

U9016B GPON

■ User Guide



ubiQuoss

U9016B GPON

■ User Guide

[Copyrights]

Copyright© UbiQuoss Inc. All rights Reserved.

Copyrights of this guide is owned by UbiQuoss Inc.

Without prior written approval of UbiQuoss, any contents included in this document shall not be reproduced, copied, or partially extracted in any kind of format, including electrical, mechanical, and acoustical media, and in any other reason.

The information regarding the product in this guide is subject to change without notice for specific reasons.

The figures and information regarding the product in this guide may include some errata and printing errors. Those will be removed and corrected in the next revision version.



Preface

This preface provides an overview of the U9016B user guide, setting out guide conventions, and listing other publications that may be useful.

Introduction

This guide provides the information required for configuring and operating the network environment after the installation of the U9016B 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 information on how to solve problems that may occur during the network operation. Therefore, this guide assumes that readers have a 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 U9016B hardware, refer to the hardware installation guide of each system.

Conventions

The following Conventions Table and list conventions and icons used throughout this guide.

Text 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] Input	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]
<i>Italics</i>	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

Notice and Warning Icons

Icon	Type	Description
	Notice	Important features, characteristics, commands or tips
	Warning	There is a danger of bodily injury, data loss, or system damage

Related Documents

For additional information on this equipment, refer to the following manuals:

Manual	Contents
<i>Hardware Installation Guide</i>	Switch hardware installation Initial operating environment configuration Trouble Shooting



Notice

This document is the manual for the U9016B.



Organization

The chapters of this manual are organized as follows:

Chapter 1.Overview

This chapter provides the following information required for system users to set up configuration and start up U9016B.

Chapter 2.Interface

This chapter describes the system interface.

Chapter 3.VLAN

This chapter describes the VLAN of system.

Chapter 4.IP Configuration

This chapter explains how to set an IP address.

Chapter 5.Utilities

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

Chapter 6.OS Image and Configuration Files

This chapter describes Flash File System management and using USB or Compact Flash (CF) memory. OS Image and Configuration File are saved in the File System provided by U9016B.

Chapter 7.NTP

This chapter describes the NTP configuration of the system.

Chapter 8.DHCP

This chapter describes the DHCP configuration of the system.

Chapter 9.IGMP Snooping

This chapter introduces IGMP Snooping Configuration.

Chapter 10.Multicast Routing

This chapter describes IP multicast routing elements and IP multicast routing setting.

Chapter 11.Statistics Monitoring

This chapter describes the monitoring function for the system and statistics of U9016B OLT systems:

Chapter 12.STP, RSTP, MSTP, and SLD

This chapter introduces how to configure the Spanning Tree Protocol (STP) and Rapid Spanning Tree Protocol (RSTP) on the switch. It also explains frame transmission from the bridge.

Chapter 13.BFD

This chapter describes BFD (Bidirectional Forwarding Detection). BFD is a protocol for

rapid detecting the error of forwarding path. BFD independently runs regardless of network type and routing protocol.

Chapter 14.LACP

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

Chapter 15.IP-OPTION

This chapter describes the IP-option of system.

Chapter 16.Dynamic ARP Inspection

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

Chapter 17.QoS and ACL

This chapter describes the QoS configuration and the ACL of system.

Chapter 18.GPON Configuration

This chapter describes how to make the setting in relation with GPON in the U9016B. This chapter consists of the following sections:

Chapter 19.IPv6 Configuration

This chapter describes how to configure the IPv6 address.

Chapter 20.MLD_Snooping

This chapter describes how to configure MLD snooping.

Chapter 21.RIP

This chapter introduces how to set up RIP (Routing Information Protocol). RIP has been used for many years and is still used for IGP (Interior Gateway Protocol) of small network.

Chapter 22.OSPF

This chapter introduces OSPF routing protocol used in U9016B. OSPF routing protocol is described in RFC 2328.

Chapter 23.BGP

This chapter introduces BGP among available IP Unicast routing protocols of U9016B.

Chapter 24.VRRP

This chapter describes the VRRP configuration of system.



Table of Contents

Preface.....	I
Introduction	I
Conventions	I
Notice and Warning Icons	II
Related Documents	II
Organization.....	III
Table of Contents	V
List of Tables	XVI
List of Figures.....	XXIII

Chapter 1. Overview..... 1

Command Line Editor and Help	2
Command Syntax	2
Command Syntax Helper	2
Abbreviated Syntax.....	4
Command Symbols.....	4
Command Line Editing Key and Help Function.....	5
Switch Command Mode	7
U9016B Startup	8
User Interface.....	9
Connection through Console Port	9
Connection through Telnet	10
Connection through SNMP Network Manager	10
User Management.....	11
Add/Delete User.....	11
Password Setting	12
AAA (Authentication Authorization Accounting).....	14
Authentication	14
User Authentication.....	14
Setting User Authentication.....	15
Authorization	15
Accounting	17
Session Access Management	17
Privilege level Configuration	18
Server Configuration	19
RADIUS Server Configuration.....	19
TACACS+ Server Configuration.....	20
Setting Hostname.....	21
SNMP (Simple Network Management Protocol)	22
SNMP Configuration	22
SNMP Community	22
SNMP Trap host.....	23
SNMP Trap	25
SNMPv3 Configuration	25
SNMP engineID	26
User of SNMPv3	26
ACL (Access Control List)	28
Rules for ACL Creation	28
Configuration of Standard IP Access List	28

Configuration of Access List for Telnet Connection.....	29
Banner Configuration.....	30
AFSMGR (Alarm Fault Status Manager).....	32
Setting AFS Alarm	32
Clear AFS Alarm Event.....	33
Clearing AFS history	33
Setting AFS Masking Function.....	34
Setting AFS Severity Class.....	34
Setting AFS SNMP Trap	35
Changing AFS Configuration with default-config	36

Chapter 2.Interface 37

Overview.....	38
Common Commands.....	39
Interface name.....	39
Interface ID	39
Interface mode prompt	39
Description Command	40
Show Interface Information	41
Show Interface Command	41
Show Interface Status Command	41
Show idprom Command	43
Physical Port Configuration.....	44
Shutdown.....	44
Speed and Duplex	44
Flow control	44
Carrier delay	45
Broadcast Suppression.....	46
Port Mirroring.....	47
Layer 2 Interface Configuration.....	48
VLAN Trunking	48
Layer 2 Interface mode.....	48
Layer 2 Interface Defaults.....	48
Enabling/disabling Layer 2 Interface.....	48
Trunk Port Setting.....	49
Access Port Setting	49
Port group	51
Overview of Port Group	51
Port group configuration	51

Chapter 3.VLAN 53

VLAN Introduction.....	54
Advantages of VLAN.....	55
Efficient Traffic Control.....	55
Enhanced Network Security	55
Flexible Network and Device management	55
VLAN Types.....	56
Port-based VLANs.....	56
Tagged VLANs.....	58
Uses of Tagged VLANs.....	58
Assigning a VLAN Tag.....	58

Hybrid VLAN (Mixing Port-based VLAN and Tagged VLAN)	60
VLAN Configuration	61
VLAN ID	61
Default VLAN	61
Native VLAN	61
VLAN Setting.....	63
Commands for VLAN Configuration	63
Examples of VLAN Configuration.....	64
Displaying VLAN Settings	68
802.1 Q-in-Q	70
Private Edge VLAN	72
Abnormal MAC Drop	74
Chapter 4.IP Configuration	75
Assigning an IP address.....	76
ARP (Address Resolution Protocol)	78
Configuring Static Routes.....	79
IP Configuration Example.....	80
Chapter 5.Utilities	82
Status dump command	83
Commands.....	83
Command History Function.....	85
Output Post Processing	86
Overview of output post processing	86
DDM (Digital Diagnostic Monitoring)	87
SFP DDM Monitoring	87
Chapter 6.OS Image and Configuration Files	88
File System	89
Image/Configuration/BSP Down/Upload	91
Download/Upload with the FTP.....	91
Down/UpLoading File with the TFTP	92
Download/Upload through SFTP	93
Configuration File Management	94
Running configuration	94
Startup configuration	94
Saving Configuration File.....	94
Configuration File Erase	95
Boot Mode Setting and System Restart	96
Boot Mode Setting	96
System Reload.....	96
Chapter 7.NTP.....	98
Understanding Time Sources	99
Network Time Protocol.....	99
Hardware Clock	99
Configuring NTP.....	100
Configuring Poll-Based NTP Associations	100
Configuring Time and Date Manually	103
Configuring the Time Zone.....	103

Configuring Summer Time (Daylight Savings Time)	103
Manually Setting the Software Clock	104
Using the Hardware Clock	105
Setting the Hardware Clock	105
Setting the Software Clock from the Hardware Clock	105
Setting the Hardware Clock from the Software Clock	105
Monitoring Time and Calendar Services	106
Configuration Examples	106

Chapter 8.DHCP 107

DHCP Server Features and Configuration	108
Overview of DHCP Server Functions	108
Enabling DHCP Server Function	110
DHCP Address Pool	110
DHCP Network Pool Configuration	110
DHCP Host Pool Configuration	115
Other Global Commands	117
DHCP relay agent Features and Configuration	118
DHCP relay agent Overview	118
Enabling DHCP Relay Function	118
DHCP Server Configuration on DHCP Relay Agent	120
DHCP Relay Agent Information option (OPTION82) Configuration	122
DHCP Smart Relay Configuration	124
DHCP Relay Agent Verify MAC-Address Configuration	125
DHCP Class based DHCP packet forwarding	126
DHCP Snooping Function	128
DHCP Snooping Function Overview	128
DHCP Snooping Function Activation	128
DHCP Snooping VLAN Configuration	129
DHCP Snooping Information option (OPTION82) Configuration	129
DHCP Snooping Trust Port Configuration	130
DHCP snooping max-entry Configuration	131
DHCP Snooping Entry Time Configuration	131
DHCP Snooping Rate-Limit Configuration	132
DHCP Snooping Verify MAC-Address Configuration	132
DHCP Snooping Manual Binding Configuration	133
DHCP server Monitoring and Management	134
DHCP server Pool Information Inquiry	134
DHCP relay Monitoring and Control	135
DHCP Snooping Monitoring and Control	135
DHCP Configuration Examples	136
DHCP Network Pool Configuration	136
Example of DHCP Host Pool Configuration	136
DHCP server Monitoring and Control	137
DHCP relay agent Configuration	139
DHCP Snooping Configuration	141
Functions and Configuration of DHCPv6 Relay	142
DHCPv6 Relay Function Overview	142
Configuring DHCPv6 Relay Agent	143
Enabling U9016B DHCPv6 Relay Function	143
Setting Outgoing Interface on DHCPv6 Relay Agent	143

Setting Server from DHCPv6 Relay Agent	143
Monitoring and Managing DHCPv6 Relay	145
Examples of Configuring DHCPv6 Relay	146
Chapter 9.IGMP Snooping	149
IGMP Snooping Overview	150
IGMP Snooping Configuration.....	151
Enable IGMP Snooping on a VLAN	151
Enabling IGMP Snooping.....	151
Display System and Network Statistics	156
Chapter 10.Multicast Routing.....	157
IP Multicast Routing Overview	158
IGMP Proxy Overview	159
PIM-SM Overview	160
MVLAN Overview.....	161
IP Multicast Routing Configuration.....	161
Configure Multicast Functionality	162
Configuring IGMP Functionality	165
Configuring MVLAN Functionality	177
Display System and Network Statistics	178
Chapter 11.Statistics Monitoring.....	181
Status Monitoring	182
System Threshold Configuration	183
Temperature Configuration	183
CPU Usage Configuration.....	183
Memory Usage Configuration	184
Application Memory Usage Display	184
Port Statistics	185
RMON (Remote MONitoring)	188
RMON Overview	188
RMON Alarm and Event Group Configuration	190
Logging	193
System Log Message Context	193
Default Logging Value	194
Examples of Logging Configuration	194
sFlow.....	196
sFlow Agent	196
sFlow Collector	197
sFlow Network Configuriton	199
Chapter 12.STP, RSTP, MSTP, and SLD	201
Understanding Spanning-Tree Features	202
STP Overview	202
Bridge Protocol Data Units.....	202
Election of Root Switch	203
Bridge ID, Switch Priority, and Extended System ID	204
Spanning-Tree Timers.....	204
Creating the Spanning-Tree Topology.....	204
Spanning-Tree Interface States.....	205

Understanding RSTP	208
RSTP Overview	208
Port Roles and the Active Topology	208
Rapid Convergence	209
Bridge Protocol Data Unit Format and Processing	210
About MSTP	211
MST Region.....	211
IST, CST and CIST	211
Configuring Spanning-Tree Features	213
Default STP Configuration	213
STP Configuration Guidelines	213
Enabling STP	213
Enable STP in NO default Bridge	215
Configuring the Port Priority.....	216
Configuring the Path Cost	217
Configuring the Switch Priority of a VLAN	219
Configuring the Hello Time	221
Configuring the Forwarding-Delay Time for a VLAN.....	223
Configuring the Maximum-Aging Time for a VLAN	224
Changing the Max-hops for switch	225
Changing the Spanning-Tree mode for switch.....	226
Specifying the Link Type to Ensure Rapid Transitions	233
Configuring MSTP Features	237
Instance and port configuration	240
Setting region and revision number for MST	244
Pathcost for MSTP	244
Displaying the Spanning-Tree Status	245
Configuring Bridge MAC Forwarding	247
Self-loop Detection	249
Understanding Self-loop Detection	249

Chapter 13.BFD..... 253

Understanding BFD	254
BFD Operation.....	254
Benefits of using BFD for Failure Detection.....	254
BFD Session Type.....	255
BFD Version Interoperability	255
BFD Restrictions.....	256
Default BFD Configuration.....	256
Configuring BFD	257
Configuring BFD session parameters on the interface	257
Configuring multi-hop BFD session parameters	258
Configuring BFD support for BGP	258
Configuring BFD support for OSPF	259
Configuring BFD support for Static routing	260
Configuring Passive Mode on the Interface.....	261
Configuring BFD Echo Mode	261
Configuring BFD slow timer.....	263
Displaying BFD information	263
BFD Configuration Samples	264
Sample One: Configuring BFD in an OSPF Network.....	264

Sample Two: Configuring BFD in an BGP Network.....	266
Sample Three: Configuring BFD for static routing.....	269
Chapter 14.LACP	271
Understanding Link Aggregation Control Protocol.....	272
LACP Operation Principle	272
LACPDU Configuration	272
LACP Modes.....	272
LACP Parameters	273
Configuring LACP and SLA.....	274
Specifying the System Priority	274
Specifying the Port Priority	274
Specifying the Timeout Value	275
Configuration LACP and static port group.....	275
Clearing LACP Statistics	276
Displaying 802.3ad Statistics and Status.....	277
Chapter 15.IP-OPTION.....	279
IP OPTOIN command	280
IPv6 OPTOIN Overview	282
IPv6 OPTION DROP Command	282
IPv6 OPTOIN RATE-LIMIT Command.....	283
Chapter 16.Dynamic ARP Inspection.....	287
Understanding DAI.....	288
Understanding ARP	288
Understanding ARP Spoofing Attacks	288
Understanding DAI and ARP Spoofing Attacks	290
Interface Trust States and Network Security	290
Rate Limiting of ARP Packets	291
Relative Priority of ARP ACLs and DHCP Snooping Entries	292
Logging of Dropped Packets.....	292
Default DAI Configuration	293
DAI Configuration Guidelines and Restrictions	294
Configuring DAI.....	295
Enabling DAI on VLANs.....	295
Configuring the DAI Interface Trust State.....	296
Applying ARP ACLs for DAI Filtering.....	297
Configuring ARP Packet Rate Limiting.....	297
Enabling DAI Error-Disabled Recovery	299
Enabling Additional Validation	299
Configuring DAI Logging	302
DAI Logging Overview	302
Configuring the DAI Logging Buffer Size.....	302
Configuring the DAI Logging System Messages.....	303
Configuring the DAI Log Filtering	303
Displaying DAI Information	304
DAI Configuration Samples.....	305
Sample: Interoperate with DHCP Relay.....	305
Chapter 17.QoS and ACL	307

QOS.....	308
Global Configuration	308
TX Scheduling Configuration	308
Port Trust Mode	309
DSCP Conversion Map Configuration	310
DSCP to COS Configuration.....	310
COS Conversion Map Configuration	312
ACL Configuration.....	314
Standard IP ACL	314
Extended IP ACL	315
IPv6 Standard ACL	316
IPv6 Extended ACL	317
MAC ACL.....	318
Application of ACL to Interface	318
Service-policy Configuration	319
Class-map	319
Policy-map.....	320
Service-policy	322
COPP	323
Service-policy on COPP	323
Rate-limit on COPP	323

Chapter 18.GPON Configuration 325

GPON Overview	326
OLT/ ONT Management.....	328
Setting / View of PON OLT, Port status.....	328
Management/View of State of PON OLT and PORT (optical power alarm).....	330
Management/View of State of PON OLT and PORT (performance check)	330
Management/View of State of PON OLT and PORT (others)	330
Setting Status of ONU/ONT	331
Management/View of State of ONU/ONT (OMCI-related).....	331
Management/View of State of ONU/ONT (performance check).....	333
Management/View of State of ONU/ONT (optical power alarm)	333
ONT Registration and Display	334
Modification and Deletion of ONU/ONT Information	335
Clear counters	337
Clear unadmin-list.....	337
Automatic Deletion of unused ONU/ONT	338
ONU/ONT equip-id Authentication - Registration/Deletion/Display of equip-id.....	339
ONU/ONT equip-id Authentication: Function Usage	340
ONU/ONT Password: Setting the password function	341
ONU/ONT password function: How to perform the function	342
VLAN Mapping Table Creation (QinQ Function)	343
VoIP Config Mode.....	343
PON Environment Setting.....	344
PON OLT Environment Setting.....	344
PON ONU Environment Setting.....	349
Defective Optic Module ONT Management	356
Auto Shutdown of ONU/ONT with fiber optic module fault.....	356
Limiting the tx-power of ONT fiber optic module.....	356
Firmware upgrade.....	357

