Normal       Normal     Alarm(H)     Normal
 (warn)   127.0 -128.06.6       0.0     131.0       0.0    -12.73 -40.00    -12.73 -40.00
(alarm)   127.0 -128.06.6       0.0     131.0       0.0    -12.73 -40.00    -12.73 -40.00
.....................................................................................
 gi2.
.....................................................................................
 gi3       gbic     ddm50.6'C       3.5 V       14.0 mA    -6.08 dBm-40.00 dBm
   Normal       Normal       Normal     Alarm(L)    Alarm(L)
 (warn)   100.0    -10.04.0       1.0     131.0       0.0       8.00     0.00       8.00     0.00
(alarm)   100.0    -10.04.0       1.0     131.0       0.0       8.00     0.00       8.00     0.00
..................................................................................... gi1/2     .
   Normal       Normal       Normal       Normal       Normal
     (warn)   128.0 -128.06.6       0.0     131.0       0.0       8.20 -40.00       8.00 -40.00
    (alarm)   128.0 -128.06.6       0.0     131.0       0.0       8.20 -40.00       8.00 -40.00
.....................................................................
```

Setting DDM monitoring threshold

You can set the threshold range for alarm/warning for each GBIC. Because the threshold is stored in GBIC, it is not reflected in the user configuration. It is maintained even when the GBIC port is deleted, and is reflected automatically when the GBIC port is installed again.

Table 117. DDM monitoring threshold

Command	Mode	Description
write gbic-ddm-threshold ***<IFNAME>***	Privileged	Show and set the alarm/warning threshold for the current temperature, voltage, current, Rx power and Tx power for GBIC (IFNAME) that supports DDM.

You should set warning / alarm threshold for each item, and press ‘y’ to save the setting.

```
-------------------------------------------------------------------------------------------
 ifname gbic     ddm    TemperatureVoltage Bias CurrentTx Power    Rx Power
 (warn)     high     lowhigh     lowhigh     lowhigh     lowhigh     low
(alarm)     high     lowhigh     lowhigh     lowhigh     lowhigh     low
-------------------------------------------------------------------------------------------
 (warn)     90.0     -5.03.5       3.1       70.0       4.0     -3.00    -9.50     -3.00 -21.02
(alarm)   100.0    -10.03.6       3.0       80.0       2.0     -2.00 -10.50     -2.00 -22.01
-------------------------------------------------------------------------------------------
Configure Temperature[y/n] ? y
      Warning High (128.0'C ~ -128.0'C ) [       90.0'C] ? 128
```

```
      Warning Low    (128.0'C ~ -128.0'C ) [       -5.0'C] ? -128
      Alarm      High (128.0'C ~ -128.0'C ) [     100.0'C] ? 128
      Alarm      Low    (128.0'C ~ -128.0'C ) [     -10.0'C] ? -128
Configure Voltage       [y/n] ? y
      Warning High (    6.55 V ~ 0.00 V    ) [       3.50 V] ? 6.55
      Warning Low    (    6.55 V ~ 0.00 V    ) [       3.10 V] ? 0
      Alarm      High (    6.55 V ~ 0.00 V    ) [       3.60 V] ? 6.55
      Alarm      Low    (    6.55 V ~ 0.00 V    ) [       3.00 V] ? 0
Configure Bias Current       [y/n] ? y
      Warning High ( 131.0 mA ~ 0.0 mA ) [     70.0 mA] ? 131
      Warning Low    ( 131.0 mA ~ 0.0 mA ) [       4.0 mA] ? 0
      Alarm      High ( 131.0 mA ~ 0.0 mA ) [     80.0 mA] ? 131
      Alarm      Low    ( 131.0 mA ~ 0.0 mA ) [       2.0 mA] ? 0
Configure Tx Power      [y/n] ? n
Configure Rx Power      [y/n] ? n
-----------------------------------------------------------------------------------------------
  ifname gbic      ddm    TemperatureVoltage Bias CurrentTx Power    Rx Power
  (warn)     high      lowhigh      lowhigh      lowhigh      lowhigh      low
(alarm)      high      lowhigh      lowhigh      lowhigh      lowhigh      low
-----------------------------------------------------------------------------------------------
  (warn)    128.0 -128.06.6       0.0      131.0       0.0      -3.00    -9.50      -3.00 -21.02
(alarm)    128.0 -128.06.6       0.0      131.0       0.0      -2.00 -10.50      -2.00 -22.01
-----------------------------------------------------------------------------------------------
Do you really want to SAVE [y/n] ? y
```

Chapter 18. Dynamic ARP Inspection

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

Note Refer to the command reference for detailed description on the CLI commands used in this chapter.

This chapter consists of the following sections:

- Understanding DAI
- Default DAI Configuration
- DAI Configuration Guidelines and Restrictions
- Configuring DAI
- DAI Configuration Samples

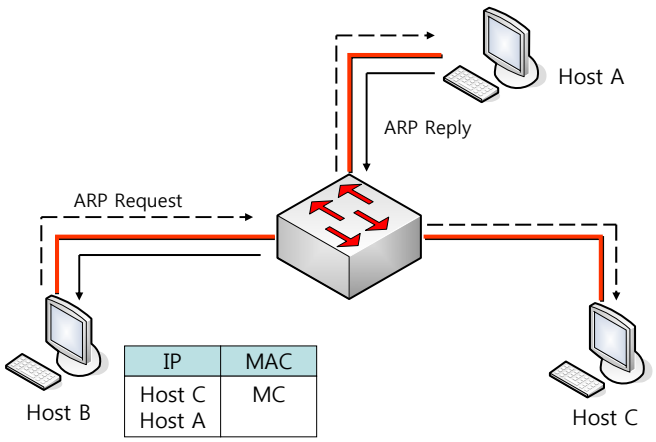
Understanding DAI

This section describes the basic function of DAI and the method to protect the ARP spoofing attack by using of DAI function. This section comprises following subsections.