OLT firmware upgrade	357
ONT/ONU firmware upgrade (manual-upgrade)	359
ONT/ONU firmware Upgrade (Auto-Upgrade)	362
Chapter 19.IPv6 Configuration	363
Overview	364
Assigning IPv6 Address	365
ND (Neighbor Discovery)	368
Neighbor Advertisement (ND) Overview	368
Configure Neighbor Advertisement Functionality	368
Router Advertisement Overview.....	371
Configure Router Advertisement Functionality	372
IPv6 Tools.....	375
Telnet	375
Ping.....	375
Chapter 20.MLD_Snooping.....	376
MLD Snooping Overview	377
Configuring MLD Snooping	378
Enable MLD Snooping on a VLAN.....	378
Configure MLD Static Group Functionality	384
Display System and Network Statistics	385
Chapter 21.RIP.....	386
Information about RIP	387
How to Configure RIP	388
Enabling RIP	388
Allowing Unicast updates for RIP.....	388
Passive interface.....	388
Applying Offsets to Routing metrics	389
Adjusting Timers	389
Specifying a RIP Version.....	389
Applying Distance	390
Enabling Split Horizon.....	390
Configuration Examples for RIP	391
RIP Construction.....	391
Offset-list Setting.....	393
Passive-interface Configuration	394
Chapter 22.OSPF.....	395
OSPF Overview	396
Link-state Database	396
Areas	396
AREA 0	397
Stub areas.....	397
Virtual links.....	397
Route Redistribution	397
OSPF Configuration	398
OSPF interface parameters	398
Different Physical Networks	399
OSPF Network type	399

Point-to-Multipoint, Broadcast Networks.....	400
Nonbroadcast Networks	400
OSPF Area parameters	400
OSPF NSSA.....	401
OSPF Area Route Summarization	402
Route Summarization of Redistributed Routes.....	402
Virtual Links	402
Generating a Default Router.....	403
Router ID Choice with a Loopback Interface	403
Default metric	403
OSPF administrative Distance.....	403
Passive interface	404
Route Calculation Timers	404
Logging Neighbors Going Up/Down	404
Blocking LSA Flooding.....	404
Ignoring MOSPF LSA Packets.....	405
Monitoring and Maintaining OSPF.....	405

Chapter 23.BGP 407

BGP Overview	408
BGP Configuration	409
Enabling BGP Protocol.....	409
Neighbor Configuration.....	410
BGP Filtering	410
Route Filtering	410
Path Filtering	412
Community Filtering.....	413
BGP Attribute Configuration.....	415
Routing Policy Modification	428
BGP Peer Groups.....	429
BGP Multipath	431
BGP graceful-restart.....	432
BGP default-metric	433
BGP redistribute-internal	433
BGP Password encryption.....	433
BGP disable-adj-out	434
Use of set as-path prepend Command.....	434
Route Flap Dampening.....	435

Chapter 24.VRRP 436

Information about VRRP.....	437
VRRP Operation.....	437
VRRP Benefits.....	438
How to Configure VRRP	440
Enabling VRRP.....	440
Disabling VRRP on an Interface	441
Customizing VRRP.....	441
Configuring VRRP circuit failover	442
Configuration Examples for VRRP.....	443
Configuring VRRP: Example	443
VRRP circuit failover: Example.....	444

VRRP Circuit fail-over Verification: Example.....	444
Disabling a VRRP Group on an Interface: Example.....	444

List of Tables

Table 1 Command Syntax Symbol	4
Table 2 Basic Command Line Editing Command and Help	5
Table 3 Switch Command Mode	7
Table 4 Change of Switch Command Modes	7
Table 5 Commands for User Registration, Deletion, and management	11
Table 6 Commands for Enable Password Setting	12
Table 7 Commands for Setting Password Encryption Mode	13
Table 8 Commands for Setting User Authentication of Privileged Mode	15
Table 9 Commands for Setting EXEC Shell Authorization	16
Table 10 Authorization of Command Execution	16
Table 11 Session Access Management	17
Table 12 Managing Command Execution History	18
Table 13 Privilege level Configuration	18
Table 14 RADIUS Server Configuration Commands	19
Table 15 TACACS+ Server Commands	20
Table 16 Commands for Setting Hostname	21
Table 17 Commands for Setting SNMP Configuration	22
Table 18 Setting SNMP Community	22
Table 19 Commands for Setting SNMP Trap Host	24
Table 20 Commands for Setting Enable Basic SNMP Trap	24
Table 21 Commands for Setting SNMPv3	25
Table 22 Commands for setting ACL (Access Control List)	28
Table 23 Command for Login Banner and MOTD Banner	30
Table 24 Commands for Setting AFS	32
Table 25 Interfaces Supported in U9016B	38
Table 26 Common Commands	39
Table 27 Interface Name	39
Table 28 Interface ID and Range Supported	39
Table 29 Interface information and status related commands	41
Table 30 Physical port configuration commands	44
Table 31 Speed and Duplex	44
Table 32 Broadcast Suppression	46
Table 33 Port Mirroring	47
Table 34 Layer 2 Interface mode supported in U9016B	48
Table 35 Layer 2 Interface Defaults	48
Table 36 Commands to enable/disable Layer 2 interface configuration	48
Table 37 Commands for Trunk port configuration	49
Table 38 Access port configuration commands	49
Table 39 Overview of Port Group	51
Table 40 Port Group Configuration Commands	51
Table 41 Commands for VLAN Configuration	63
Table 42 Displaying VLAN Settings	68
Table 43 802.1 QinQ Command set	70
Table 44 Private Edge VLAN setting table	72
Table 45 Abnormal MAC Drop commands	74
Table 46 Available IP Addresses	76
Table 47 Commands for Assigning IP Address	77
Table 48 Commands for ARP Configuration	78

Table 49 Commands for configuring Static route path	79
Table 50 Default administrative distances of dynamic routing protocol	79
Table 51 Showing IP route Information.....	79
Table 52 Command history Function	85
Table 53 Overview of output post processing	86
Table 54 IP OPTION command	87
Table 55 SFP DDM Monitoring	87
Table 56 File Management Command.....	89
Table 57 Download/Upload with the FTP.....	91
Table 58 Down/UpLoading File with TFTP	92
Table 59. Download/Upload Command through SFTP	93
Table 60 Configuration Management Command	94
Table 61 Boot Mode Setting and System Restart	96
Table 62 Boot Mode Setting and System Reload	96
Table 63 Setting NTP Server	100
Table 64 Configuring NTP Authentication	101
Table 65 Configuring the Source IP Address for NTP Packets	101
Table 66 Configuring the System as an Authoritative NTP Server	101
Table 67 Updating the Hardware Clock	102
Table 68 Configuring the Time Zone.....	103
Table 69 Configuring Summer Time (Daylight Savings Time).....	103
Table 70 Configuring Summer Time	103
Table 71 Manually Setting the Software Clock	104
Table 72 Setting the Hardware Clock	105
Table 73 Setting the Software Clock from the Hardware Clock	105
Table 74 Setting the Hardware Clock from the Software Clock	105
Table 75 Monitoring Time and Calendar Services	106
Table 76 Enabling DHCP Server Function.....	110
Table 77 IP DHCP Pool	110
Table 78 DHCP Subnet and Network Mask Configuration.....	111
Table 79 Setting IP Address Range to be Assigned in Network Pool.....	112
Table 80 Setting the Default Router for Client	112
Table 81 Setting DNS IP Server for Client.....	112
Table 82 Setting the Domain Name for Client.....	113
Table 83 Setting Group for Network Pool	113
Table 84 Setting the Address Lease Time	115
Table 85 Setting DHCP Host Pool Name and Entering DHCP Configuration Mode	116
Table 86 Host Pool Configuration Command.....	116
Table 87 Client Configuration for DHCP Manual Binding.....	117
Table 88 Manual Binding Command.....	117
Table 89 Global Command List	117
Table 90 Enabling DHCP Relay Function	118
Table 91 DHCP Server Configuration on DHCP Relay Agent.....	120
Table 92 DHCP Server Configuration on DHCP Relay Agent.....	120
Table 93 Enabling DHCP relay agent information option.....	122
Table 94 Relay agent information option reforwarding Policy Configuration.....	123
Table 95 enabling DHCP smart-relay	124
Table 96 the number of trials that a client can change IP address	124
Table 97 DHCP Relay Agent Verify MAC-Address Configuration	125
Table 98 DHCP Class Configuration.....	126
Table 99 DHCP Relay-Pool Configuration	127
Table 100 DHCP Snooping Function Activation.....	128

Table 101 DHCP Snooping VLAN Configuration.....	129
Table 102 Enable DHCP Snooping information option function	130
Table 103 DHCP Snooping information option reforwarding policy Configuration.....	130
Table 104 DHCP Snooping Trust Port Configuration.....	131
Table 105 DHCP snooping max-entry Configuration.....	131
Table 106 DHCP Snooping Entry Time Configuration.....	131
Table 107 DHCP Snooping Rate-Limit Configuration.....	132
Table 108 DHCP Snooping Verify MAC-Address Configuration.....	132
Table 109 DHCP Snooping Manual Binding Configuration	133
Table 110 DHCP server Pool Information Inquiry	134
Table 111 DHCP Server Binding Information Search	134
Table 112 DHCP Server Statistics Search.....	134
Table 113 DHCP Server Conflict Search.....	134
Table 114 DHCP Server Variables Initialization Command	134
Table 115 DHCP relay Monitoring and Control Command	135
Table 116 Showing DHCP Snooping and Control	135
Table 117. Enabling U9016B DHCPv6 Relay Function	143
Table 118. Setting Outgoing Interface on DHCPv6 Relay Agent	143
Table 119. Setting Server from DHCPv6 Relay Agent.....	143
Table 120. Commands to Monitor and Manage DHCPv6 Relay	145
Table 121. Description on Input Message	147
Table 122 Enable IGMP Snooping on a VLAN.....	151
Table 123 IGMP Report-Suppression.....	151
Table 124 IGMP Fast-Leave	153
Table 125 IGMP Mrouter-Port	154
Table 126 IGMP Access-Group.....	154
Table 127 Multicast Group of IGMP Host only to specific VLAN interface	155
Table 128 IGMP Group-Limit.....	155
Table 129 Multicast Group number only to specific VLAN interface	155
Table 130 IGMP Snooping-related Monitoring Command	156
Table 131 Multicast Protocol	158
Table 132 Enable IP Multicast Routing.....	161
Table 133 Enable IGMP and PIM on an interface	161
Table 134 Router-Guard IP Multicast	162
Table 135 Multicast Traffic Forwarding-TTL-Limit.....	163
Table 136 Static Multicast Route Path.....	163
Table 137 Global Multicast Group-Limit	164
Table 138 Multicast Load-Split	164
Table 139 Multicast Route-Limit	164
Table 140 IGMP Version	165
Table 141 IGMP Access-Group.....	166
Table 142 IGMP Query-Interval.....	166
Table 143 IGMP Last-Member-Query-Count.....	167
Table 144 IGMP Last-Member-Query-Interval	168
Table 145 IGMP Immediate-Leave.....	168
Table 146 IGMP Group Limit.....	169
Table 147 IGMP Global Limit	169
Table 148 IGMP Minimum-Version.....	169
Table 149 IGMP Querier-Timeout	170
Table 150 IGMP Query-Max-Response-Time	170
Table 151 IGMP Rate.....	171
Table 152 IGMP Robustness-Variable	172

Table 153 IGMP Static-Group	172
Table 154 IGMP Class-Map	172
Table 155 IGMP Rate	174
Table 156 IGMP SSM-MAP	175
Table 157 IGMP SSM-MAP	175
Table 158 IGMP Proxy-Service	176
Table 159 IGMP Mroute-Proxy	176
Table 160 PIM SSM	177
Table 161 Enable MVLAN	178
Table 162 MVLAN Status Information	178
Table 163 Monitoring Commands of IP Multicast Routing	178
Table 164 Status Monitoring Command	182
Table 165 Temperature Configuration Command	183
Table 166 CPU Usage Threshold Command	183
Table 167 Memory Usage Command	184
Table 168 Memory Display Command	184
Table 169 Commands for Port Statistics Check	185
Table 170 Commands for Port Statistics Configuration	187
Table 171 Command for Initialization of Port Statistic	187
Table 172 RMON Items	189
Table 173 Commands for RMON Alarm and Event Configuration	190
Table 174 Commands for RMON History Setting and Statistics	191
Table 175 U9016B Log Level	193
Table 176 System Log Default	194
Table 177 Commands for System Message Logging Configuration	194
Table 178 sFlow Command	197
Table 179 Switch Priority Value and Extended System ID	204
Table 180 Spanning-Tree Timers	204
Table 181 Port State Comparison	209
Table 182 RSTP BPDU Flags	210
Table 183 Default STP Configuration	213
Table 184 Configuring the Port Priority	216
Table 185 Configuring the Path Cost	217
Table 186 Configuring the Switch Priority of a VLAN	219
Table 187 Configuring the Hello Time	221
Table 188 Configuring the Forwarding-Delay Time for a VLAN	223
Table 189 Configuring the Maximum-Aging Time for a VLAN	224
Table 190 Changing the Spanning-Tree mode for switch	226
Table 191 Configuring the Port as Edge Port	231
Table 192 Specifying the Link Type to Ensure Rapid Transitions	233
Table 193. Port enable	250
Table 194 Disabling Self-loop Detection	251
Table 195 Default BFD Configuration	256
Table 196 Configuring BFD session parameters on the interface	257
Table 197 Configuring multi-hop BFD session parameters	258
Table 198 Configuring BFD support for BGP	258
Table 199 Configuring BFD support for OSPF for all interface	259
Table 200 Configure BFD Support for OSPF for One or More Interface	260
Table 201 Configuring BFD support for Static routing	260
Table 202 Configuring Passive Mode on the Interface	261
Table 203 Configuring BFD Echo Mode	261
Table 204 Configuring BFD slow timer	263

Table 205 Displaying BFD information	263
Table 206 Configuring BFD in an OSPF Network	264
Table 207 BFD on specific OSPF interface	265
Table 208 Configuring BFD in an BGP Network	266
Table 209 BFD on internal BGP	268
Table 210 Configuring BFD for static routing	269
Table 211. LACPDU Configuration	272
Table 212 LACP Modes	273
Table 213 Specifying the System Priority	274
Table 214 Specifying the Port Priority	274
Table 215 Specifying the Timeout Value	275
Table 216 Configuration LACP and static port group	275
Table 217 Clearing LACP Statistics	276
Table 218 Displaying 802.3ad Statistics and Status	277
Table 219 IP OPTION command	280
Table 220 IPv6 OPTION DROP Command	282
Table 221 IPv6 OPTION RATE-LIMIT Command	283
Table 222 Default DAI Configuration	293
Table 223 Enabling DAI on a VLAN	295
Table 224 IP OPTION command	296
Table 225 Applying ARP ACLs for DAI Filtering	297
Table 226 Configuring ARP Packet Rate Limiting	298
Table 227 Enabling DAI Error-Disabled Recovery	299
Table 228 Enabling Additional Validation	299
Table 229 Configuring the DAI Logging Buffer Size	302
Table 230 Configuring the DAI Logging System Messages	303
Table 231 Configuring the DAI Log Filtering	303
Table 232 Displaying DAI Information	304
Table 233 Initialize DAI Statistics	304
Table 234 Initialize the DAI logging information	304
Table 235 DAI Configuration	305
Table 236 QOS Global Configuration Command	308
Table 237 TX Scheduling Configuration	308
Table 238 Tx-Scheduling Map Configuration Command	309
Table 239 Tx-scheduling Configuration Command	309
Table 240 Port Trust Configuration Command	310
Table 241 dscp-queue map Configuration Command	310
Table 242 Cos-Dscp map Configuration Command	312
Table 243 cos-queue map Configuration Command	312
Table 244 Cos-Dscp map Configuration Command	313
Table 245 cos-mutation Map Configuration Command	313
Table 246 Standard IP ACL Configuration Command	314
Table 247 SRC_IP_ADDRESS	314
Table 248 Extended IP ACL Configuration Command	315
Table 249 IPv6 Standard ACL	317
Table 250 IPv6 Extended ACL	317
Table 251 standard IP ACL Configuration Command	318
Table 252 Commands for the Application of ACL to Interface	318
Table 253 Class-map Configuration Command	319
Table 254 Class-map Configuration Command	321
Table 255 Service-Policy Configuration Command	322
Table 256 Commands for Control-plane of Service-policy Configuration	323