- Understanding ARP
- Understanding ARP Spoofing Attacks
- Understanding DAI and ARP Spoofing Attacks
- Interface Trust States and Network Security
- Rate Limiting of ARP Packets
- Relative Priority of ARP ACLs and DHCP Snooping Entries
- Logging of Dropped Packets

Understanding ARP

ARP makes it possible to correlate IP address and MAC address by putting into a mapping table so that IP communication can be conducted within Layer 2 broadcast domain. For example, when host B wants to transmit data to host A, let's assume that there would be no registered information of host A within the ARP table in host B.

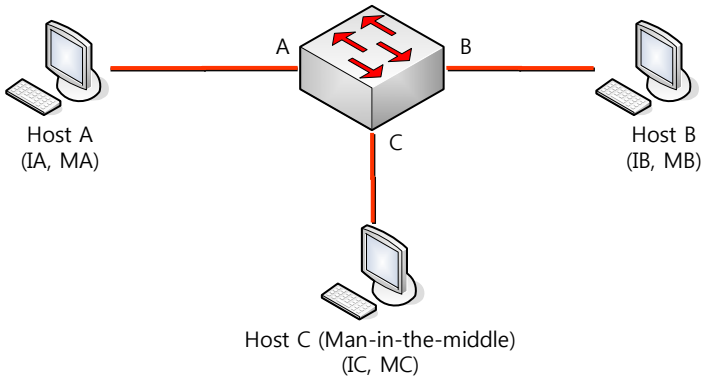


In order for host B to find out the MAC address for host A's IP address, host B sends out broadcast massage (ARP request) to all the hosts in the broadcast domain. Then all the hosts in the broadcast domain shall receive the ARP request which was sent by host B and host A will reply to host B with its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

Understanding ARP Spoofing Attacks

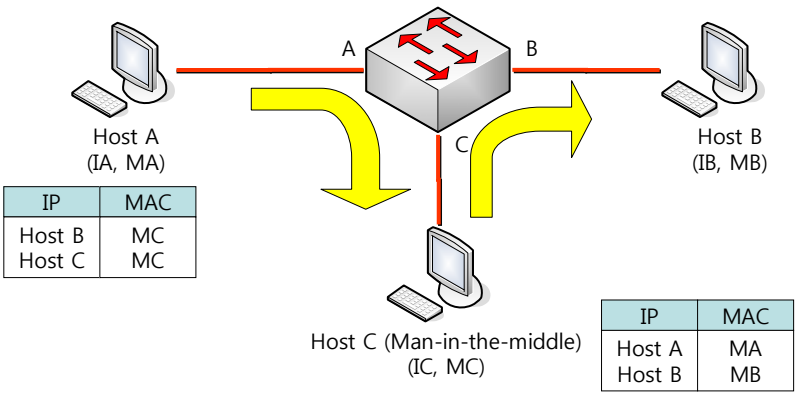
ARP unintentionally gets to have ARP table changed by the gratuitous reply which is sent by a host who has not received ARP request. Due to this defect, the ARP spoofing attack or ARP cache poisoning might happen. After this attack, the traffic of the victimized switch shall be transferred to other routers,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

ARP spoofing attack affects the ARP cache of the host, switch, or router which are connected in the Layer 2 network. And it intercepts the traffics which are intended for other network. The following figure shows the example of ARP cache poisoning.



Host A, B and C are interconnected through the interfaces A, B, and C of the switch centered in the picture, and they are all in same subnet. The IP address and MAC address are shown in parenthesis in the figure. For example, host A uses IP address, 'IA' and MAC address, 'MA'. When host A needs to communicate with host B in IP layer, in order to know the related MAC address of IP address 'IB' it sends out ARP request in broadcast manner. And if the switch and host B receive the ARP request, they update their ARP cache so as to replace the IP address IA and MAC address MA with latest values.

Host C may pollute the ARP cache of host A and host B by which it sends out broadcasted ARP response that includes the faked MAC address, 'MC' at here for IP address IA (or IB). The host that has a polluted ARP cache shall use the MAC address of MC as the destination for the traffic which is intended to be heading for IA or IB. This means that host C intercepts the traffic. Host C knows the genuine MAC address of IA and IB, it can forward the intercepted traffic by inserting the right MAC address to the originally targeted host. Thus host C is placed in between host A and host B, and we call this symptom as '*man-in-the middle* attack'.



Understanding DAI and ARP Spoofing Attacks

DAI is a security function that is used to check out ARP packet. DAI inspects invalid IP-to-MAC address binding and drop the ARP packet after logging the relevant information. This feature protects network from the main-in-the-middle attack.

DAI makes sure the ARP table be changed only by valid ARP request and response. The switch that is enabled for DAI function behaves as the following:

- Check out and inspect all ARP packets that come through the untrusted ports.
- Check out the received packets whether it has the valid IP-to-MAC address binding before updating its own ARP cache.
- Drop the invalid ARP packets.

When DAI checks out the validity of the ARP packet, it must utilize 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

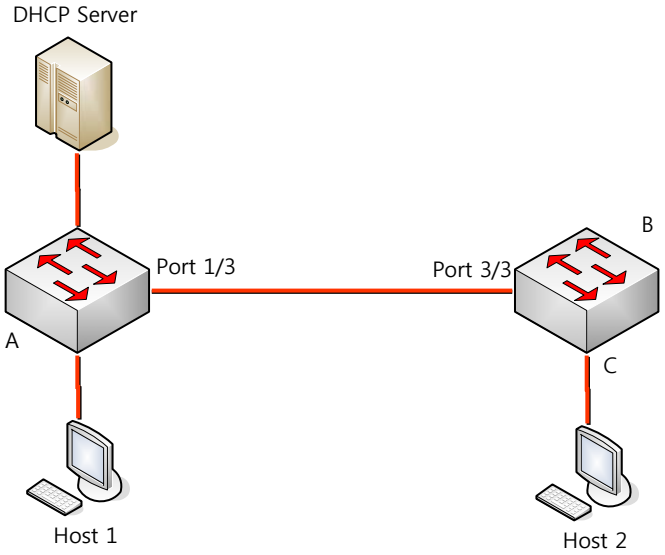
DAI basically maintains the information of trust status of each interface in the switch. With respect to the packets that come through the trusted interface, DAI will not take any forms of DAI inspection. On the contrary, for the packets from untrusted interface, DAI inspection will duly take place.

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 P8800 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 loggin**g' you can specify the type of packets to log.

Default DAI Configuration

The following table shows the default DAI configuration.

Feature	Default Setting
DAI	'Inactive' for all VLAN.
Interface trust state	'Untrusted' for all interfaces.
Rate limit of incoming ARP packets	15 pps for untrusted interfaces. In case of Trusted interfaces, there is no limitation on rate. Burst interval is 1second. The rate limit for interfaces is in 'Disabled' status.
ARP ACLs for non-DHCP environments	ARP ACLs is not defined.
Validation checks	No inspection is to be conducted.
Log buffer	When DAI is enabled, all ARP packet which is denied or dropped will be logged. The number of log entry is 32. The number of system message generated is 5 per second. The period of logging-rate 1 second .
Per-VLAN logging	All ARP packet which is denied or dropped will be logged.

DAI Configuration Guidelines and Restrictions

When DAI is configured, you have to keep the followings in mind:

- DAI basically takes care of the ARP table only in the switch. As a better method to protect whole network, the trap function which will have ARP packet to be processed in CPU.
- DAI is intended to be used as an ingress security tool. You ought not to use it at an egress port.
- DAI is not effective for the hosts that are connected to the DAI-disenabled switch. As the man-in-the-middle attack is confined to a single Layer 2 broadcast domain, you ought to seperate a domain which adopts DAI from other domains which don't use DAI. This will make sure that the ARP table of the switch that are in DAI activated domain.
- DAI uses the DHCP snooping binding database in order to check the IP-to-MAC address binding of the coming ARP request and ARP response packets. To allow the ARP packets which will have dynamically assigned IP address, you ought to activate DHCP snooping.

Note In case DAI is in use together with DHCP server, it can use the binding information of the DHCP server.

- If DHCP snooping is inactive or DHCP is not in use, then you can utilize ARP ACL to permit or deny packets.
- Configure to set the rate of ARP packets considering the characteristics of the port.

Configuring DAI

In this section, the way to configure DAI is explained:

- Enabling DAI on VLANs (Mandatory)
- Configuring the DAI Interface Trust State (Optional)
- Applying ARP ACLs for DAI Filtering (Optional)
- Configuring ARP Packet Rate Limiting (Optional)
- Enabling DAI Error-Disabled Recovery (Optional)
- Enabling Additional Validation (Optional)
- Configuring DAI Logging (Optional)
- Displaying DAI Information

Enabling DAI on VLANs

When DAI is enabled for a VLAN, the switch will inspect the ARP packet that come through the VLAN as following:

- Broadcasted ARP
- ARP request packets that ask for switch's MAC address.
- Reply packets that answer to the requesting ARP request.
- All unicast ARP packets that are transferred among terminals.

After checking out these packets, it only replies to the valid packets and updates the ARP table.
To make DAI work on a VLAN, execute the following commands:

Command	Description
Switch# **configure terminal**	To get in global configuration mode.
Switch(config)# **ip arp inspection vlan** *vlan-id* Switch(config)# **no ip arp inspection vlan** *vlan-id*	To enable DAI on a VLAN. To disable DAI from a VLAN.
Switch# **show ip arp inspection**	To check out current setting.

Note When you enable DAI on a VLAN, all the ARP packets that flow through the VLAN will be inspected. In other words, the ARP cache of the switch and network are to be protected.

The following example shows how to enable DAI on VLAN 200:

Switch# **configure terminal**
Switch(config)# **ip arp inspection vlan 200**

The following example shows how to retrieve current settings:

Switch# **show ip arp inspection**
DHCP Snoop Bootstrap : Disabled
Source MAC Validation : Disabled
Destination MAC Validation : Disabled
IP Address Validation : Disabled
ARP Field Validation : Disabled

Vlan Config Operation ACL Match Static ACL ACL Log DHCP Log
---- -------- --------- -------------------- ---------- --------- --------
200 Enabled Active+ NoDeny 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:

Command	Description
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-gi1)# **ip arp inspection trust** Switch(config-if-gi1)# **no ip arp inspection trust**	To configure the interface to be trusted. (default: untrusted) To configure the interface to be untrusted.