Table 257 Commands for Control-plane of Rate-limit Configuration.....	323
Table 258 Setting/View of PON OLT, PORT status.....	328
Table 259. Management/View of State of PON OLT and PORT (optical power alarm)	330
Table 260 Management/View of State of PON OLT and PORT (performance check)	330
Table 261 Management/View of State of PON OLT and PORT (others).....	330
Table 262 Setting Status of ONU/ONT	331
Table 263. Management/View of State of ONU/ONT (OMCI-related)	331
Table 264. Management/View of State of ONU/ONT (performance check)	333
Table 265. Management/View of State of ONU/ONT (optical power alarm)	333
Table 266 ONT Registration and Display.....	334
Table 267 Modification and Deletion of ONU/ONT Information	335
Table 268 Clear unadmin-list.....	337
Table 269 Automatic Deletion of unused ONU/ONT	338
Table 270 ONU/ONT equip-id Authentication - Registration/Deletion/Display of equip-id.....	339
Table 271 ONU/ONT password function: Setting the password function.....	341
Table 272 VLAN Mapping Table Creation (QinQ Function)	343
Table 273 PON OLT Environment Setting	344
Table 274 Writing and Applying OLT Service Profile.....	344
Table 275 Deleting and displaying Policy map	344
Table 276 Writing an OLT Policy-map	345
Table 277 Configuring OLT Bridge-map	346
Table 278 IP OLT Igmp-map.....	348
Table 279 PON ONU Environment	349
Table 280 PON ONU Environment Setting.....	349
Table 281 Creating and Deleting ONU Sla-map	349
Table 282 Creating and Deleting ONU policy-map	350
Table 283 Writing and Deleting ONU Bridge-map	353
Table 284 Writing and Deleting ONU Multicast-map.....	353
Table 285 Configuration and Display of ONU default service-policy.....	355
Table 286 Configuration, Display and Deletion of ONU service-policy	355
Table 287 Auto shutdown of ONU/ONT wigh fiber optic module fault.....	356
Table 288 limiting the tx-power of ONT fiber optic module	356
Table 289 OLT firmware upgrade	357
Table 290. ONT/ONU firmware upgrade (manual-upgrade)	359
Table 291 ONT/ONU firmware upgrades (TFTP)	360
Table 292 ONT/ONU firmware upgrades (auto-upgrade)	362
Table 293. Assigning IPv6 Address	365
Table 294. Neighbor Solicitation Interval	368
Table 295. Neighbor Reachable Time	369
Table 296. DAD	369
Table 297. Router Advertisement Interval.....	372
Table 298. Suppress Router Advertisement	372
Table 299. Router Advertisement Lifetime.....	373
Table 300. Router Advertisement Prefix	373
Table 301. Router Advertisement Current Hoplimit.....	374
Table 302. Router Advertisement Reachable Time.....	374
Table 303. Router Advertisement Retransmission Time	374
Table 304 Enable MLD Snooping on a VLAN.....	378
Table 305. MLD Report-Suppression	378
Table 306. MLD Fast-Leave	379
Table 307. MLD Mrouter-Port	380
Table 308. MLD Access-Group.....	381

Table 309. Ipv6 mld snooping access-group	381
Table 310. MLD Group-Limit	382
Table 311. Ipv6 mld snooping limit	382
Table 312. Ipv6 mld limit.....	382
Table 313. Limit the number of all multicast groups	383
Table 314. MLD snooping forced-source-ip.....	383
Table 315. MLD snooping version	383
Table 316. MLD snooping version.....	384
Table 317. MLD Snooping-related Monitoring Command.....	385
Table 318 Enabling RIP.....	388
Table 319 Allowing Unicast updates for RIP.....	388
Table 320 Passive interface	388
Table 321 Applying Offsets to Routing metrics	389
Table 322 Adjusting Timers	389
Table 323 Specifying a RIP Version	389
Table 324 Specifying a RIP Version	389
Table 325 Specifying a RIP Version	390
Table 326 Applying Distance	390
Table 327 Enabling Split Horizon	390
Table 328 LSA Type number	396
Table 329 OSPF interface parameter CLI	398
Table 330 OSPF network type CLI	399
Table 331 P-to-Multipoint Network, Broadcast Network Configuration	400
Table 332 Nonbroadcast network CLI	400
Table 333 Nonbroadcast network Configuration	400
Table 334 OSPF area parameter CLI.....	401
Table 335 OSPF NSSA CLI.....	401
Table 336 OSPF area router summarization CLI	402
Table 337 External Router summarization CLI	402
Table 338 OSPF virtual link CLI	402
Table 339 OSPF default route CLI	403
Table 340 Loopback Interface Configuration.....	403
Table 341 Reference bandwidth CLI	403
Table 342 OSPF distance CLI.....	404
Table 343 OSPF passive interface CLI	404
Table 344 OSPF SPF timer CLI	404
Table 345 OSPF adjacency LOG CLI.....	404
Table 346 Block LSA CLI.....	404
Table 347 Ignore MOSPF LSA CLI	405
Table 348 Monitoring OSPF CLI	405
Table 349 Maintaining OSPF CLI.....	406
Table 350 Terminology used in route dampening.....	435
Table 351 Enabling VRRP.....	440
Table 352 Disabling VRRP on an Interface	441
Table 353 Customizing VRRP	441
Table 354 Configuring VRRP circuit failover	442

List of Figures

Figure 2. Example of a Port-based VLAN Configuration (U9016B)	56
Figure 3. Single Port-based VLANs Connecting 2 Switches	57
Figure 4. Two Port-based VLANs Connecting 2 Switches	57
Figure 5. Physical Diagram of Tagged and Untagged Frame	59
Figure 6. Logical Diagram of Tagged Frame and Untagged frame	60
Figure 7. Native VLAN.....	61
Figure 8. Configuration Example – Tagged and Untagged VLAN.....	66
Figure 9. Configuring 802.1 QinQ.....	71
Figure 10. Network Configuration Example – multiple IP address.....	80
Figure 11. Network Configuration Example – Static route	81
Figure 12. U9016BSwitch as a DHCP server.....	109
Figure 13. Message transmissions of DHCP server as a DHCP relay agent	118
Figure 14. DHCP Relay Option82.....	122
Figure 15. DHCP Smart-Relay running procedure	124
Figure 16. DHCP Class based on DHCP packet Relay	126
Figure 17. Network – DHCP Relay Agent Configuration.....	139
Figure 18. DHCP Snooping Configuration.....	141
Figure 19. DHCPv6 Relay Agent sends a message to DHCPv6 Server.....	142
Figure 20. Example Network – Configuring DHCPv6 Relay Agent.....	146
Figure 21. Multicasting to Transmit Traffic to Many Destinations.....	158
Figure 22. RMON Manager and RMON Probe.....	188
Figure 23 Key Map of sFlow (sFlow agent and collector)	196
Figure 24. sFlow Network Configuration	199
Figure 25. Traffic flow sampling	200
Figure 26. Interface statistics sampling	200
Figure 27. Spanning-Tree Topology.....	204
Figure 28. Spanning-Tree Interface States	205
Figure 29. Proposal and Agreement Handshaking for Rapid Convergence	210
Figure 30. Load Balance	211
Figure 31. CST, IST, CIST	212
Figure 32. The network of View from CST.....	212
Figure 33. restricted-tcn.....	237
Figure 34. Environment Where a Self-loop is Formed.....	249
Figure 35. Establishing a BFD neighbor relationship.....	254
Figure 36. Tearing down an OSPF neighbor relationship	254
Figure 37. BFD single hop session.....	255
Figure 38. BFD multhop session	255
Figure 39. Configuring BFD in an OSPF Network	264
Figure 40. Configuring BFD in an BGP Network	266
Figure 41. Configuring BFD for static routing	269
Figure 42. Understanding ARP	288
Figure 43. Understanding ARP Spoofing Attacks.....	289
Figure 44. Understanding ARP Spoofing Attacks.....	289
Figure 45. Interface Trust States and Network Security	291
Figure 46. Hierarchy of Policy-Map	320
Figure 47. Basic Structure of PON	326
Figure 48. Architecture of GPON.....	326
Figure 49 IPv6 Neighbor Solicitation-Neighbor Advertisement Message.....	368

Figure 50 IPv6 Router Advertisement Message (Periodic).....	371
Figure 51 IPv6 Router Solicitation-Router Advertisement Message.....	371
Figure 52. RIP Network Configuration Example and Diagram	391
Figure 53. OSPF Network	401
Figure 54. Route Filtering.....	411
Figure 55. Path Filtering.....	412
Figure 56. Community Filtering	413
Figure 57. As_path Attribute.....	416
Figure 58. Origin Attribute	417
Figure 59. BGP Nexthop Attribute	418
Figure 60. BGP Nexthop (Multiple access networks)	420
Figure 61. BGP Nexthop (NBMA)	421
Figure 62. Local Preference Attribute.....	422
Figure 63. Metric Attribute	424
Figure 64. Weight Attribute.....	427
Figure 65. BGP backdoor.....	430
Figure 66. Basic VRRP Topology	437
Figure 67. Load Sharing and Redundancy VRRP Topology	438

Chapter 1. Overview

This chapter provides the following information required for system users to set up configuration and start up U9016B.

- Command line edit and help
- Switch command mode
- Switch startup
- U9016B user interface
- Login and password setting
- SNMP configuration
- Viewing and saving the files and configuration of switch
- Access list
- Telnet Client

Command Line Editor and Help

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

Command Syntax

The following are the steps necessary to enter a command. More information about using command-line interface is described in the following chapter.

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

1. When entering a command at the prompt, make sure that you have the appropriate privilege level. Most configuration commands require the administrator privilege level.
2. Enter a command. If the command does not include a parameter or value, go to step 3.
 - If the command includes a parameter, enter the parameter name and any values.
 - The value of the command specifies how you want the parameter to be set. Values include numbers, strings, or addresses, depending on the parameter.
3. 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 U9016B has built-in command syntax helper. Help may be requested at any point in a command by entering a question mark '?'. U9016B provides two styles of help.

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 to know which arguments match the input (e.g. 'show me?'). There is no space between the command and question mark.

The following shows an example of full help with 'show' command.

When '?' mark is used together with a space after 'show' command, the list of parameters and values that the administrator can use will be displayed. Then the cursor awaits input from the administrator, blinking in the "Switch# show" prompt. The question mark '?' is not displayed on the terminal screen.

```
.Switch# show ?
access-list      List IP Access Lists
arp              Internet Protocol (IP)
bfd              BFD Information
bgp              Border Gateway Protocol (BGP)
bootvar          Boot and Related Environment Variables
```

bridge	Bridge Information
cal	Shows CAL
calendar	Displays the Hardware Calendar
class-map	Class Map Entry
cli	Shows the CLI Tree of the Current Mode
clock	Displays the System Clock
command	Shell Command
cpu	CPU Status and Configuration
debugging	Debugging Functions (see also 'undebug')
disk1:	disk1: File System
dot1x	IEEE 802.1X Port-Based Access Control
environment	Temperature and FAN Status Information
etherchannel	EtherChannel Information
flash:	Displays Information about the flash: File System
flowcontrol	IEEE 802.3x Flow Control
fm-status	Show the Current Status
history	Display the Session Command History
hosts	IP Domain-Name, Lookup Style and Nameservers
idprom	Show IDPROMs for FRUs
inet-service	Display Enabled Internet Services
interface	IP Interface Status and Configuration
ip	Internet Protocol (IP)
ipv6	Internet Protocol Version 6 (IPv6)
lACP	LACP Commands
lACP-counter	LACP Commands
list	Show Command Lists
logging	Show the Contents of Logging Buffers
mac-access-list	List MAC Access Lists
mac-address-table	MAC Forwarding Table
memory	Memory Information
mirror	Port Mirroring
mls	mls Global Commands
module	Module Info
nsm	NSM
ntp	Network Time Protocol
policy-map	Policy Map Entry
port	Port Commands
port-mib	Port-Mib Count
power	Switches Power
pppoe	Point-to-Point over Ethernet (PPPoE)
privilege	Displays your Current Level of Privilege
processes	Active Process Statistics
redundancy	Redundancy Facility (RF) Information
reload	Scheduled reload information
rmon	Remote Monitoring Protocol (RMON)
route-map	Route-Map Information
router-guard	Multicast Router-Guard Commands
router-id	Router ID
running-config	Current Operating configuration
service	Setup Miscellaneous Services
service-policy	Service Policy Entry
slot	Slot Info
snmp	Shows snmp Statistics
spanning-tree	Displays Spanning Tree Information
startup-config	Contents of Startup Configuration
system	Displays System Information
tech-support	Shows System Information for Tech-Support
uptime	Displays Elapsed Time Since Boot
usbflash:	usbflash: File System
users	Displays Information about Terminal Lines
version	System Software Status
virtual-servers	Virtual-Servers
VLAN	Displays VLAN Information
vrrp	VRRP Information

whoami Displays Information about the Current User

Switch #show_

The result of 'show' command when the partial help function is used is as below. If '?' is entered after 'show' command, the description on the show command is displayed, and a blinking cursor waits the next command input.

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

Enter 'p' and a question mark '?' with no space when you wish to check the status of a port, but do not know the right command. CLI helper provides a list of options for the remainder of command as below. The command entered by the administrator is displayed again, and a blinking cursor waits the next input.

```
Switch# show p?
      policy-map  Policy map entry
      port        port commands
      port-mib    Port-Mib Count
      power       Switch Power
      pppoe       Point-to-Point over Ethernet (PPPoE)
      privilege   Display your current level of privilege
      processes   Active process statistics
Switch# show p_
```

Abbreviated Syntax

U9016B CLI supports abbreviated syntax, the shortest, most unambiguous, allowable abbreviation of a command or parameter. Typically, this is the first two or three letters of the command.



Notice

When using abbreviated command syntax, users must enter enough characters to make the command unambiguous and distinguishable to U9016B. Users may receive - %Ambiguous command, which means there are more than one command with the same prefix that you have entered in the mode.

```
Switch# show i
% Ambiguous command: "show i"
Switch# show i?
      idprom      show IDPROMs for FRUs
      inet-service Display enabled internet services
      interface   IP interface status and configuration
      ip          Internet Protocol (IP)
      ipv6        Internet Protocol version 6 (IPv6)
Switch# show i_
```

Command Symbols

Various symbols are used to describe the command syntax in this guide. These symbols explain how to enter the command and parameters. The following table summarizes the symbols applied to the system command syntax.

Table 1 Command Syntax Symbol

Symbol	Name	Description
<>:	Angle	Enclose a variable or value in the command syntax. You must specify the

	brackets	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 lists to specify the 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 the access or trunk mode of the switch port in the command. Do not type the vertical bar.
<i>Italic</i>		Variables to enter
Bold		The command the administrator must enter
A.B.C.D		IP address or subnet mask
A.B.C.D/M		IP prefix (e.g. 192.168.0.0/24)

Command Line Editing Key and Help Function

The CLI of U9016B supports Emacs-like line editing commands. The following table describes the line-editing keys used in the CLI.

Table 2 Basic Command Line Editing Command and Help

Command	Description
[Ctrl] + [A]	Moves the cursor to the beginning of the line.
[Ctrl] + [E]	Moves the cursor to the end of the line.
[Ctrl] + [B]	Moves the cursor to the next word.
[Ctrl] + [F]	Moves the cursor to the left character.
Backspace	Deletes the character in front of the cursor.
[Ctrl] + [K]	Deletes all the characters from the cursor to the end of the line
[Ctrl] + [U]	Deletes 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 remaining part of the command is completed.
[Ctrl] + [P] or ↑	Displays the history of the last 20 commands you have entered.
[Ctrl] + [N] or ↓	Displays the next command.
?	Displays 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

U9016B provides the following various CLI (Command Line Interface) access modes, as shown in the following table. Various commands of each switch offer different authority to an administrator.

Table 3 Switch Command Mode

Access Mode	Prompt	Description
User mode	Switch>	Displays common statistical information.
Privileged mode	Switch#	Uses the Show or Debug commands
Config mode	Switch(config) #	Changes the scope of the switch configuration into global.
Interface mode	Switch(config-if-Giga1/1)# Switch(config-if-vlan1)#	Changes the configuration of the switch interface.
Router mode	Switch(config-rip)# Switch(config-ospf)#	Changes the configuration of routing protocols such as RIP or OSPF.
DHCP pool mode	Switch(config-dhcp)#	Configures the DHCP address pool.



Notice

The command prompt uses the name of the U9016B as the host name in front of character(s) of each mode. The prompt 'Switch' will be used as common host name throughout this manual.

When you set up the configuration of U9016B, you 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 that are used to change command prompt mode are described in the following table:

Table 4 Change of Switch Command Modes

Command	Description
enable	Moves from the User mode to the Privileged mode. Needs to enter the password of the Privileged mode.
disable	Moves from the Privileged mode to the User mode.
configure terminal	Moves from the Privileged mode to the Config mode.
interface <i>[ifname]</i>	Moves from the Config mode to the Interface mode.
router <i>{rip ospf}</i>	Moves from the Config mode to the Router mode.
exit	Moves back to the previous mode.
end	Moves from any mode to the Privileged mode. Do not move from the User mode.
ip dhcp pool <i>name</i>	Moves from the Config mode to the DHCP Pool mode

U9016B Startup

When starting up the switch for the first time, U9016B performs a self test which loads the OS image from the flash 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, U9016B manages two OS images including Primary and Secondary. The Primary OS image can be loaded by the default settings. The system administrator can change the configuration in either switch boot mode or privileged mode.

User Interface

Network administrators can access the OLT for configuration setting, configuration verification, and switch status management and etc. The simplest way to access the switch is by local OAM terminal connected to the separate console port that U9016B offers (*Out-of-band management*).

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

The system administrator can use the following methods to manage U9016B.

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

U9016B support up to multiple user sessions concurrently, as follows:

- 1 console session
- Up to 10 Telnet sessions



Notice

For the security to access the system or server, the some specific system can only use the SSH2 with the accessing way.

If the telnet does not work to connect the system, try SSH2 connection way.

Connection through Console Port

The command-line interface built into the system is accessible by RJ-45 type Ethernet port console. OAM terminal (or workstation with terminal-emulation software) must support 9-pin, RS-232 DB9 port. Console port is located at the back of U9016B *SGIM* (Switching, Gigabit Ethernet I/O & Management Module).

Connect the terminal to the console port provided by U9016B, as shown in the following figure. Once a connection is established, you will see the switch prompt and you can log in.