Switch(config-if-gi1)# **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 gi1**
Switch(config-if-gi1)# **ip arp inspection trust**
Switch(config-if-gi1)# **end**
Switch# **show ip arp inspection interfaces**
Interface Trust State Rate (pps) Burst Interval Auto Recovery
--------------- ----------- ---------- -------------- -------------
gi Trusted None1 Disabled
gi2 Untrusted 151 Disabled

Applying ARP ACLs for DAI Filtering

To utilize ARP ACL feature, the following steps are to be executed:

Command	Description
Switch# **configure terminal**	To get in global configuration mode.
Switch(config)# **ip arp inspection filter** *arp_acl_name* **vlan** *vlan-id* [**static**]	To apply ARP ACL to a VLAN.
Switch(config)# **end**	To get back to Enable mode.
Switch# **show ip arp inspection**	To retrieve current settings.

The following example shows how to apply the ARP ACL whose name is example_arp_acl to VLAN 200:

Switch# **configure terminal**
Switch(config)# **ip arp inspection filter example_arp_acl vlan 200**
Switch(config)# **end**
Switch# **show ip arp inspection**
DHCP Snoop Bootstrap : Disabled
Source MAC Validation : Disabled
Destination MAC Validation : Disabled
IP Address Validation : Disabled
ARP Field Validation : Disabled

Vlan	Config	Operation	ACL Match	Static ACL	ACL Log	DHCP Log
200	Enabled	Activeexample_arp_acl		NoDeny	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:

Command	Description
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-gi1)# **ip arp inspection limit** {**rate** *pps* [**burst interval** *seconds*] **| none**} Switch(config-if-gi1)# **no ip arp inspection limit**	(Optional) To set the rate limit upon ARP packet. To get back to default configuration.
Switch(config-if-gi1)# **ip arp inspection limit enable** Switch(config-if-gi1)# **no ip arp inspection limit enable**	To enable the ARP rate limit of an interface. To disable the ARP rate limit of an interface .
Switch(config)# **end**	To get back to Enable mode.
Switch# **show ip arp inspection interfaces**	To retrieve current settings.

When you configure the ARP packet rate limit, you have to keep the followings in mind:

- Default value for untrusted interface is 15 pps (packet per second), and for trusted interface is no limitation at all.
- **rate** is the upper limit value in terms of *pps* which may have between 0 to 2048.
- **rate none** means there is no limitation on the rate of received ARP packets.
- (Optional) **burst interval** *seconds* (default is 1) is the time duration for which the system will watch to see if ARP packet rate is over the upper limit. Thus, if the value of **rate** is reached during the time lapse of **burst interval**, then the incoming ARP packets will be restricted. The range is 1 ~ 15.
- If the incoming ARP packet rate is over the predefined value, the switch will discard all the received ARP packets at the port. This setting will be maintained until the operator would change the setting.
- While the rate-limit of an interface is not changed, if the trust status of an interface is changed, then the default value of the rate-limit of an interface will be changed. Once rate-limit value is changed, then even though the trust status would be changed, the configured value will be maintained. By use of the command '**no ip arp inspection limit'** the rate-limit of an interface will be returned to default value.
- After configuring by use of the command '**ip arp inspection limit enable'** the rate limit for ARP packet will be activated.

The following example shows how to configure ARP packet rate limit upon gi1 port.

Switch**# configure terminal**
Switch(config)**# interface gi1**
Switch(config-if-gi1)**# ip arp inspection limit rate 20 burst interval 2**
Switch(config-if-gi1)**# ip arp inspection limit enable**
Switch(config-if-gi1)**# end**
Switch**# show ip arp inspection interfaces**

Interface	Trust State	Rate (pps)	Burst Interval	Auto Recovery
Gi1	Untrusted	202	Disabled	
Gi2	Untrusted	151	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:

Command	Description
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-gi1)**# 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 gi1 to normal automatically after 10 seconds:

Switch# **configure terminal**
Switch(config)# **interface gi1**
Switch(config-if-gi1)# **ip arp inspection limit auto-recovery 10**
Switch(config-if-gi1)# **ip arp inspection limit enable**
Switch(config-if-gi1)# **end**
Switch# **show ip arp inspection interfaces**

Interface	Trust State	Rate (pps)	Burst Interval	Auto Recovery
gi1	Untrusted	202	10	
gi2	Untrusted	151	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:

Command	Description
Switch# **configure terminal**	To get in global configuration mode.
Switch(config)# **ip arp inspection validate** {**dst-mac** | **ip** | **src-mac**} Switch(config)# **no ip arp inspection validate** {**dst-mac** | **ip** | **src-mac**}	(Optional) To enable additive validity check. (default: none) To disable additive validity check.
Switch(config)# **end**	To get back to Enable mode.
Switch# **show ip arp inspection**	To retrieve current settings.

To enable additive validity check, you have to keep the followings in mind:

- At least one keyword among the options ought to be used.
- Each '**ip arp inspection validate'** command nullify the former command. If, **ip arp inspection validate** command has enabled **src-mac** and **dst-mac** inspection first, and then the second command '**ip arp inspection validate'** enables only **ip** inspection, then the **src-mac** and **dst-mac** inspection will be disabled and only the **ip** inspection will be in its effect.
- Additive validity inspections according to command arguments are as below:
  - **dst-mac** – With respect to the ARP response packet, it makes comparison between the destination MAC address in Ethernet header and the target MAC address in ARP body.
  - **ip –** It checks out the invalid IP address in ARP body. Thus addresses like 0.0.0.0 or 255.255.255.255 or multicast IP address will be discarded. It also verifies the sender IP address of ARP request and the sender/target IP address of ARP response.

- **src-mac** – With respect to all ARP packets, it makes comparison between the source MAC address in Ethernet header and the sender MAC address in ARP body.

The following example shows how to enable the additive validity inspection as to the command argument 'src-mac':

Switch# **configure terminal**
Switch(config)# **ip arp inspection validate src-mac**
Switch(config)# **end**
Switch# **show ip arp inspection**
DHCP Snoop Bootstrap : Disabled
Source MAC Validation : Enabled
Destination MAC Validation : Disabled
IP Address Validation : Disabled
ARP Field Validation : Disabled

Vlan	Config	Operation	ACL Match	Static ACL	ACL Log	DHCP Log
200	Enabled	Active	NoDeny	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	NoDeny	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	NoDeny	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	NoDeny	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:

Command	Description
Switch# **configure terminal**	To get in global configuration mode.
Switch(config)# **ip arp inspection log-buffer entries** *number* Switch(config)# **no ip arp inspection log-buffer entries**	To set the size of DAI log buffer (range: 0 ~ 1024). To return to default value (The default size: 32)
Switch(config)# **end**	To get back to Enable mode.
Switch# **show ip arp inspection log**	To retrieve current settings.

The following example shows how to adjust the size of DAI log buffer to be 64:

Switch# **configure terminal**
Switch(config)# **ip arp inspection log-buffer entries 64**
Switch(config)# **end**
Switch# **show ip arp inspection log**
Total Log Buffer Size: 32
Syslog rate : 5 entries per 1 seconds.
No entries in log buffer.

Configuring the DAI Logging System Messages

To configure the log message that DAI generates, you need to execute the following steps:

Command	Description
Switch# **configure terminal**	To get in global configuration mode.
Switch(config)# **ip arp inspection log-buffer logs** *number_of_messges* **interval** *length_in_seconds* Switch(config)# **no ip arp inspection log-buffer logs**	To configure the DAI log buffer. 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_messges'*, the range of value is 0 ~ 1024, and default is 5. If you set it to be 0, then log message will not be generated.
- As to '**interval** *length_in_seconds'*, the range of value is 0 ~ 86400 (one day), and default is 1. If you set it to be 0, then log message will be generated immediately (Thus, the log buffer is empty constantly).
- The system log message shall be generated in the ratio of '*number_of_messages'* times *per 'length_in_seconds'* duration.

The following example shows how to configure to generate 12 DAI log messages per every 2 seconds:

Switch# **configure terminal**

Switch(config)# **ip arp inspection log-buffer logs 12 interval 2**
Switch(config)# **end**
Switch# **show ip arp inspection log**
Total Log Buffer Size: 32
Syslog rate : 12 entries per 2 seconds.
No entries in log buffer.

Configuring the DAI Log Filtering

After inspecting the ARP packets, you can selectively collect the result of the inspection so as to generate the system message.

To configure the log filtering function for DAI, execute the following steps:

Command	Description
Switch# **configure terminal**	To get in global configuration mode.
Switch(config)# **ip arp inspection vlan** *vlan-id* {**acl-match** {**matchlog** | **none**} | **dhcp-bindings** {**all** | **none** | **permit**}}	To apply the log filtering to a VLAN.
Switch(config)# **end**	To get back to Enable mode.
Switch# **show running-config**	To retrieve current settings.

When you configure the logging system message of DAI you have to be aware of the followings:

- All the denied packets will be logged as Default.
- **acl-match matchlog** — it makes logging work based upon ACL setting. If '**matchlog'** is specified and '**log'** keyword is used in the **permit** or **deny** command of ARP access-list configuration, the ARP packets that are permitted or denied by ACL will be logged.
- **acl-match none** — it will NOT log for the packets that are consistent with ACL.
- **dhcp-bindings all** — it will do log for the packets that are consistent with DHCP binding.
- **dhcp-bindings none** — it will NOT log for the packets that are consistent with DHCP binding.
- **dhcp-bindings permit** — it will do log for the packets that are allowed by DHCP binding.

The following example shows how to configure not to generate log message for the packets that are consistent with ACL:

Switch# **configure terminal**
Switch(config)# **ip arp inspection vlan 200 logging acl-match none**
Switch(config)# **end**
Switch# **show ip arp inspection**
DHCP Snoop Bootstrap : Disabled
Source MAC Validation : Disabled
Destination MAC Validation : Disabled
IP Address Validation : Disabled
ARP Field Validation : Disabled

Vlan Config Operation ACL Match Static ACL ACL Log DHCP Log
---- -------- --------- -------------------- ---------- --------- --------

200 Enabled Active NoNone Deny

Displaying DAI Information

To retrieve the information about DAI, use the following commands:

Command	Description
show arp access-list	To display the information about ARP ACL.
show ip arp inspection interfaces	To display the trust status of the interface.
show ip arp inspection vlan [*vlan-id*]	To display the DAI configuration and its behavior of a VLAN.
show ip arp inspection arp-rate	To display the rate information of ARP packet reception in the interface.

To display or initialize the DAI statistics, use the following commands:

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

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

Command	Description
clear ip arp inspection log	To initialize DAI log buffer.
show ip arp inspection log	To display the configuration and content of DAI log buffer.