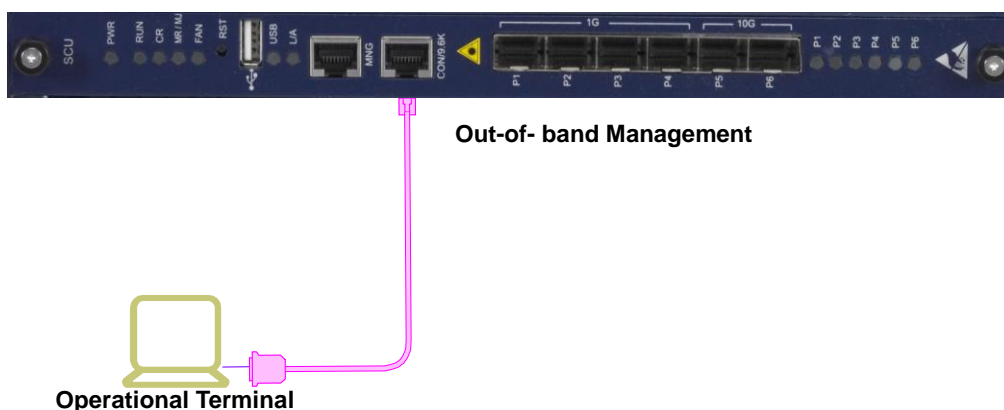


Figure 1 Connection of U9016B and OAM Terminal



Notice

For the information on the terminal configuration and console port pinouts, refer to the U9016B Hardware Installation Guide.

Connection through Telnet

You can connect to U9016B at a workstation with Telnet or TCP/IP. In order to use Telnet you must setup an ID and password first, and your switch must have at least one IP address.

```
Telnet [<ipaddress> | <hostname>] {<port_number>}
```

After the Telnet connection is successfully completed, a prompt for user password will be displayed. When you type in the Telnet user password, you will enter into *User mode* of the switch.

For security purposes, you can use access list to restrict the Telnet connection.

Connection through SNMP Network Manager

Any network manager running the Simple Network Management Protocol (SNMP) can manage the U9016B.

**Notice**

For more information on SNMP Network Manager.

User Management

Add/Delete User

A system manager can connect to the system using a console port or Telnet to configure or manage U9016B. You can manage users connected to the system by configuring ID and password, and give different authorities using the privilege level.

A new user has a privilege level set as 1 and can enter the privileged mode. If you execute "enable" command in user mode, you can enter privileged mode.

The following list describes privilege levels:

- Privilege level 0 is non-privileged status.
- Privilege level 1-14 can execute user mode commands.
- Privilege level 15 can execute privilege mode commands.

Table 5 Commands for User Registration, Deletion, and management

Command	Description	Mode
<code>username name {[password [0 7] password secret [0 5] password]}</code>	Registers users. password or secret: When you log in the system, the system prompts for this. The password and secret value are as follows: 0 – No encryption. 5 – MD5 encryption. 7 – DES encryption.	Config
<code>no username name</code>	Deletes a user. In case that user is root, the password is changed as default value.	Config
<code>username name privilege <0-15></code>	Changes a user's privilege level.	Config
<code>username name access-class <1-99></code>	Enables access-list. <1-99> : IP standard access list	Config
<code>no username name access-class</code>	Disable access-list.	Config
<code>username name user-maxlinks value</code>	Sets maximum session numbers	Config
<code>no username name user-maxlinks value</code>	Changes maximum session number as default value. Default: 32	Config
<code>username name unlimited-session-ip A.B.C.D</code>	Enables unlimited session ip as user name.	Config
<code>no username name unlimited-session-ip</code>	Disables unlimited session ip as user name.	Config

Add User

The following example shows how to set user name, password and privilege level:

```
Switch# configure terminal
Switch# configure terminal
Switch(config)# username testuser2 password testpw
Switch(config)# username testuser3 privilege 15 password testpw
Switch(config)# end
Switch # show running-config
!
username testuser2 password 0 testpw
username testuser3 privilege 15 password 0 testpw
!
```

Switch#

However, because this setting way shows the user password on the screen, we provide the following setting way not to show the password.

```
Switch# configure terminal
Switch (config)# username testuser4 password
Password:
Retype Password:
Switch (config)# end
Switch # show running-config
!
username testuser4 privilege 15 password 0 SQW92SWDAS
!
Switch#
```

The following shows an example where 'testuser3', privilege level 15, logs into privileged mode.

```
UbiQuoss L3 Switch

Switch login: testuser3
Password: testuser3

Hello.

Switch> enable
Switch#
```



Notice

After you set AAA authorization exec command, in the case that your level is more than the privilege level 15, you can enter the privileged mode directly.

Password Setting

U9016B is able to configure user password and enable password for system security.

For security purposes U9016B allows to setup user password and enable password.

Enable password

- Used for security in 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 enable password setting.

Table 6 Commands for Enable Password Setting

Command	Description	Mode
enable password {password [0 7] password} secret [0 5] password}	Sets the password to access the privileged mode. password or secret: When you enter the privileged mode, You need to enter the password. The password and the secret value differ according to the method of encryption. 0 – None Encryption.	Config

	5 – MD5 Encryption 7 – DES Encryption	
no enable password	Disables the password configuration to enter the privileged mode.	Config

Setting Enable password

The following example shows how to enable a password for access to privileged mode.

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

If you enter the set password, access is granted to privileged mode.

```
Switch
Switch login: root
Password:
Hello.
Switch>enable
Password: testpw
Switch#
```

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

Table 7 Commands for Setting Password Encryption Mode

Command	Description	Mode
service password-encryption	Enables password-encryption.	Config
no service password-encryption	Disables password-encryption.	Config



Notice

You can not decrypt with “**no service password-encryption**” command. This command is only to disable the encryption-password service.

Enabling Password Encryption Mode

If you enable password encryption mode, display the password as encryption status.

```
Switch# configure terminal
Switch(config)# service password-encryption
Switch(config)# end
Switch# show running-config
!
enable password 7 xxEp88GxHJlgc
username testuser2 password 7 XX1LtbDbOY4
username testuser3 privilege 15 password 7 XX1LtbDbOY4
!
```

AAA (Authentication Authorization Accounting)

The system 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.

Authentication

Three ways of user authentication are as follows:

- Local
- RADIUS
- TACACS+

You can set authentication more than one way. In the case of setting various methods of authentication, the system attempts authentication in the order set. In the case that the user does not receive a result of the success or failure of authentication, you must set various methods of authentication for trying authentication with ways of another authentication. In the case of trying authentication with Local system, if the information about user who want to log in or enter privileged mode does not exist, the system attempts authentication with the next set way.

Local authentication is always enabled. In case that you does not specify authentication setting, the sytem does user authentication with Local authentication way basically.

User Authentication

The system attempts authentication with the user name and password for the user. It is possible to authenticate via the local system for user information, as well as via RADIUS or TACACS+. To authenticate via the local system, the user must be already registered.

Command	Description	Mode
AAA authentication login default {local radius tacacs+}	Chooses the authentication system (local, radius, and tacacs+). Various authentication methods are possible.	Config
no AAA authentication login default	Backs to default about authentication login. Default: Local	Config
AAA authentication login template-user <i>name</i>	User authenticated by RADIUS or TACACS+ can not login without local account. The user should set up account to use.	Config
no AAA authentication login template-user	Clears the account of users without an account	Config
AAA authentication login authen-type (chap pap)	In the case of authentication with TACACS+, it sends an authentication message by the chap or par methods. Default: Ascii	Config
no AAA authentication login authen-type	Clears the account of users without account	Config

Setting User Authentication

Three ways of user authentication are as following:

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

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

```
Switch# configure terminal
Switch(config)# AAA authentication login default tacacs+ radius
Switch(config)# end
Switch#
```

Enable Password Authentication

When you want to enter the privileged mode, you can authenticate with the password enabled. In the case of authentication with the local system, it performs authentication via the password enabled for the system.

It can also perform authentication via RADIUS or TACACS+. When you do not set password to the local system, the authentication method always succeeds. So you must set enable password to perform authentication with privileged mode.

Table 8 Commands for Setting User Authentication of Privileged Mode

Command	Description	Mode
AAA authentication enable default {enable radius tacacs+}	Authenticates about enable password.	Config
no AAA authentication enable default	Backs to default. Default: enable password(Local system)	Config

Setting User Authentication of Privileged Mode

If the user enters privileged mode, the system attempts authentication to the TACACS+ server about the password enabled. If the system does not receive a response from TACACS+, it attempts authentication to the RADIUS server. In the same way, if the system dose not receive response from RADIUS server, it try authentication via the local system.

```
Switch# configure terminal
Switch(config)# AAA authentication enable default tacacs+ radius
Switch(config)# end
Switch#
```

Authorization

The system checks the authorization level for using the system resources via preivilege level. When you execute EXEC shell, it compares the user's privilege level with the user's privilege level setting using the local system or a remote server (RADIUS or TACACS+). In the case that the privilege level of a user who wants to use the particular system resource is lower than the set privilege level, the system shows an error message and fails to execute. When you also execute specific command, the sysem compares the privilege level of each command with the privilege level set. Then the system can check the executive authorization of relevant command via the local system or remote server (TACACS+).

In the case that the system does not receive the result from the authorization server or else fails to connect with the authorization server, you must always add the method of authorization verification

from the local system. In the case of authorization verification with the local system, the system always fails authorization verification. In this case, you need to change this via the settings console. The user who logs in the system via the console does not need to have authorization checked.

Authorization for EXEC Activation

When you enter the privileged mode, the EXEC shell executed is user definition shell. The authorization that can executes the EXEC shell makes sure that the user's privilege level is registered with the system. In the case that the system makes sure the user's EXEC shell execution authorization is with a RADIUS or TACACS+ server, you must set the user's privilege information for checking authorization to the relevant server.

Table 9 Commands for Setting EXEC Shell Authorization

Command	Description	Mode
AAA authorization exec default [local radius tacacs+]	Checks authorization to execute EXEC shell with user's privilege level.	Config
no AAA authorization exec default	Does not check authorization to execute EXEC shell.	Config

Checking EXEC shell Execution Authorization with TACACS+ Server

When you execute EXEC shell, the system checks authorization by referring to the user's privilege level setting to TACACS+. Furthermore, in the case that the system does not receive a result from the TACACS+ server, the system can check authorization from the local system.

The following example shows how to set authorization for EXEC activation.

```
Switch# configure terminal
Switch(config)# AAA authorization exec default tacacs+ local
Switch(config)#
Switch# exit
```

In the case that 'testuser1' user is registered with a TACACS+ server and the privilege level is set with 15, you can do EXEC shell after logging in as in the following (In this case, as the privilege level is more than 15, you can enter privileged mode directly).

```
L3 Switch
Switch login: testuser1
Password: testuser1
Hello.
Switch#
```

Authorization of Command Execution

When you execute a specific command, you can check the command execution authorization with the privilege level given to a command. In other words, the privilege level of each command has the privilege level of the mode that the command is executed and you can change the settings as necessary. The system can check the execution authorization of a specific command via the local system or a TACACS+ server.

You can set the command group for checking authorization with designating privilege level that command is executed. The system can check the executable authorization from the local system or TACACS+ server about whether the command has the relevant privilege level.

Table 10 Authorization of Command Execution

Command	Description	Mode
aaa authorization commands <0-15> default (tacacs+ local)	Sets to do checking authorization to execute command in privilege level with the local system or TACACS+ server.	Config

	<0-15>: privilege level	
no AAA authorization commands <0-15> default	Sets to do not check for authorization to execute the command at the privilege level. <0-15>: privilege level	Config

Checking Command Execution Authorization with TACACS+ Server

The following example shows how to check the authorization of command execution using a TACACS+ server when the interface command is executed in config mode. When there is a failure to connect to the TACACS+ server, the command execution authorization is checked by the local server. Set the interface command to Privilege Level 2 and then check the authorization for the Privilege Level 2. When the TACACS+ server successfully operates, the TACACS+ server determines whether to deny or permit the command authorization set. When the TACACS+ server does not successfully operate, this is determined by the local server. If the privilege level of the connected user is lower than the specified level, user access is denied based on the privilege config level 2 interface command.

The following example shows how to check authorization of command execution with TACACS+.

```
Switch# configure terminal
Switch(config)# privilege config level 2 interface
Switch(config)# AAA authorization commands 2 default tacacs+ local
Switch(config)# end
Switch#
Switch# show command privilege
COMMAND-MODE      LEVEL    Command
=====
config             2        interface
Switch#
```

When you execute interface command in the case of authorization, the following error occurs:

```
Switch (config)# interface VLAN 1
% Command authorization failed
Switch (config)#
```

Accounting

The system can manage session access history and command execution history via the AAA accounting.

Session Access Management

You can record the system access history to the TACACS+ server with the following command:

Table 11 Session Access Management

Command	Description	Mode
AAA accounting exec default (start-stop stop-only) tacacs+	Sends system access history to TACACS+ server. start-stop: Records start-stop log stop-only: Only records stop log	Config
no AAA accounting exec default	Does not send system access history to TACACS+ server.	Config

The following example shows how to send session access status to TACACS+ server.

```
Switch# configure terminal
Switch(config)# AAA accounting exec default start-stop tacacs+
```


Managing Command Execution History

When you execute specific command, you can manage execution history with TACACS+ server.

In other words, each command has a privilege level, and you can change the settings as necessary.

Table 12 Managing Command Execution History

Command	Description	Mode
AAA accounting commands <0-15> default tacacs+	Records command execution history having relevant privilege level to TACACS+ server. <0-15>: privilege level.	Config
no AAA accounting commands <0-15> default	Does not record command execution history having relevant privilege level to TACACS+ server. <0-15>: privilege level.	Config

Command Execution Status Management

The following example shows how to change the privilege level of all show commands in the EXEC mode as 15 and send execution history to TACACS+ server. In other words, all commands being privilege level 15 also send the execution history to the TACACS+ server.

```
Switch# configure terminal
Switch(config)# privilege exec level 15 show
Switch(config)# AAA accounting commands 15 default tacacs+
Switch(config)# end
Switch#
Switch# show command privilege
COMMAND-MODE      LEVEL    Command
=====
config             15      show
Switch#
```

Privilege level Configuration

The system is able to perform authorization and accounting functions for specific commands via the privilege level. In the case that you do not set the privilege level about specific command, each command refers to the executed mode of the privilege level.

Table 13 Privilege level Configuration

Command	Description	Mode
privilege <i>mode</i> level <0-15> <i>command</i>	Assigns privilege level about specific command. <0-15>: privilege level	Config
no privilege <i>mode</i> level <0-15> <i>command</i>	Changes privilege level to default value about specific command. Default: privilege level of command execution mode.	Config
show command privilege	Shows the current information.	Privileged

Server Configuration

U9016B provide features such as authentication through remote server, authorization, and account management to control the RADIUS or TACACS+ server. The following are the various configurations of the RADIUS and TACAS+ servers.

RADIUS Server Configuration

Table 14 RADIUS Server Configuration Commands

Command	Description	Mode
radius-server host (<i>A.B.C.D/X::X:X</i>) [key [0 7] <i>key-string</i>]	Sets RADIUS server. <i>A.B.C.D</i> : RADIUS server address <i>X::X:X</i> : RADIUS server IPv6 address key: Sets encryption key. 0 – Does not encryption 7 – DES encryption	Config
no radius-server host (<i>A.B.C.D/X::X:X</i>)	Deletes the set RADIUS server. <i>A.B.C.D</i> : RADIUS server address <i>X::X:X</i> : RADIUS server IPv6 address	Config
radius-server host (<i>A.B.C.D/X::X:X</i>) [auth-port <i>PORT</i>]	Sets RADIUS server and auth-port for using to server. <i>A.B.C.D</i> : RADIUS server address <i>X::X:X</i> : RADIUS server IPv6 address <i>PORT</i> : auth-port number	Config
no radius-server host (<i>A.B.C.D/X::X:X</i>) auth-port <i>PORT</i>	Sets auth-port for using to server with default value. Default: 1812	Config
radius-server key [0 7] <i>key-string</i>	Sets common encryption key for using when the system connects to RADIUS server.	Config
no radius-server key	Deletes common encryption key.	Config
radius-server retransmit <i>count</i>	Sets count retransmitting AAA information to RADIUS server. <i>count</i> : Sets count number.	Config
no radius-server retransmit	Sets retransmitting number with default value. Default: 3 times	Config
radius-server timeout <i>seconds</i>	Sets timeout from RADIUS server. <i>seconds</i> : Timeout setting with second	Config
no radius-server timeout	Sets timeout with default value. Default: 5 seconds	Config
ip radius source-interface <i>ifname</i>	Sets source IP address of information for sending to RADIUS server. <i>ifname</i> : interface name information	Config
no ip radius source-interface	Disables the set source IP address.	Config

The following example shows how to set some RADIUS server and common secret key with test 123. It sends AAA information to server. If the system does not receive response, it attempts to send it to the next RADIUS server.

```
Switch# configure terminal
Switch(config)# radius-server host 192.168.0.1
Switch(config)# radius-server key test123
Switch(config)# radius-server host 192.168.0.2 key 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#
```

TACACS+ Server Configuration

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

Table 15 TACACS+ Server Commands

Command	Description	Mode
tacacs-server host (A.B.C.D/X::X:X) key [0 7] <i>key-string</i>	Sets TACACS+ server. A.B.C.D: TACACS+ server address X::X:X : RADIUS server IPv6 address Key: Sets security key. 0 – None Encryption 7 – DES Encryption	Config
no tacacs-server host (A.B.C.D/X::X:X)	Deletes tacacs+ server setting. A.B.C.D: TACACS+ server address X::X:X : RADIUS server IPv6 address	Config
tacacs-server host (A.B.C.D/X::X:X) timeout <i>seconds</i>	Sets timeout vaule with TACACS+ server. <i>seconds</i> : Timeout value	Config
tacacs-server host (A.B.C.D/X::X:X) timeout	Sets default timeout Default: 5 seconds	Config
ip tacacs source-interface <i>ifname</i>	Sets source IP address of information sent to TACACS+ server. <i>ifname</i> : Interface name	Config
no ip tacacs source-interface	Remove source IP address.	Config

The following example shows how to set TACACS+ Server.

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

Setting Hostname

Hostname 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 mode. In U9016B, the system model name is the default hostname and the administrator can change the default hostname to a new hostname.

Table 16 Commands for Setting Hostname

Command	Description	Mode
hostname <i>string</i>	Changes hostname	Config
no hostname	Changes hostname with default name	Config

The following example shows how to set or change the hostname.

```
Switch# configure terminal
Switch(config)# hostname U9016B
U9016B(config)# end
U9016B#
U9016B# configure terminal
U9016B(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 a user interface for ease of management. You have to properly configure the switch environment in order to use the SNMP manager to manage the system.

SNMP Configuration

The following commands are for setting the SNMP configuration.

Table 17 Commands for Setting SNMP Configuration

Command	Description	Mode
snmp-server contact <i>string</i>	Enters the information of system manager	Config
no snmp-server contact	Deletes the information of system manager	Config
snmp-server location <i>string</i>	Enters the location information where switch is installed.	Config
no snmp-server location	Deletes Input the location information where switch is installed.	Config

The following example shows how to set the information of the system manager:

```
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#
```

The following example shows how to set the system location information:

```
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#
```

SNMP Community

Network Operator can access the SNMP agent and read or write MIB information. When connecting to the SNMP agent, the network manager is authenticated as a community. There are two types of community strings on U9016B.

Read-only community

- Access to the system in read-only mode

Read-write community

- Access to the system in read and write mode

Table 18 Setting SNMP Community

Command	Description	Mode
---------	-------------	------

snmp-server community <i>string</i> [<i>access-type</i>] view <i>view-name</i> <1-99>]	Set the SNMP community access-type: SNMP Agent access type ro: read only rw: read write View: designates MIB access scope, the detail information refers to snmp-server view setting. <1-99>: Applies access-list about access host.	Config
no snmp-server community <i>string</i>	Deletes SNMP community.	Config

The following example shows how to set 'testcom' community of read-write access type:

```
Switch# configure terminal
Switch(config)# snmp-server community testcom rw 99
Switch(config)# end
Switch# show running-config
!
snmp-server community testcom rw access-class 99
!
Switch#
```

SNMP Trap host

The system can provide the event like system running error or system status change to a network manager with a setting trap. The system provides the following trap version. In other words, if you can not set trap command or trap host, the trap does not occur.

SNMPv1 Trap

SNMPv2c Trap

- Basic trap version

SNMPv3 Trap

- Supports authentication and encryption function, you can set security model.
1. noAuth: does not authentication and encryption.
 2. Auth: does authentication.
 3. Priv: does authentication and encryption.

Table 19 Commands for Setting SNMP Trap Host

Command	Description	Mode
snmp-server trap-host <i>A.B.C.D</i> [version 1 2c 3 <i>sec-level</i>] <i>community-string</i>	Sets the host for sending trap. <i>A.B.C.D</i> : trap host address version: trap version (Default: 2c) <i>sec-level</i> : In the case of trap version , sets security model. <i>community-string</i> : community configuration	Config
no snmp-server trap-host <i>A.B.C.D</i> [version 1 2c 3 <i>sec-level</i>] <i>community-string</i>	Deletes trap host	Config
snmp-server trap-source <i>ifname</i>	Sets source IP address of trap for sending. <i>ifname</i> : interface name	Config
no snmp-server trap-source	Removes source IP address	Config

Table 20 Commands for Setting Enable Basic SNMP Trap

Command	Description	Mode
snmp-server enable traps alarm [fallingAlarm risingAlarm]	Enables trap for sending RMON alar.	Config
no snmp-server enable traps alarm [fallingAlarm risingAlarm]	Disables trap for sending RMON alarm.	Config
snmp-server enable traps envmon [ext- supply fan supply temperature]	Enables trap for sending system environment (fan, power, etc) information.	Config
no snmp-server enable traps envmon [ext- supply fan supply temperature]	Disables trap for sending system environment (fan, power, etc) information.	Config
snmp-server enable traps fru-ctrl	Enables trap for sending module, slot status information.	Config
no snmp-server enable traps fru-ctrl	Disables trap for sending module, slot status information.	Config
snmp-server enable traps interface	Enables trap for sending interface information.	Config
no snmp-server enable traps interface	Disables trap for sending interface information.	Config
snmp-server enable traps resource [cpu- load-monitor memory-free-monitor]	Enable trap for sending system resource information.	Config
no snmp-server enable traps resource [cpu- load-monitor memory-free-monitor]	Disables trap for sending system resource information.	Config
snmp-server enable traps snmp [coldStart warmStart authFail]	Enables trap for sending Cold start, warm start, authentication failure information.	Config
no snmp-server enable traps snmp [coldStart warmStart authFail]	Disables trap for sending Cold start, warm start, authentication failure.	Config

SNMP Trap

The following example shows how to set to send trap of pan, power, and temperature information to 192.168.0.1 host.

```
Switch# configure terminal
Switch(config)# snmp-server host 192.168.0.1 public
Switch(config)# snmp-server enable traps envmon
Switch(config)# snmp-server enable traps snmp
Switch#(config)# end
Switch# show running-config
!
snmp-server enable traps interface
snmp-server enable traps envmon fan supply temperature ext-supply
snmp-server host 192.168.0.1 version 2c public
!
Switch#
```

SNMPv3 Configuration

The system provides SNMPv3 for system management. SNMPv3 provides authentication about user and encryption about data.

Table 21 Commands for Setting SNMPv3

Command	Description	Mode
snmp-server engineID <i>engineid-string</i>	Sets engine ID for dividing SNMP agent only. In the case of changing SNMP engineID, you again set the set user because user setting makes MD5 and security digest of SHA using engine ID.	Config
no snmp-server engineID	Sets Engine ID with default value made automatically. Default value is made by enterprise OID (1.3.6.1.4.1.7800) of our company and first MAC address of system.	Config
show snmp engineID	Shows Engine ID.	Privileged
snmp-server group <i>groupname</i> {v1 v2c v3 <i>sec-level</i> } [read <i>read-view</i>] write <i>write-view</i>]	Sets SNMP group. <i>group-name</i> : Group name v1, v2c, v3: Group version <i>sec-level</i> : In the case of trap version 3, sets security model. read: Read view setting. In case that you do not specify Read-view, the system sets default value with internet (1.3.6.1). write: Write view setting	Config
no snmp-server group <i>groupname</i> {v1 v2c v3 <i>sec-level</i> }	Deletes SNMP group	Config
show snmp group	Displays SNMP group	Privileged
snmp-server user <i>username</i> <i>groupname</i> {v1 v2c v3 [auth (md5 sha) <i>auth-passwd</i>] [priv (des aes) <i>priv-passwd</i>] [access <1-99>]}	Sets SNMP user v1, v2c, v3: User versions auth: In the case of SNMPv3, the system can do user authentication and you can set MD5 or SHA with a specified method of encryption. Auth-passwd: password setting for authentication. priv: You can encrypt SNMP PDU, set DES or AES with the specified method of encryption.	Config

	<i>priv-passwd</i> : Setting password for encryption. <i>access</i> : applies access-list about user. <1-99> : IP standard access list	
no snmp-server user username groupname {v1 v2c v3}	Removes SNMP user	Config
show snmp user	Shows SNMP user.	Privileged
snmp-server view viewname viewoid {excluded included}	Sets SNMP view. <i>viewoid</i> : Designates scope of MIB that can do read / write function with User or community and can designate MIB name or OID. excluded included: Sets viewoid as excluded or included.	Config
no snmp-server view viewname viewoid	Deletes SNMP view	Config

SNMP engineID

The following example shows how to change SNMP engine ID of the system. If SNMPv3 user is already set, after you change engine ID, the network manager can access as relevant user.

```
Switch# show snmp engineID
Local SNMP engineID: 0x80001f8880236ed0864b7a760f
Switch#configure terminal
Switch(config)# snmp-server engineID 0x1234567890
Switch(config)# exit
Switch#
Switch# show snmp engineID
Local SNMP engineID: 0x1234567890
Switch#
```

User of SNMPv3

The following example shows how to make 'testuser' user that does authentication and encryption. 'testgroup' includes 'testuser', it applies 'testview' that reads or writes ifEntry(1.3.6.1.2.1.2.2.1).

```
Switch# configure terminal
Switch(config)# snmp-server user testuser testgroup v3 auth md5 mysecretpass priv des myprivpass
Switch(config)# snmp-server group testgroup v3 priv read testview write testview
Switch(config)# snmp-server view testview 1.3.6.1 included
Switch(config)# snmp-server view testview 1.3.6.1.2.1.2.2.1 excluded
Switch(config)# end
Switch# show running-config
!
snmp-server group testgroup v3 priv read readview write writeview
snmp-server view testview 1.3.6.1 included
snmp-server view testview 1.3.6.1.2.1.2.2.1 excluded
!
Switch#
Switch# show snmp user

User name : testuser
```

Engine ID : 0x80001f8880236ed0864b7a760f
storage-type: nonvolatile active
Authentication Protocol: MD5
Group-name: testgroup

**Notice**

Due to the password security in SNMPv3, user settings do not show with **show running-config** command. You can make sure **show snmp user** command.

ACL (Access Control List)

ACL enables the network manager to closely control the traffic delivered through the inter-network. The manager can get basic statistical 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 access. ACL can be used to allow or reject the packets from the router, or it can be used to access the router through Telnet (vty), SSH2 or SNMP.

The access list is classified into the standard IP access list and the extended IP access list, each of which is assigned the numbers <1-99>.

Table 22 Commands for setting ACL (Access Control List)

Command	Description	Mode
access-list <1-99> {deny permit} address	Set up the standard IP access list Set up the Source address/network only <i>address ::= {any A.B.C.D A.B.C.D host A.B.C.D}</i>	Config
no access-list <1-99>	Delete the access list	Config

Rules for ACL Creation

- Declare the access list with a smaller range first.
- Declare an 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 newly added conditions will be added as the last line(s).

Configuration of Standard IP Access List

Permit any access

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

Deny any access

```
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 Access List for Telnet Connection

Access list is applied by user and the configured access list can be set to permit/limit from remote access. The commands shown below are used to configure access list for Telnet connection.

The following example shows the procedure in the case of creating access list allowing 192.168.0.0/24 network to access the switch and limiting the Telnet access:

```
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#
```

Banner Configuration

U9016B can register login banner and MOTD banner. Login banner is message displayed before user log in the system, MOTD banner is message displayed after logging in the system. You can send message like cautions to user via banner.

Table 23 Command for Login Banner and MOTD Banner

Command	Description	Mode
banner login <i>banner-string</i> banner login default	Registers login banner. <i>banner-string</i> : login banner message default: default setting banner	Config
no banner login	Deletes login banner.	Config
banner motd <i>banner-string</i> banner motd default	Registers MOTD banner. <i>banner-string</i> : MOTD banner message default: default MOTD banner message	Config
no banner motd	Deletes MOTD banner.	Config

The system is basically registered as follows:

L3 Switch	<- Login Banner
Switch login: root	
Password:	
Hello.	<- MOTD Banner
Switch >enable	
Switch #	

The following example shows how to change logging in banner. The banner can enter several lines.

The banner message is registered while the same end-character appears with start-character.

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# banner login . 
```

U9016B

Login Banner TEST!

```
!
Switch(config)#
Switch(config)#exit
Switch#show running-config
!
banner login ^C
```

U9016B

Login Banner TEST!

```
^C
!
```



Notice

When you make set the banner with the '**show running-config**' command, make sure the start and end characters are '**^C**'

The following example shows the login banner when logging in:

```
U9016B
Login Banner TEST!
Switch login: root
Password:
Hello.
Switch >
```

AFSMGR (Alarm Fault Status Manager)

AFS manager provides the log masking, report masking, fault class setting and management about Alarm, Status, and fault message in SNMP trap event occurring from system. Moreover it provides a search about faults currently occurring and a past history.

Setting AFS Alarm

Table 24 Commands for Setting AFS

Command	Description	Mode
<code>afs current clear [alarm-index]</code>	Clears alarm that does not clear in the AFS event. <i>alarm-index</i> : index <1-99999>	Config
<code>afs history clear</code>	removes the history of AFS event	Config
<code>afs mask enable/disable [afs-type [event-type [afs-id]]]</code>	Enables or disables the masking function about AFS event. If masking is enabled, the event does not occur. <i>afs-type</i> : type of message (alarm, fault, status) <i>event-type</i> : type of event (communications, environment, equipment, processing, protocol, qos, security) <i>afs-id</i> : A01001, S01001, F01001,...	Config
<code>afs severity critical major minor afs-id</code>	Changes class about AFS event. <i>afs-id</i> : A01001, S01001, F01001,...	Config
<code>afs snmp enable/disable [afs-type [event-type [afs-id]]]</code>	Enables or disables snmp trap reporting about AFS event. If SNMP trap reporting enable, the SNMP trap does not occur. <i>afs-type</i> : type of message (alarm, fault, status) <i>event-type</i> : type of event (communications, environment, equipment, processing, protocol, qos, security) <i>afs-id</i> : A01001, S01001, F01001,...	Config
<code>afs factory-default running-config [mask snmp]</code>	Changes the mask set to current afs running-config and snmp value with default-config. <i>mask</i> : changes mask configuration only <i>snm</i> : changes snmp configuration only	

Clear AFS Alarm Event

You can forcibly clear the Alarm when the error is not clear while there is an AFS Event.

Switch# **show afs current**

no	id	type	level	date
3	A04003	processing	major	2006-09-07 10:43:59

Switch# **show afs current 3**

Probable Cause	MEMORY OVERLOAD ALARM
ID	A04003
Type	processing
Level	major
Date	2006-09-07 10:43:59
Physical Location	sys<1>
Logical Location	
Additional Text	vlaue<45> thres<50>

Switch# **configure terminal**

Switch(config)# **afs current clear**

Switch# **show afs current**

no	id	type	level	date
----	----	------	-------	------

Switch#

Clearing AFS history

You can clear AFS history. The following example shows how to clear AFS history:

Switch# **show afs history**

2006-08-06 09:21:22	A04002	processing	maj on	sys<1> vlaue<4> thres<1>
2006-08-06 09:21:22	A04001	processing	maj on	sys<1> vlaue<4> thres<3>
2006-08-06 09:21:22	A04003	processing	maj on	sys<1> vlaue<49> thres<50>
2006-08-06 09:21:23	A01002	equipment	maj off	sys<1>

Switch# **configure terminal**

Switch(config)# **afs history clear**

Switch# **show afs history**

start history

Switch#

Setting AFS Masking Function

In an AFS event, you can set AFS masking about a specific event. Before the event set masking clears any masking, no message occurs.

Switch# **show afs running-config**

ID	Type	Level	Mask	Snmp	Desc
A01001	equipment	critical	disable	enable	system cold start alarm
A01002	equipment	major	disable	enable	system warm start alarm

Switch# **configure terminal**

Switch(config)# **afs mask enable alarm**

Switch(config)# **afs mask enable status equipment**

Switch(config)# **afs mask enable fault qos F03023**

Switch(config)# **end**

Switch# **show running-config**

!

afs snmp enable alarm equipment A01001

afs snmp enable alarm equipment A01002

afs snmp enable status equipment S01003

afs snmp enable status equipment S01006

afs snmp enable fault qos F03023

!

Switch# **show afs running-config**

ID	Type	Level	Mask	Snmp	Desc
A01001	equipment	critical	enable	enable	system cold start alarm
A01002	equipment	major	disable	enable	system warm start alarm

Switch#



Notice

Default value is disabled in masking setting and follows setting value of default-config.
The default value of some message (S02009, S06002, and F02003) is enabled.

Setting AFS Severity Class

In the middle of an AFS event you can change the alarm level of the event.

Switch# **show afs running-config**

ID	Type	Level	Mask	Snmp	Desc
A01001	equipment	critical	disable	enable	system cold start alarm
A01002	equipment	major	disable	enable	system warm start alarm

Switch# **configure terminal**

Switch(config)# **afs severity major A01001**

Switch(config)# **end**

Switch# **show running-config**

!

afs severity major A01001

!

Switch# **show afs running-config**

ID	Type	Level	Mask	Snmp	Desc
A01001	equipment	major	disable	enable	system cold start alarm
A01002	equipment	major	disable	enable	system warm start alarm

Switch#



Notice

Error class obeys the set value of AFS default-config.

Setting AFS SNMP Trap

You can set SNMP Trap about AFS event. Moreover, you can set All for AFS events or else for each event accordingly.

Switch# **show afs running-config**

ID	Type	Level	Mask	Snmp	Desc
A01001	equipment	critical	disable	enable	system cold start alarm
A01002	equipment	major	disable	enable	system warm start alarm
S01003	equipment	warning	disable	enable	slot status change
S01006	equipment	warning	disable	enable	SFP status change
F03023	QoS	warning	disable	enable	crc count threshold alarm

Switch# **configure terminal**

Switch(config)# **afs snmp disable alarm**

Switch(config)# **afs snmp disable status equipment**

Switch(config)# **afs snmp disable fault qos F03023**

Switch(config)# **end**

Switch# **show running-config**

afs snmp disable alarm equipment A01001

afs snmp disable alarm equipment A01002

afs snmp disable status equipment S01003

afs snmp disable status equipment S01006

afs snmp disable fault qos F03023

Switch# **show afs running-config**

ID	Type	Level	Mask	Snmp	Desc
A01001	equipment	critical	disable	disable	system cold start alarm
A01002	equipment	major	disable	disable	system warm start alarm
S01003	equipment	warning	disable	disable	slot status change
S01006	equipment	warning	disable	disable	SFP status change
F03023	QoS	warning	disable	disable	crc count threshold alarm

Switch#



Notice

The default snmp trap setting is disabled. It obeys AFS default-config value.

Changing AFS Configuration with default-config

You can change afs mask and snmp setting value when running to that of the current system. You can also change the mask or snmp as required.