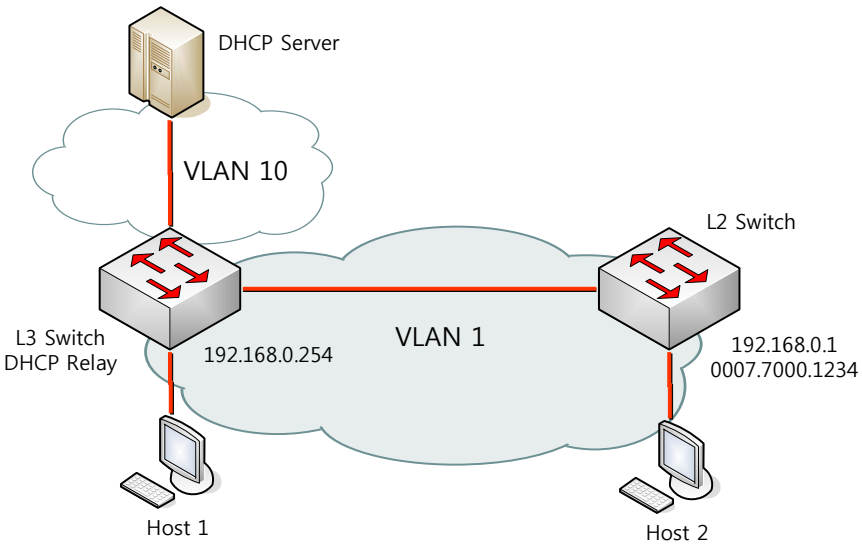
DAI Configuration Samples

This section includes the following examples:

- Sample One: Interoperate with DHCP Relay
- Sample Two: Interoperate with DHCP Server

Sample: Interoperate with DHCP Relay

This example explains how you can configure DAI upon a switch that uses DHCP snoop function. Consider the network in the figure below.



L3 switch relays DHCP message to DHCP server via VLAN 10 and connects with host or L2 switch. The L2 switch connected to L3 switch uses static ip address. The host 1 and host 2 is assigned via DHCP. All switchs and hosts also place with VLAN 1.

Note The DAI in this configuration depends on DHCP snooping binding information about IP-to-MAC binding information. Refer to DHCP snooping chapter about DHCP snooping configuration.

To use DAI on a switch that is enabled for DHCP relay function, do the following steps.

Table 118. DAI Configuration

Step	Descripiton
Step 1	Enables DHCP relay function. Switch**# configure terminal** Switch(config)**# ip dhcp helper-address 10.1.1.1** Switch(config)**# service dhcp relay**
Step 2	To configure IP-to-MAC binding information of host assigned IP from DHCP, enable DHCP snooping within VLAN 10 to build up the IP-to-MAC binding information of a host. Switch**# configure terminal** Switch(config)**# ip dhcp snooping vlan 1** Switch(config)**# ip dhcp snooping vlan 10** Switch(config)**# ip dhcp snooping**

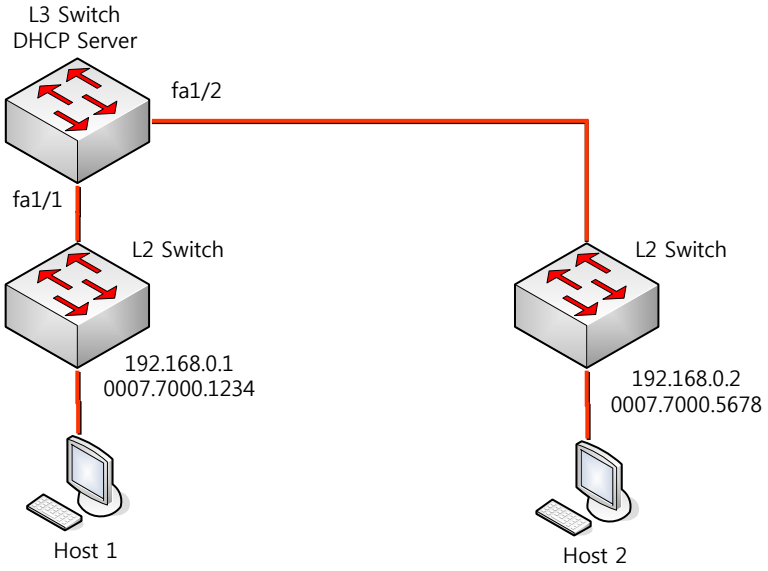
Step 3	To permit ARP packet of switch using static ip, set ARP ACL. Switch# **configure terminal** Switch(config)# **arp access-list permit-switch** Switch(config-arp-nacl)# **permit ip host 192.168.0.1 mac host 0007.7000.1234** Switch(config-arp-nacl)# **exit** Switch(config)# **ip arp inspection filter permit-switch vlan 1** Switch(config)# **end** To see if the configuration has been set correctly. Switch# **show ip arp inspection vlan 1**
Step 4	Enables DAI to VLAN1 connected with host. Switch# **configure terminal** Switch(config)# **ip arp inspection vlan 1** Switch(config)# **end** To see if the configuration has been set correctly. Switch# **show ip arp inspection vlan 1**

The setting of L3 switch is as follows:

```
!
arp access-list permit-switch
   permit ip host 192.168.0.1 mac host 0007.7000.1234
!
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
!
```

Sample Two: Interoperate with DHCP Server

This sample explains how to configure DAI in the switch used as a DHCP server. In this sample, the network is configured as below diagram:



L3 switch relays DHCP messages to the DHCP server, and host or L2 switch is connected to the L3 switch. L2 switche connected to the L3 switch does not provide any DHCP related functions, and uses a static IP address. Host 1 and Host 2 gets the IP addresses assigned through DHCP. All the switches and hosts belong to VLAN 1.

Note In those configurations, DAI completely relies on DHCP snooping binding info for IP-to-MAC binding. For DHCP snooping settings, see the *DHCP snooping* section of the manual.

To use DAI function in the switch working as a DHCP server, please configure the switch as follows:

Step 1 **Enable DAI to VLAN 1.**

Switch# **configure terminal**
Switch(config)# **ip arp inspection vlan 1**
Switch(config)# **end**

Check if the configuration is conrrect.