```
Switch# show afs default-config
```

ID	Type	Level	Mask	Snmp	Desc
A01001	equipment	critical	disable	disable	system cold start alarm
A01002	equipment	major	disable	disable	system warm start alarm
A01006	equipment	major	disable	disable	power alarm
A01007	equipment	critical	disable	disable	fan alarm
A01014	equipment	critical	disable	disable	olt alarm
A02004	communication	major	disable	disable	onu ld shutdown
A02005	communication	critical	disable	disable	olt dying gasp alarm
A02006	communication	critical	disable	disable	olt link fault alarm

```
Switch# show afs running-config
```

ID	Type	Level	Mask	Snmp	Desc
A01001	equipment	critical	disable	disable	system cold start alarm
A01002	equipment	major	enable	enable	system warm start alarm
A01006	equipment	major	enable	disable	power alarm
A01007	equipment	critical	enable	enable	fan alarm
A01014	equipment	critical	disable	disable	olt alarm
A02004	communication	major	disable	disable	onu ld shutdown
A02005	communication	critical	disable	disable	olt dying gasp alarm
A02006	communication	critical	disable	disable	olt link fault alarm

```
Switch# configure terminal
```

```
Switch(config)# afs factory-default running-config
```

```
Switch(config)# end
```

```
Switch# show afs running-config
```

ID	Type	Level	Mask	Snmp	Desc
A01001	equipment	critical	disable	disable	system cold start alarm
A01002	equipment	major	disable	disable	system warm start alarm
A01006	equipment	major	disable	disable	power alarm
A01007	equipment	critical	disable	disable	fan alarm
A01014	equipment	critical	disable	disable	olt alarm
A02004	communication	major	disable	disable	onu ld shutdown
A02005	communication	critical	disable	disable	olt dying gasp alarm
A02006	communication	critical	disable	disable	olt link fault alarm

Chapter 2. Interface

This chapter describes the system interface.

Overview

The interfaces supported in U9016B are as follows:

Table 25 Interfaces Supported in U9016B

Interface	Type
Physical interfaces	Gigabit Ethernet 1000Base-T 1000Base-X GE-PON Interface GPON Interface 2.5G 10 Gigabit Ethernet 10G Base-R
port-group interfaces	Port-group
VLAN Interfaces	VLAN
Loopback interface	Loopback
Management interface	Out of band interface for management

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

- Enter the config mode from the privileged mode using “configure terminal” command.
- Enter into the interface mode using “interface” command.
- Use the configuration commands for a particular interface.

Common Commands

The commands commonly used in interface configuration are as follows:

Table 26 Common Commands

Command	Description
interface <i>IFNAME</i>	Enters into the interface. <i>IFNAME</i> : Name of the specific interface for configuration.
description <i>string</i>	Registers a description for the interface. <i>string</i> : The description of the interface within a length of 80 characters maximum
no description	Deletes the description of the registered interface.

Interface name

U9016B uses an interface name in all interface configurations. The interface name consists of an interface type identifier and an interface ID as shown below:

Table 27 Interface Name

Interface	Interface type	Interface name	Example
Physical interface	Gigabit Ethernet 10 Gigabit Ethernet Gpon interface EPON Interface	"Gi" + slot_id + port_id "Te" + slot_id + port_id "Gp" + slot_id + port_id "Ep" + slot_id + port_id	Gi1/1 Te1/1 Gp1/1 Ep1/1
Port-group interface	Port group	"po" + port-group id	po1
VLAN interface	VLAN	"VLAN" + VLAN id	Vlan10
Loopback interface	Loopback	"lo" + id	Loopback0
Management interface	Fast Ethernet	"eth" + id	eth0

Interface ID

Interface name consists of interface type and id. The following shows the naming of U9016B interface and range supported.

Table 28 Interface ID and Range Supported

Model	Interface Type	ID	ID Range	Name
U9016B	Gigabit Ethernet	slot_id + port_id	slot_id: 1-12 port_id: 1-8	Gi1/1
	10 Gigabit Ethernet	slot_id + port_id	slot_id: 1-12 port_id: 1-8	Te1/1
	Gpon Interface	slot_id + port_id	slot_id: 1-12 port_id: 1-8	Gp1/1
	Port group	port-group id	1 – 256	po1, po30
	VLAN	VLAN id	1 – 4094	Vlan1
	LoopBack	interface id	0 – 3	Loopback0
	management	interface id	0	eth0

Interface mode prompt

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

Switch (config-if-Giga5/1)#

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 the “show interface” command.

Show Interface Information

The following commands are used to view the interface configuration information, the status information, and the statistical data:

Table 29 Interface information and status related commands

Command	Description	Mode
show interface <i>IFNAME</i>	Shows the configuration, status, and statistics information of the interface.	Privileged
show interface status	Shows the link status, speed, duplex information of the physical interface.	Privileged
show interface transceiver [detail]	Shows DDM (Digital Diagnostic Monitoring) information of the physical interface.	Privileged
show idprom all show idprom <i>fru-type</i> show idprom interface <i>IFNAME</i>	Shows system FRU information. all: Shows all the FRU type information <i>fru-type</i> : Shows the information of each FRU type interface <i>IFNAME</i> : Shows the interface information	Privileged

Show Interface Command

Show interface command is used to view the interface configuration information, the link status, and the interface-related statistics. Show interface command shows the information on all the interfaces defined.

Switch# **show interface**

```
Giga5/1 is down, line protocol is down (notconnect)
Hardware is Ethernet, address is 0007.7074.ff01 (bia 0007.7074.ff01)
index 1101 metric 1 mtu 1500 arp ageing timeout 7200
Full-duplex, Auto-speed, media type is 1000BaseLX
<UP,BROADCAST,MULTICAST>
VRF Binding: Not bound
Bandwidth 1g
inet 10.2.1.1/16 broadcast 10.2.255.255
VRRP Master of : VRRP is not configured on this interface.
Last clearing of "show interface" counters never
60 seconds input rate 0 bits/sec, 0 packets/sec
60 seconds output rate 0 bits/sec, 0 packets/sec
L2/L3 in Switched: ucast 0 pkt - mcast 0 pkt
L2/L3 out Switched: ucast 0 pkt - mcast 0 pkt
0 packets input, 0 bytes
Received 0 broadcast pkt (0 multicast pkt)
0 CRC, 0 oversized, 0 dropped
0 packets output, 0 bytes
0 collisions
0 late collisions, 0 deferred
```

-- More--

Show Interface 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 interface status

Port	Name	Status	VLAN	Duplex	Speed	Type
Gp1/1		notconnect	1	full	auto	No Transceiver
Gp1/2		notconnect	1	full	auto	No Transceiver
Gp1/3		notconnect	1	full	auto	No Transceiver
Gp1/4		notconnect	1	full	auto	No Transceiver
Gp1/5		notconnect	1	full	auto	No Transceiver
Gp1/6		notconnect	1	full	auto	No Transceiver
Gp1/7		notconnect	1	full	auto	No Transceiver
Gp1/8		notconnect	1	full	auto	No Transceiver
Gi5/1		notconnect	700	full	auto	10/100/1000BaseT
Gi5/2		notconnect	700	full	auto	10/100/1000BaseT
Gi5/3		connected	100	full	a-1000	10/100/1000BaseT
Gi5/4		connected	100	full	a-1000	10/100/1000BaseT
Gi5/5		connected	200	full	a-1000	10/100/1000BaseT
Gi5/6		connected	200	full	a-1000	10/100/1000BaseT
Gi5/7		notconnect	700	full	auto	10/100/1000BaseT
Gi5/8		notconnect	700	full	auto	10/100/1000BaseT
Gi10/1		connected	100	full	a-1000	1000BaseLX
Gi10/2		connected	200	full	a-1000	1000BaseLX
Gi10/3		notconnect	1	full	auto	No Transceiver
Gi10/4		notconnect	1	full	auto	No Transceiver
Gi10/5		notconnect	1	full	auto	No Transceiver
Gi10/6		notconnect	1	full	auto	No Transceiver
Gi10/7		notconnect	1	full	auto	No Transceiver
Gi10/8		notconnect	1	full	auto	No Transceiver

Show idprom Command

show idprom command shows FRU (Field Replaceable Unit) information of the system. U9016B can show the information for the below FRU types.

- Chassis
- FAN
- FMU
- Module
- SCU
- PMU
- Power
- Slot
- Tranceiver

The following is an example of showing all the FRU type of systems that use show idprom all.

```
Switch# show idprom all
IDPROM for chassis
  Name = 'UbiQuoss Evolution'
  Description = 'UbiQuoss Chassis System'
  SNMP index = '1'

IDPROM for scu 1
  Name = 'Physical Module SCU 1'
  Description = 'UbiQuoss Physical Module SCU 1'
  SNMP index = '2'

IDPROM for slot 1
  Name = 'Physical Slot 1'
  Description = 'UbiQuoss Physical Slot 1'
  SNMP index = '10'

IDPROM for slot 5
  Name = 'Physical Slot 1'
  Description = 'UbiQuoss Physical Slot 1'
  SNMP index = '14'

IDPROM for slot 10
  Name = 'Physical Slot 1'
  Description = 'UbiQuoss Physical Slot 1'
  SNMP index = '19'
```

... Omitted intentionally ...

Physical Port Configuration

The following commands are used for the configuration of physical ports:

Table 30 Physical port configuration commands

Command	Description	Mode
shutdown no shutdown	Disables/enables the physical port	Interface
speed {10 100 1000} speed auto	Speed setting (Unit: Mbps)	Interface
duplex {full half}	Duplex mode setting	Interface
flowcontrol (send receive) (on off) flowcontrol both no flowcontrol	flow-control On and Off	Interface
carrier-delay <0-60> carrier-delay msec <0-1000>	Sets Carrier-delay in second unit or in ms unit	Interface



Notice

These commands are not shown in GPON interface.

Shutdown

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

```
Switch # configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch (config)# interface GigabitEthernet 5/1
Switch (config-if-Giga5/1)# shutdown          <- disable port
Switch (config-if-Giga5/1)# no shutdown        <- enable port
Switch (config-if-Giga5/1)#
```

Speed and Duplex

The speed options supported in each interface of U9016B are as follows:

Table 31 Speed and Duplex

Type	speed	duplex
1000Base-T	10/100/1000/auto	full/half
	1000	full
1000Base-X	1000/auto	full
	1000	full
10GBase-R	10000	full

When configuring speed or duplex, note the following:

- 10-Gigabit Ethernet and Gigabit Ethernet support full duplex only.

Flow control

U9016B supports IEEE 802.3x Flow control for Gigabit Ethernet, 10-Gigabitethernet interfaces. Flow control is the function not to send any packet for specific time duration by sending IEEE 802.3x pause frame to the other interface when the receive buffer of any interface is full.

The following example shows how to send IEEE 802.3x pause frame to an interface and how to receive and process it in the interface.

```
Switch# configure terminal
Switch(config)#
Switch(config)# interface Giga5/1
Switch(config-if-Giga5/1)# flowcontrol send on
Switch(config-if-Giga5/1)# flowcontrol receive on
Switch(config-if-Giga5/1)# end
Switch# show flowcontrol
```

Port	Send FlowControl admin	oper	Receive FlowControl admin	oper	RxPause	TxPause
Giga1/1/1	on	on	on	off	307	154

```
Switch#
```

Flowcontrol send on is the command to set to send IEEE 802.3x pause frames, while flowcontrol receive on is the command to set not to send packets for specific time period upon reception of IEEE 802.3x pause frames. Use the show flowcontrol (IFNAME) command to check those setting. To disable the settings, use no flowcontrol command.

Carrier delay

When there is any link up/down event occurred in an Interface, it's possible to set not to detect it as down if the link status changes up -> down -> up within the period of time shorter than the time set by carrier delay.

```
Switch# configure terminal
Switch(config)#
Switch(config)# interface Giga5/1
Switch(config-if-Giga5/1)# carrier-delay msec 500
Switch(config-if-Giga5/1)# end
Switch#
```

To disable this setting, use **no carrier-delay** command.

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 32 Broadcast Suppression

Command	Description	Mode
storm-control (broadcast/multicast/unicast)	Suppression of Multicast, broadcast, unicast, packet	Interface
storm-control level LEVEL no storm-control level	Sets broadcast suppression rate	Interface

To set broadcast suppression, it's required to set the rate first. Then the setting for the traffic is required.

The following example shows a configuration of storm-control:

```
Switch # configure terminal
Switch(config)#
Switch(config)# int GigabitEthernet 5/3
Switch(config-if-Giga5/3)# storm-control level 50
Switch(config-if-Giga5/3)# storm-control broadcast
Switch(config-if-Giga5/3)# storm-control multicast
Switch# show interface counters storm-control
Port      TotalLevel % UMB UcastDiscards McastDiscards BcastDiscards
-----
.....
Gi5/1      0.00          0          0          0
Gi5/2      0.00          0          0          0
Gi5/3      50.00      **          0          0          0
Gi5/4      0.00          0          0          0
.....
Switch#
```

To disable storm-control, use the no storm-control command.

Port Mirroring

Port mirroring mirrors 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.

U9016B can monitor RX/TX traffic from different source ports with one port.

Table 33 Port Mirroring

Command	Description	Mode
mirror interface IFNAME direction (receive transmit both)	Specifies the port to mirror and I/O packets.	Interface
no mirror interface IFNAME direction (receive transmit)	Disables the port to mirror.	Interface

The following example shows a case of port mirroring:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# int GigabitEthernet 5/1
Switch(config-if-Giga5/1)# mirror interface gi5/2 direction receive
Switch(config-if-Giga5/1)# mirror interface gi5/3 direction receive
Switch(config-if-Giga5/1)# mirror interface gi5/4 direction receive
Switch(config-if-Giga5/1)# end
Switch# show mirror
Mirror Test Port Name: Giga5/1
Mirror option: Enabled
Mirror direction: receive
Monitored Port Name: Giga5/2
Mirror Test Port Name: Giga5/1
Mirror option: Enabled
Mirror direction: receive
Monitored Port Name: Giga5/3
Mirror Test Port Name: Giga5/1
Mirror option: Enabled
Mirror direction: receive
Monitored Port Name: Giga5/4
Switch#
```



Notice

Port mirroring can't work together with netflow at the same time. When Netflow is enabled, employ the no mls netflow command in config mode to use port mirroring.

Layer 2 Interface Configuration

Layer 2 is an interface that works in the Layer 2 switching mode (IEEE 802.3 Bridged VLAN). In U9016B, the physical port and the port-group interface works in the Layer 2 switching mode.

This section describes the Layer 2 interface and the commands to set the physical port and the port-group as Layer 2 interface with examples.

VLAN Trunking

Trunk refers to the point-to-point link between the 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 using trunks.

U9016B 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 mode

Layer 2 interface modes supported by U9016B are the trunk mode and the access mode.

Table 34 Layer 2 Interface mode supported in U9016B

Mode	Description
switchport mode access	Non trunking mode. Only native VLAN can be configured
switchport mode hybrid	Single native VLAN and multiple tagged, untagged VLAN can be configured
switchport mode trunk	Trunking mode. Single native VLAN and multiple tagged VLAN can be configured

Layer 2 Interface Defaults

U9016B has the following default values when a physical port or a port-group is set as Layer 2 interface:

Table 35 Layer 2 Interface Defaults

Item	Default
interface mode	switchport mode access
native VLAN	VLAN 1

Enabling/disabling Layer 2 Interface

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

Table 36 Commands to enable/disable Layer 2 interface configuration

Command	Description	Mode
switchport	Enables Layer2 interface	interface
no switchport	Disables Layer2 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, but if Layer 2 interface is enabled by switchport command, the previous configurations are recovered.



Notice

All the physical ports of U9016B are configured as Layer 2 interface by default.

Trunk Port Setting

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

Table 37 Commands for Trunk port configuration

Command	Description	Mode
switchport mode trunk	Configures trunk mode	Interface
switchport trunk native <1-4094>	Configures trunk port native VLAN	Interface
no switchport trunk native	Sets trunk port native VLAN to default	Interface
switchport trunk allowed VLAN add <2-4094>	Registers a trunk port tagged VLAN	Interface
switchport trunk remove <2-4094> switchport trunk remove all	Removes a trunk port tagged VLAN	Interface

The following example shows how to set a physical port as a Layer 2 trunk port:

```
Switch# configure terminal
Switch(config)# interface gi1/1
Switch(config-if-gi1/1)# switchport          ! layer2 interface set
Switch(config-if-gi1/1)# switchport mode trunk    ! trunk port set
Switch(config-if-gi1/1)# switchport trunk native 2    ! native VLAN set
Switch(config-if-gi1/1)# switchport trunk allowed vlan add 3    ! tagged VLAN reg.
Switch(config-if-gi1/1)# switchport trunk allowed vlan add 4
Switch(config-if-gi1/1)# end
```

The following example shows how to set a port-group interface as a Layer 2 trunk 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 allowed add 3    ! tagged VLAN reg.
Switch(config-if-po2)# switchport trunk allowed add 4
Switch(config-if-po2)# end
```

Access Port Setting

The commands to set a physical port or a port-group interface as a Layer 2 access port:

Table 38 Access port configuration commands

Command	Description	Mode
switchport mode access	Sets to access mode	Interface
switchport access VLAN <1-4094>	Sets native VLAN	Interface
no switchport access VLAN	Sets native VLAN to default (VLAN 1)	Interface

The following example shows how to configure a physical port as a Layer 2 access port:

```
Switch# configure terminal
Switch(config)# interface gi1/1
Switch(config-if-gi1/1)# switchport          ! layer2 interface set
```

```
Switch(config-if-gi1/1)# switchport mode access      ! access port set
Switch(config-if-gi1/1)# switchport access VLAN 5    ! native VLAN set
```

The following example shows how to configure 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
```



Notice

For more detailed information on VLAN configuration, refer to the VLAN manual.

Port group

Overview of Port Group

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 U9016B can be used as Layer 2 interface.

The following table shows the number of port groups available in U9016B by model:

Table 39 Overview of Port Group

Model	Number of port groups	Max. no of ports per group
U9016B	256	8

Port group configuration

The commands for configuring Port group are as follows:

Table 40 Port Group Configuration Commands

Command	Description	Mode
Channel-group <1-256> mode on	Includes the interface in the port group, and creates a port group interface.	interface
no port-group ifname	Deletes the port-group	config
port-channel load-balance src-dst-mac	Refers to MAC address for load-balance.	config
port-channel load-balance src-dst-ip	Refers to ip field for load-balance.	config
port-channel load-balance src-dst-port	Refers to tcp/udp port for load-balance	config
no channel group	Excludes the interface from the port group.	Interface *
no interface Channel-group <1-256>	Deletes the port group interface. Used when there is no member in the Port group.	config
show etherchannel	Shows port group configuration	Privileged



Notice

For more detailed description on the port group, refer to the LACP manual.

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 Introduction

VLAN (Virtual LAN) is an 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, and prevents traffic from flowing into other VLANs; it transmits traffic only to the same VLAN equipment to improve 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 the physical movement or arrangement of equipment or a cable.

VLAN is used to provide a 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

VLAN has 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 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 thus 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 administrators of 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

U9016B supports up to 4094 VLANs and creates VLANs according to the following criteria:

- Physical port
- 802.1Q tag
- Hybrid type (Combination of the port-based VLAN and Tag-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. In other words, all ports are assigned as the access ports of VLAN 1 (default VLAN).

For example, U9016B assigns 2 ports to each VLAN A and VLAN B, and 2 ports to VLAN C.

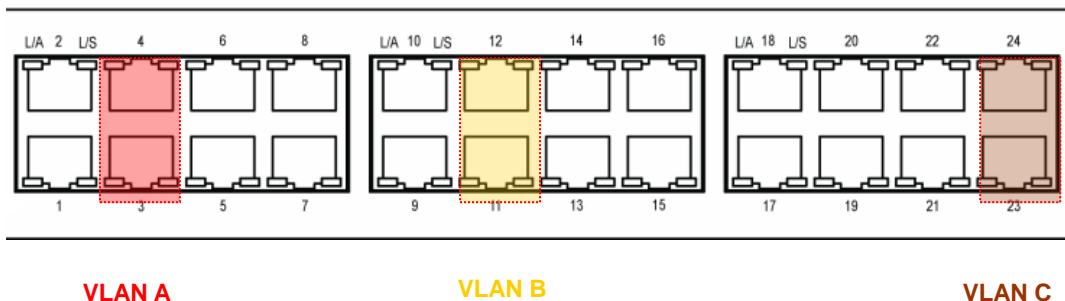


Figure 2. Example of a Port-based VLAN Configuration (U9016B)

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

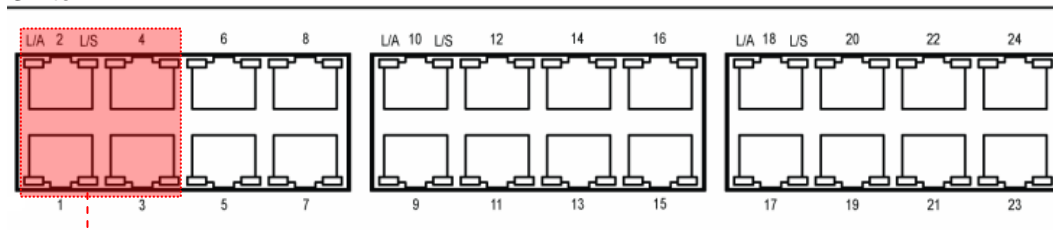
Connecting Switches with a Port-Based VLAN

To connect two switches with a port-based VLAN, do the following tasks:

1. Assign the 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 figure below illustrates how to bind two systems into one VLAN. First, two ports of the switch 1 are assigned to VLAN A, and two ports of the switch 2 are assigned to an access port of VLAN A. Two switches are connected each other and form single broadcast domain like the following figure.

Switch 1



Switch 2

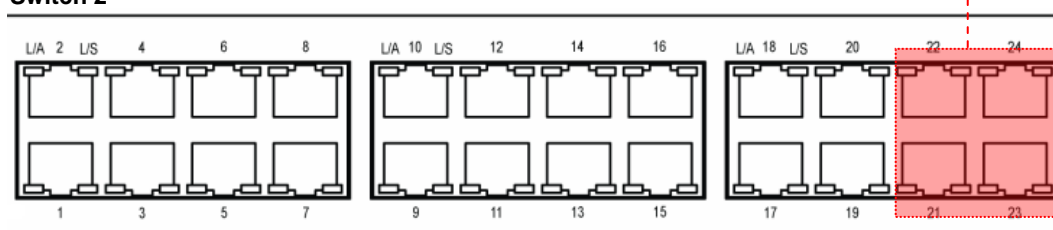
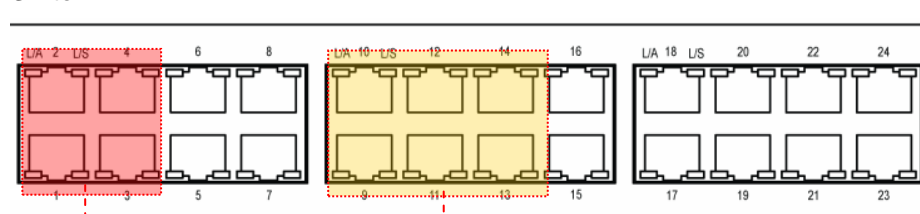


Figure 3. Single Port-based VLANs Connecting 2 Switches

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 system must be assigned as the access port of the corresponding VLANs. The following figure illustrates two VLANs spanning two systems. Port 1~4 in a switch 1 is an access port of VLAN A, and Port 9~14 are assigned as an access port of VLAN B. Port 1~4 in a switch 2 are an access port of VLAN A, and Port 9~14 are assigned as an access port of VLAN B.

Switch 1



Switch 2

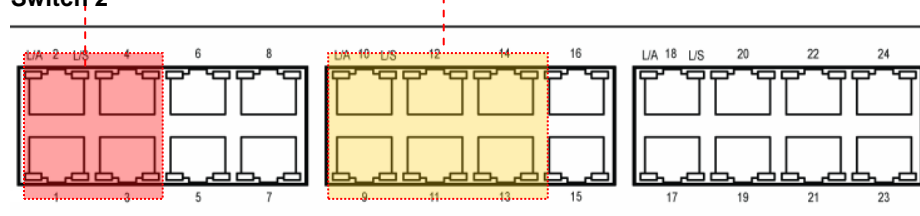


Figure 4. Two Port-based VLANs Connecting 2 Switches

VLAN A binds switch 1 and switch 2 as a connection between port 2 of switch 1 and port 1 of 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 a *trunk*. A trunk can transmit many VLANs traffic and extends VLANs from one switch to another switch. A port that is a member of a tagged VLAN and that sends and receives tagged frames is called the *trunk port*. Using tags, several VLANs can send and receive frames by using one or more trunks.

As previous figure describes, in a port-based VLAN, a pair of ports must be assigned in each VLAN to connect two switches. 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 figure below illustrates the physical configuration of a network using tagged frames and untagged frames:

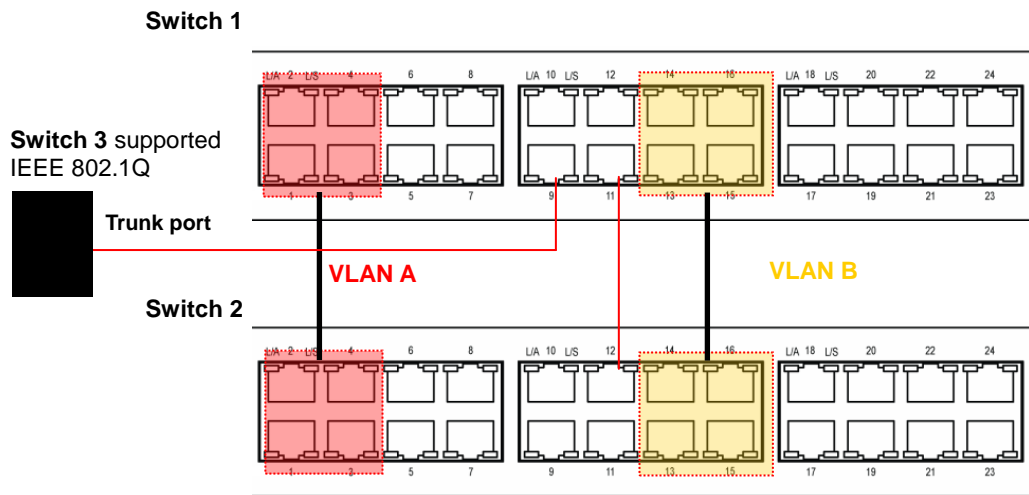


Figure 5. Physical Diagram of Tagged and Untagged Frame

Switch 3

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

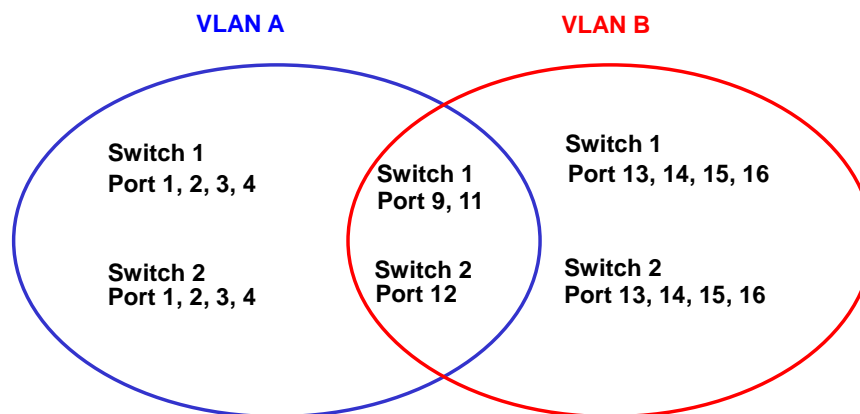


Figure 6. Logical Diagram of Tagged Frame and Untagged frame

- In previous figures, the trunk port (tagged port) of each switch transmits the traffic for both VLAN *a* and VLAN *b*.
- The trunk port of each switch transmits the frame tagged.
- The server connected to port 17 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.

Hybrid VLAN (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 Configuration

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.

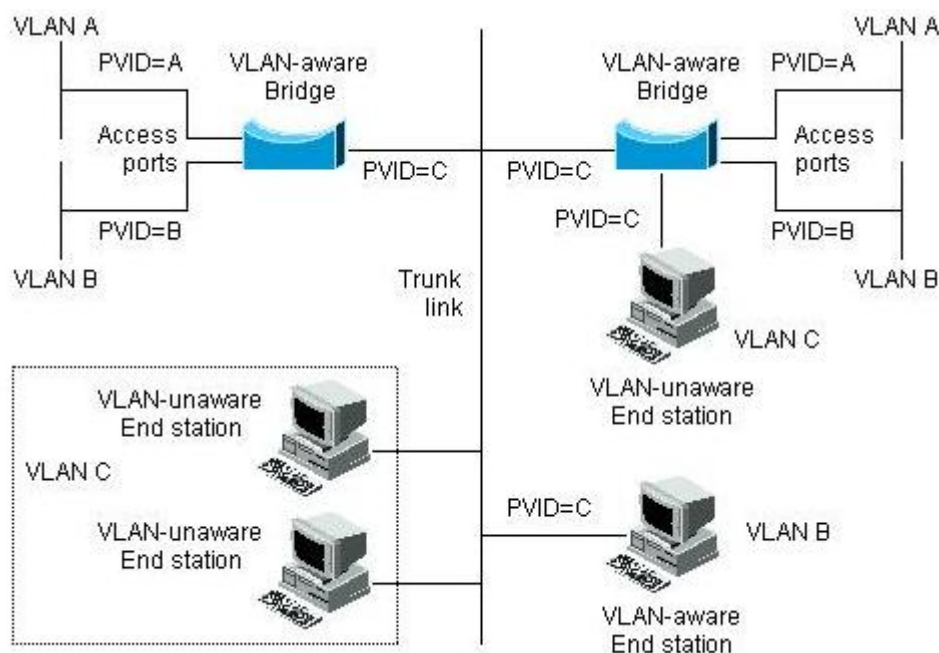


Figure 7. Native VLAN

For example, assume that two end stations not supporting VLAN are connected through the trunk link as shown in the left bottom of above figure. 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 only transmit untagged frames, and when a bridge that recognizes VLAN receives these untagged frames, it sends them to VLAN *c*.

VLAN Setting

This section describes the commands used for VLAN configuration on U9016B. VLAN configuration has the following steps.

1. Create and name the VLAN.
2. Set the mode of the port according to the type of the VLAN where the port will be assigned
3. 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 is the commands used for VLAN configuration:

Table 41 Commands for VLAN Configuration

Commands	Description	Mode
VLAN database	Access to the VLAN database mode	config
VLAN <i>vlanid</i>	Creates VLAN as a value of <i>vlanid</i> Default VLAN (VLANid=1) name cannot be changed. <i>vlanid</i> : The unique VLAN identifier, a number between 2-4094	VLAN database
VLAN <i>vlanid</i> name WORD (state (enable disable))	Creates VLAN as a value of <i>vlanid</i> WORD: VLAN ascii value	VLAN database
VLAN <i>vlanid</i> bridge <1-256> name WORD (state (enable disable))	Creates VLAN as a value of <i>vlanid</i> WORD: VLAN ascii value Creates valn to bridge.	
switchport	Changes type of port as L2. If it changes to L2 port, it becomes a member of VLAN to access mode.	Interface
switchport mode {access hybrid trunk}	Set the type of VLAN on the corresponding port. <i>access</i> : Set the port as an access mode (Port-based VLAN). It works as an interface of a single VLAN that sends and receives untagged frames. <i>hybrid</i> : Set the port as a hybrid mode <i>trunk</i> :Set the port as a trunk mode (Tagged-VLAN). The port sends and receives tagged frame. In the case of untagged frame, it regards as native VLAN ID.	Interface
switchport access VLAN <i>vlanid</i>	Set the port as VLAN access port. When the access mode is set, the port works as a member of the VLAN. <i>Vlanid</i> : VLANid, a number between 2 and 4094	Interface
Switchport hybrid VLAN <i>vlanid</i>	Sets VLAN member port.In case that the received frame is untagged, set relevant frame as VLAN id. <i>Vlanid</i> : 2-4094	Interface
switchport trunk allowed VLAN (add all except) <i>vlanid</i>	Sets port as trunk port of VLAN. <i>Vlanid</i> : 2-4094	Interface

switchport trunk native <i>vlanid</i>	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. If a native VLAN is not set, the default VLAN (VLANid = 1) is set as the native VLAN. <i>vlanid</i> : a number between 2 and 4094	Interface
switchport trunk (remove none) <i>vlanid</i>	Exclude the port from the members of the specified VLAN. <i>vlanid</i> : a number between 2 and 4094. <i>none</i> : Exclude from all VLAN members.	Interface

Examples of VLAN Configuration

The following example shows how to configure VLAN whose VLAN id is 1000, assign the IP address 132.15.121.1 to VLAN, and assign the VLAN into two ports:

```
shu#
shu#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
shu(config)#VLAN database
shu(config-VLAN)#VLAN 1000
shu(config-VLAN)#exit
shu(config)#interface VLAN 1000
shu(config-if-Vlan1000)#ip address 132.15.121.1/24
shu(config-if-Vlan1000)#interface GigabitEthernet 6/1
shu(config-if-Giga6/1)#switchport
shu(config-if-Giga6/1)#switchport mode access
shu(config-if-Giga6/1)#switchport access VLAN 1000
shu(config-if-Giga6/1)#interface GigabitEthernet 6/3
shu(config-if-Giga6/3)#switchport
shu(config-if-Giga6/3)#switchport mode access
shu(config-if-Giga6/3)#switchport access VLAN 1000
shu(config-if-Giga6/3)#end
shu#show VLAN
```

VLAN Name	Status	Ports
1 default	active	Gi6/2
2 VLAN0002	active	
3 VLAN0003	active	
4 VLAN0004	active	
5 VLAN0005	active	
6 VLAN0006	active	
7 VLAN0007	active	
8 VLAN0008	active	
9 VLAN0009	active	
10 VLAN0010	active	
11 VLAN0011	active	
12 VLAN0012	active	
100 VLAN0100	active	
1000 VLAN1000	active	Gi6/1 Gi6/3

```
shu#
```

The following example shows how to configure tagged VLAN and to assign trunk port. The example creates tagged VLAN which vlanid is 2000 and adds two ports as a trunk port of VLAN 2000.

```
shu#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
shu(config)#VLAN database
shu(config-VLAN)#VLAN 2000
```

```
shu(config-VLAN)#exit
shu(config)#interface GigabitEthernet 6/4
shu(config-if-Giga6/4)#switchport
shu(config-if-Giga6/4)#switchport mode trunk
shu(config-if-Giga6/4)#switchport trunk allowed VLAN add 2000
shu(config-if-Giga6/4)#interface GigabitEthernet 6/5
shu(config-if-Giga6/5)#switchport
shu(config-if-Giga6/5)#switchport mode trunk
shu(config-if-Giga6/5)#switchport trunk allowed VLAN add 2000
shu(config-if-Giga6/5)#end
shu#show VLAN all
```

Bridge	VLAN ID	Name	State	Member ports (u)-Untagged, (t)-Tagged
0	1	default	ACTIVE	Gi6/1 (u) Gi6/4 (u) Gi6/5 (u)
0	2	VLAN0002	ACTIVE	
0	3	VLAN0003	ACTIVE	
0	4	VLAN0004	ACTIVE	
0	5	VLAN0005	ACTIVE	
0	6	VLAN0006	ACTIVE	
0	7	VLAN0007	ACTIVE	
0	8	VLAN0008	ACTIVE	
0	9	VLAN0009	ACTIVE	
0	10	VLAN0010	ACTIVE	
0	11	VLAN0011	ACTIVE	
0	12	VLAN0012	ACTIVE	
0	100	VLAN0100	ACTIVE	
0	1000	VLAN1000	ACTIVE	Gi6/2 (u) Gi6/3 (u)
0	2000	VLAN2000	ACTIVE	Gi6/4 (t) Gi6/5 (t)

```
shu#
```

The following example shows how to configure hybrid VLAN (Tagged, Untagged VLAN). Two ports are set to VLAN 3000 as hybrid port and VLAN 4000 as tagged ports.

```
shu#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
shu(config)#VLAN database
shu(config-VLAN)#VLAN 3000
shu(config-VLAN)#VLAN 4000
shu(config-VLAN)#exit
shu(config)#interface GigabitEthernet 6/6
shu(config-if-Giga6/6)#switchport
shu(config-if-Giga6/6)#switchport mode hybrid
shu(config-if-Giga6/6)#switchport hybrid VLAN 3000
shu(config-if-Giga6/6)#switchport hybrid allowed VLAN add 4000 egress-tagged enable
shu(config-if-Giga6/6)#interface GigabitEthernet 6/7
shu(config-if-Giga6/7)#switchport
shu(config-if-Giga6/7)#switchport mode hybrid
shu(config-if-Giga6/7)#switchport hybrid VLAN 3000
shu(config-if-Giga6/7)#switchport hybrid allowed VLAN add 4000 egress-tagged enable
shu(config-if-Giga6/7)#end
shu#show VLAN all
```

Bridge	VLAN ID	Name	State	Member ports (u)-Untagged, (t)-Tagged
0	1	default	ACTIVE	Gi6/1 (u) Gi6/4 (u) Gi6/5 (u)
0	2	VLAN0002	ACTIVE	
0	3	VLAN0003	ACTIVE	
0	6	VLAN0006	ACTIVE	
0	7	VLAN0007	ACTIVE	
0	8	VLAN0008	ACTIVE	

0	9	VLAN0009	ACTIVE	
0	10	VLAN0010	ACTIVE	
0	11	VLAN0011	ACTIVE	
0	12	VLAN0012	ACTIVE	
0	100	VLAN0100	ACTIVE	
0	1000	VLAN1000	ACTIVE	Gi6/2 (u) Gi6/3 (u)
0	2000	VLAN2000	ACTIVE	Gi6/4 (t) Gi6/5 (t)
0	3000	VLAN3000	ACTIVE	Gi6/6 (u) Gi6/7 (u)
0	4000	VLAN4000	ACTIVE	Gi6/6 (t) Gi6/7 (t)

shu#

The following example shown in the following figure creates a *sales* VLAN whose VLAN id is 120. VLAN includes both tagged port (trunk port) and untagged port (access port). Port gi 6/1 and gi 6/2 has tags, and port gi 6/3 and gi 6/4 are untagged. If not explicitly set, ports are configured as untagged.