Switch# **show ip arp inspection vlan 1**

Step 2 **In case 15 or more ARP packets incomes from the interface connected to the switch, configure the switch to block the ARP receiving and to try auto-recovery for the blocked interface after 10 seconds.**

Switch# **configure terminal**
Switch(config)# **interface gi1**
Switch(config-if-gi1)# **ip arp inspection limit rate 15 burst interval 3**
Switch(config-if-gi1)# **ip arp inspection limit auto-recovery 10**
Switch(config-if-gi1)# **ip arp inspection limit enable**

Switch(config-if-gi1)# **interface gi2**
Switch(config-if-gi2)# **ip arp inspection limit rate 15 burst interval 3**
Switch(config-if-gi2)# **ip arp inspection limit auto-recovery 10**
Switch(config-if-gi2)# **ip arp inspection limit enable**
Switch(config-if-gi2)# **end**

Check if the configuration is conrrect.
Switch# **show ip arp inspection interfaces**

Step 3 **Enable DHCP server to assign IP address to the hosts.**

Switch# **configure terminal**
Switch(config)# **service dhcp server**

> **Note** The DHCP network pool configuration will be skipped. Please refer to *DHCP* section of the manual.

Step 4 **Delays the time at which DAI uses DHCP snooping binding database.**

The previous IP-to-MAC binding info may not exist due to the reload of switch or disable->enable of DHCP server. So if the DAI function is not delayed, the hosts that obtained IP address through DHCP successfully can be also limited in using Internet.

Switch# **configure terminal**
Switch(config)# **ip dhcp snooping arp-inspection start 1800**
Switch(config)# **end**

Check if DAI delays DHCP inspection.
Switch# **show ip arp inspection**

> **Note** Even in this case, the ARP packet inspection by ARP ACL will continue.

Step 5 **Configure to allow ARP packets of the switches with static IP address.**

Switch# **configure terminal**
Switch(config)# **arp access-list permit-switch**
Switch(config-arp-nacl)# **permit ip host 192.168.0.1 192.168.0.10 mac host 0007.7000.1234 0000.00ff.ffff**
Switch(config-arp-nacl)# **exit**
Switch(config)# **ip arp inspection filter permit-switch vlan 1**
Switch(config)# **end**

	Note	ARP ACL provides range command for IP address and wildcard command for MAC address to allow to inspect many packets with single condition.

Check if the configuration is conrrect.
Switch# **show ip arp inspection vlan 1**

The configuration of L3 switch is as follows.

```
interface gi1
  ip arp inspection limit rate 15 burst interval 2
  ip arp inspection limit auto-recovery 10
  ip arp inspection limit enable
!
interface gi2
  ip arp inspection limit rate 15 burst interval 2
  ip arp inspection limit auto-recovery 10
ip arp inspection limit enable
!
arp access-list permit-switch
   permit ip host 192.168.0.1 192.168.0.10 mac host 0007.7000.1234 0000.00ff.ffff
!
ip arp inspection vlan 1
ip arp inspection filter permit-switch vlan 1
!
service dhcp server
!
ip dhcp snooping arp-inspection start 1800
!
```

Chapter 19. ARP Snoop

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:

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.

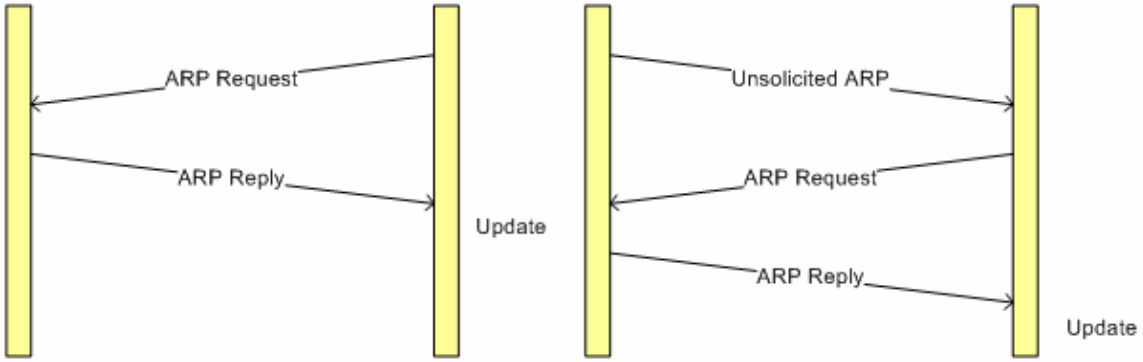


Figure 26. ARP snoop (3-way handshake)

Because the ARP packet does not have any security function 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.

ARP Snoop Entry Status

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

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.

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:

Command	Description
Switch# **configure terminal**	To enter into the global configuration mode.
Switch(config)# **arp snoop ip** *ip-address* [*ip-address*]	To set the IP address range.
Switch(config)# **arp snoop** Switch(config)# **no arp snoop**	To enabled 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:

Command	Description
Switch# **configure terminal**	To enter into the global setup mode.

Switch(config)# **arp snoop ip** *ip-address* [*ip-address*] [**aging-time** *aging-time*]	To set the range of IP address and change the ageing-time.
Switch(config)# **arp snoop** Switch(config)# **no arp snoop**	To enable 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.

Command	Description
Switch# **configure terminal**	To enter into global configuration mode.
Switch(config)# **arp snoop ip** *ip-address* [*ip-address*]	To set the range of IP address.
Switch(config)# **arp snoop** Switch(config)# **no arp snoop**	To enable 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.

Command	Description
Switch# **configure terminal**	To enter into the global setup mode.
Switch(config)# **arp snoop ip** *ip-address* [*ip-address*]	To set IP address range.
Switch(config)# **arp snoop** Switch(config)# **no arp snoop**	To enable 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:

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.

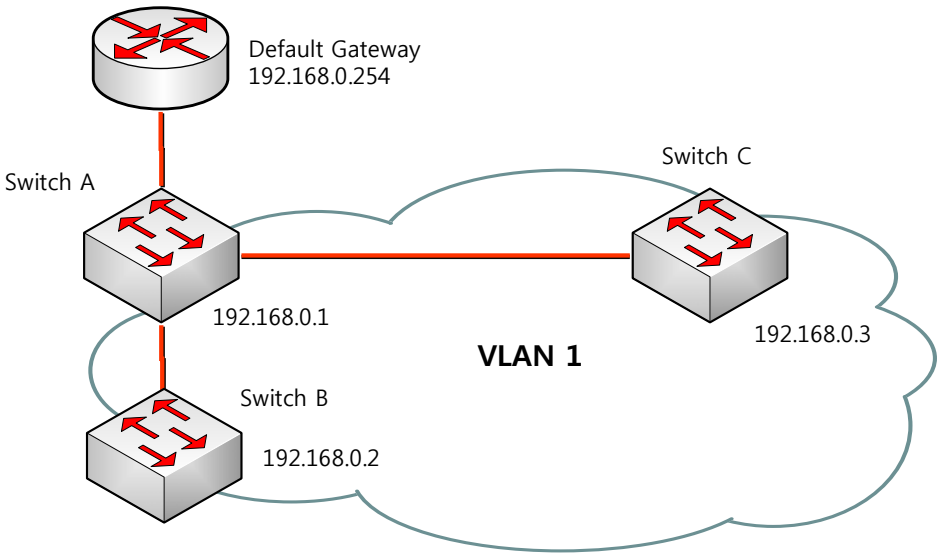
ARP Snoop Configuration Samples

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:

Step 1 **Activate the ARP snoop to create IP-to-MAC binding information for specific IP address range,.**

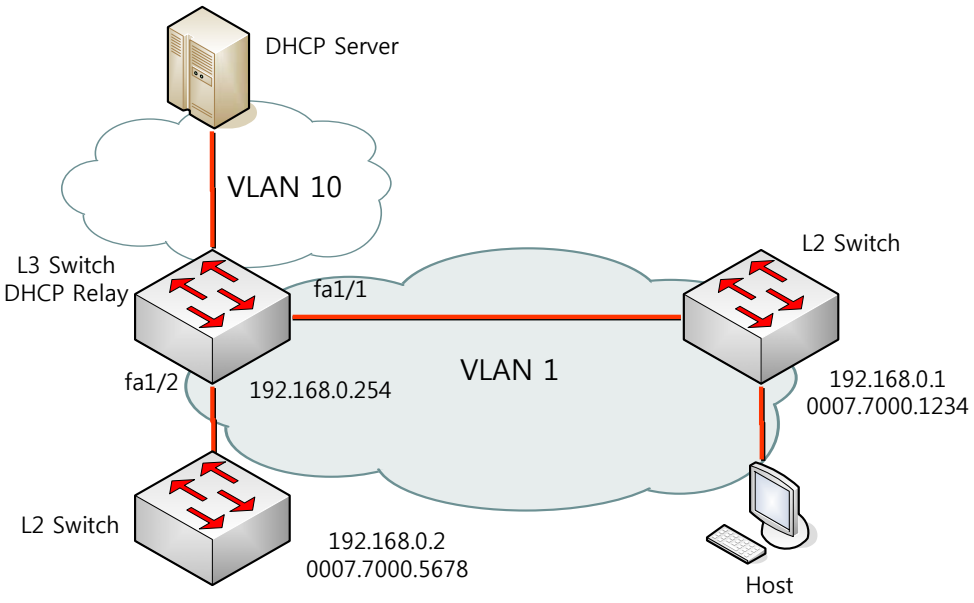
Switch**# configure terminal**
Switch(config)**# arp snoop ip 192.168.0.1 192.168.0.10**
Switch(config)**# arp snoop ip 192.168.0.254**
Switch(config)**# arp snoop**

Check if the settings are correct.
Switch**# show arp snoop**

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:

Step 1 **Activate the DHCP relay function.**

Switch# **configure terminal**
Switch(config)# **ip dhcp helper-address 10.1.1.1**
Switch(config)# **service dhcp relay**

Step 2 **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.**

Switch# **configure terminal**
Switch(config)# **ip dhcp snooping vlan 1**
Switch(config)# **ip dhcp snooping vlan 10**
Switch(config)# **ip dhcp snooping**

Step 3 **Activate ARP snoop to create IP-to-MAC binding information for IP address ranges that use Static IP.**

Switch# **configure terminal**
Switch(config)# **arp snoop ip 192.168.0.1 192.168.0.10**
Switch(config)# **arp snoop**

Step 4 **Set ARP ACL to allow ARP packets of switches that use static IP.**

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**

Check if the settings are correct.
Switch# **show ip arp inspection vlan 1**

Step 5 **Activate DAI in the VLAN 1 to which the host is connected.**

Switch# **configure terminal**
Switch(config)# **ip arp inspection vlan 1**
Switch(config)# **end**

Check if the settings are correct.
Switch# **show ip arp inspection vlan 1**

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
```