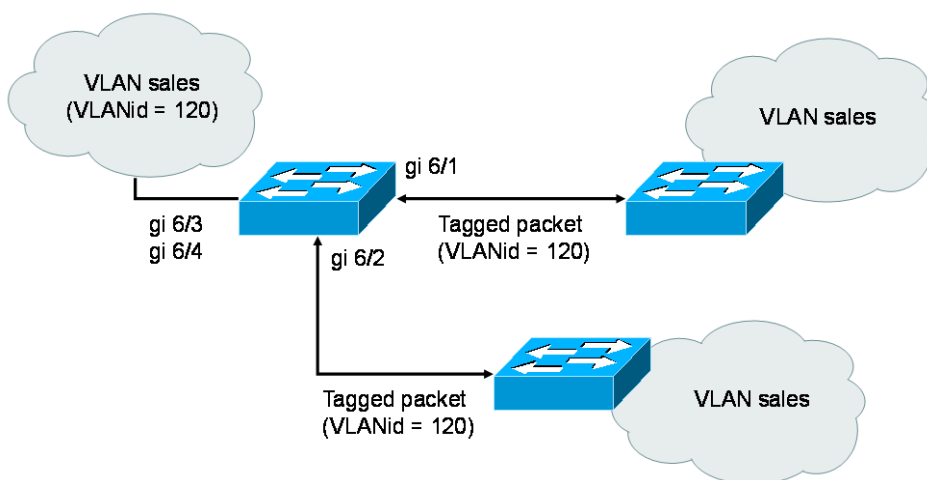


Figure 8. Configuration Example – Tagged and Untagged VLAN

```

shu#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
shu(config)#VLAN database
shu(config-VLAN)#VLAN 120
shu(config-VLAN)#exit
shu(config)#interface GigabitEthernet 6/1
shu(config-if-Giga6/1)#switchport
shu(config-if-Giga6/1)#switchport mode trunk
shu(config-if-Giga6/1)#switchport trunk allowed VLAN add 120
shu(config-if-Giga6/1)#interface GigabitEthernet 6/2
shu(config-if-Giga6/2)#switchport
shu(config-if-Giga6/2)#switchport mode trunk
shu(config-if-Giga6/2)#switchport trunk allowed VLAN add 120
shu(config-if-Giga6/2)#interface GigabitEthernet 6/3
shu(config-if-Giga6/3)#switchport
shu(config-if-Giga6/3)#switchport access VLAN 120
shu(config-if-Giga6/3)#interface GigabitEthernet 6/4
shu(config-if-Giga6/4)#switchport
shu(config-if-Giga6/4)#switchport access VLAN 120
shu(config-if-Giga6/4)#end
shu#show VLAN all

```

Bridge	VLAN ID	Name	State	Member ports (u)-Untagged, (t)-Tagged
0	1	default	ACTIVE	Gi6/1 (u) Gi6/2 (u) Gi6/5 (u)
0	120	VLAN0120	ACTIVE	Gi6/1 (t) Gi6/2 (t) Gi6/3 (u) Gi6/4 (u)

shu#

The following example shows how to configure port gi 6/1 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.

```
shu#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
shu(config)#VLAN database
shu(config-VLAN)#VLAN 200
shu(config-VLAN)#VLAN 400
shu(config-VLAN)#exit
shu(config)#interface GigabitEthernet 6/1
shu(config-if-Giga6/1)#switchport mode trunk
shu(config-if-Giga6/1)#switchport trunk allowed VLAN add 200
shu(config-if-Giga6/1)#switchport trunk native VLAN 200
shu(config-if-Giga6/1)#switchport trunk allowed VLAN add 400
shu(config-if-Giga6/1)#end
shu#show VLAN all
```

Bridge	VLAN ID	Name	State	Member ports (u)-Untagged, (t)-Tagged
0	1	default	ACTIVE	Gi6/1 (t)
0	100	VLAN0100	ACTIVE	
0	120	VLAN0120	ACTIVE	Gi6/1 (t)
0	200	VLAN0200	ACTIVE	Gi6/1 (u)
0	400	VLAN0400	ACTIVE	Gi6/1 (t)

```
shu#
```

When port gi 6/1 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:

Table 42 Displaying VLAN Settings

Command	Description	Mode
show vlans	Displays VLAN information in summary: <ul style="list-style-type: none"> VLANid Member port VLAN belonged to bridge Spanning-tree mode 	Exec
show VLAN all	Displays VLAN information as below: <ul style="list-style-type: none"> VLANid Member port tag, untagged 	Exec
show interface trunk (module <1-6>)	Displays VLAN information as below: <ul style="list-style-type: none"> Port VLAN Mode Native VLAN, Trunk VLAN 	Exec
show interface summary VLAN	Displays VLAN information as below: <ul style="list-style-type: none"> VLAN id 	Exec

The following example shows how to display the VLAN information:

```

shu#show VLAN all
Bridge          VLAN ID  Name          State  Member ports
              (u)-Untagged, (t)-Tagged
-----
0               1      default      ACTIVE  Gi6/1 (t) Gi6/2 (u)
              Gi6/5 (u)
0               2      VLAN0002      ACTIVE
0              10      VLAN0010      ACTIVE
0              11      VLAN0011      ACTIVE
0              12      VLAN0012      ACTIVE
0             100      VLAN0100      ACTIVE
0             120      VLAN0120      ACTIVE  Gi6/1 (t) Gi6/2 (t)
              Gi6/3 (u) Gi6/4 (u)
0             200      VLAN0200      ACTIVE  Gi6/1 (u)
0             400      VLAN0400      ACTIVE  Gi6/1 (t)
0            1000      VLAN1000      ACTIVE
0            2000      VLAN2000      ACTIVE  Gi6/5 (t)
0            3000      VLAN3000      ACTIVE  Gi6/6 (u) Gi6/7 (u)
0            4000      VLAN4000      ACTIVE  Gi6/6 (t) Gi6/7 (t)

```

```

shu#
shu#show VLAN

```

VLAN Name	Status	Ports
1 default	active	Gi6/1 Gi6/2 Gi6/5
120 VLAN0120	active	Gi6/1 Gi6/2 Gi6/3 Gi6/4
200 VLAN0200	active	Gi6/1
400 VLAN0400	active	Gi6/1
1000 VLAN1000	active	
2000 VLAN2000	active	Gi6/5
3000 VLAN3000	active	Gi6/6 Gi6/7
4000 VLAN4000	active	Gi6/6 Gi6/7

VLAN MTU		BridgeNo Stp Enabled		BrdgMode
1	1500	0	Yes	rstp-VLAN-bridge
120	1500	0	Yes	rstp-VLAN-bridge
200	1500	0	Yes	rstp-VLAN-bridge
400	1500	0	Yes	rstp-VLAN-bridge
1000	1500	0	Yes	rstp-VLAN-bridge
2000	1500	0	Yes	rstp-VLAN-bridge
3000	1500	0	Yes	rstp-VLAN-bridge
4000	1500	0	Yes	rstp-VLAN-bridge
shu#				

802.1 Q-in-Q

QinQ is not permitted 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. The service providing the 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.

- Service Provider Ethertype: Set up ethertype of an outer tag (default value: 0x8100).
- Service Provider VLAN ID: Use the native VLAN ID value of customer port for outer tag VLAN ID
- 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 43 802.1 QinQ Command set

Command	Description	Mode
(no) encapsulation q-in-q	Sets QinQ to be enable / disable	Config
(no) q-in-q tunneling ethertype VALUE	Sets 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)	Sets the port mode. <i>default:</i> 0x8100. <i>core:</i> add outer tag as an ethertype <i>customer:</i> configure user port type	Interface



Example gi1 → gi3

DA	SA	Ether Type	Tag	Ether Type	Tag	Len/Etype	Data	FCS
		0x8101	100	0x8100	10	-	-	-

Figure 9. Configuring 802.1 Q-in-Q

The following example shows how to set Q-in-Q.

```
Switch# configure terminal
Switch(config)# VLAN 10,20,30,40,50,60,100,200
Switch(config)# interface gi1/1
Switch(config-if-gi1/1)# switchport access VLAN 100
Switch(config-if-gi1/1)# interface gi2/1
Switch(config-if-gi2/1)# switchport access VLAN 200
Switch(config-if-gi2/1)# int gi1/1
Switch(config-if-gi1/1)# switchport mode trunk
Switch(config-if-gi1/1)# switchport trunk add 10,20,30
Switch(config-if-gi1/1)# int gi2/1
Switch(config-if-gi2/1)# switchport mode trunk
Switch(config-if-gi2/1)# switchport trunk add 40,50,60
Switch(config-if-gi2/1)# int gi3/1
Switch(config-if-gi3/1)# switchport mode trunk
Switch(config-if-gi3/1)# switchport trunk add 100,200
Switch(config-if-gi3/1)# end
```

```
Switch# show switchport
U : untagged packet drop
```

IFNAME	SWMODE	N-VLAN	TAGGED-VLAN-LIST
gi1/1	trunk	100	10 20 30
gi2/1	trunk	200	40 50 60
gi3/1	trunk	1	100 200

total 12 interfaces listed

```
Switch# configure terminal
Switch(config)# encapsulation q-in-q
Switch(config)# interface gi1/1
Switch(config-if-gi1/1)# encapsulation q-in-q customer
Switch(config-if-gi1/1)# interface gi2/1
Switch(config-if-gi2/1)# encapsulation q-in-q customer
Switch(config-if-gi2/1)# interface gi3/1
Switch(config-if-gi3/1)# 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 existing in a segment (i.e. within the VLAN), but they can only communicate between permitted ports, while the communications between other ports are blocked on Layer 2. In other words, it is to make a 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 not be sent to the ports protected on L2, and all traffic should be communicated between the protected ports only through L3 equipment.

Two methods to set the uplink between private edge VLANs in U9016B:

- IFNAME

Specify the uplink using the port name (ex. gi1/1, gi2/1, po1...)

- VLANID

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

Table 44 Private Edge VLAN setting table

Command	Description	Mode
(no) private-edge-VLAN	Enable/disable Private-edge-VLAN.	Config
(no) private-edge-VLAN <i>IFNAME</i>	Enter the IFNAME to set as uplink of the private edge VLAN to specific Interface.	Interface
(no) private-edge-VLAN stp-root-port <i>VLANID</i>	Set the uplink of the private edge VLAN as root port of <i>VLANID</i> 's root at specific interface.	Interface
Show private-edge-VLAN	Retrieve Private-edge-VLAN settings.	Privileged

The ports to be protected are gi2/1 and gi3/1, and uplink is gi1/1. Traffic between the protected ports is not allowed, but only the traffic of gi1/1 is allowed.

```
Switch# configure terminal
Switch(config)# private-edge-VLAN
Switch(config)# interface gi2/1
Switch(config-if-gi2)# private-edge-VLAN gi1/1
Switch(config-if-gi2)# interface gi3/1
Switch(config-if-gi3)# private-edge-VLAN gi1/1
```

The ports to be protected are g1/1, 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 gi1/1
Switch(config-if-gi1/1)# private-edge-VLAN stp-root-port 1
Switch(config-if-gi1/1)# 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: gi1/1      po1      *po2
        -(*): Temp Member
```

Abnormal MAC Drop

To drop the packets with abnormal MAC address or trap to the CPU, use the following commands:

Table 45 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 an IP address.

The key requirement for IP configuration is to assign an IP address to the network interface. With IP address assigned, the interface is activated as a Layer 3 interface.

- U9016B 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 to be sent. Some IP addresses are reserved for some special purpose and they cannot be used for host, subnet, or network address. The following is the range of IP addresses and it shows which addresses are reserved and which addresses are available.

Table 46 Available IP Addresses

Class	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 ~ 223.255.255.254 224.255.255.0	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 official descriptions on IP address, refer to RFC1166, Internet Number.



Notice

To obtain a network number, ask your ISP (Internet Service Provider).

U9016B supports multiple IP addresses per interface. U9016B allows up to 10 IP addresses for an interface. Multiple 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 if you use 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.

To assign an IP address to a network interface, use the following commands in interface configuration mode:

Table 47 Commands for Assigning IP Address

Command	Description
<code>ip address <i>ipaddress/prefixlen</i></code>	Assigns an IP address to an interface.



Notice

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

ARP (Address Resolution Protocol)

To check the information of ARP table, use the following commands in privilege mode. You can set Static ARP and Proxy ARP.

Table 48 Commands for ARP Configuration

Commands	Description	Mode
Show arp	Shows the entries of an ARP table.	Privileged
clear arp-cache	Deletes the entries of an ARP table.	Privileged
Clear arp-cache interface IFNAME	Deletes ARP entry of the interface.	Privileged
arp <i>ip-address</i> <i>MAC</i>	Sets static ARP entry in the ARP table <i>ip-address</i> : Shows the IP address of ARP entry. <i>MAC</i> : Shows 48bit Ethernet address of ARP entry. Alias	config
no arp <i>ip-address</i>	Deletes the ARP entry of the ip address.	config
arp-ageing-timeout <1-3000>	Sets the ageing timeout of ARP entry of the interface	interface
no arp-ageing-timeout	Sets the ARP entry ageing timeout of the interface to the default value (default : 7200 sec)	interface

The following example is to show how to set a static ARP and an ARP timeout. To set ARP, there should be an interface with an IP address.

```
Switch#
shu#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
shu(config)#arp 192.168.1.3 0111.1111.1213
% Interface does not exist
shu(config)#int GigabitEthernet 6/1
shu(config-if-Giga6/1)#ip address 192.168.1.3/24
shu(config-if-Giga6/1)#exit
shu(config)#arp 192.168.1.3 0111.1111.1213
shu(config)#end
shu#show arp
Protocol Address Hardware Addr Type Interface
-----
Internet 192.168.1.3 0111.1111.1213 static Giga6/1
Internet 10.1.17.104 0022.1926.2db3 dynamic eth0
Internet 10.1.17.254 0007.7045.a36f dynamic eth0
shu#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
shu(config)#no arp 192.168.1.3
shu(config)#end
shu#show arp
Protocol Address Hardware Addr Type Interface
-----
Internet 10.1.17.254 0007.7045.a36f dynamic eth0
shu#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
shu(config)#interface GigabitEthernet 6/1
shu(config-if-Giga6/1)#arp-ageing-timeout 2000
shu(config-if-Giga6/1)#
```


Configuring 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 extremely important. It is also useful to indicate the gateway where the packets that cannot be routed will be sent. To configure a static route, use the commands below:

Table 49 Commands for configuring Static route path

Commands	Description
ip route {destination-prefix mask destination-ipaddress/mask} {gateway-ipaddress null0} [distance-value]	Registers a static route. Destination-prefix: Specifies the network number of the destination-prefix destination. Mask: Specifies the mask of the mask destination network. Gateway-IP Address: Specifies the IP address of the gateway device. Null: Sets the null interface as a gateway. Distance-value : A number between 1 and 255 is used

A system remembers the static route until it is deleted (use no format of IP route command in the global config mode). However, the static route can overlap 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 table below. If you want a static route to be overlapped with the dynamic routing protocol information, set the administrative distance of the static route to be larger than the dynamic protocol value.

Table 50 Default administrative distances of dynamic routing protocol

Item	Default
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 hops are 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.

Table 51 Showing IP route Information

Command	Description
show ip route static	Shows IP route information.

IP Configuration Example

This section provides IP configuration examples:

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

The following example shows how to assign a C class IP address, 192.10.25.1 to vlan5 interface of the switch.

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

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.

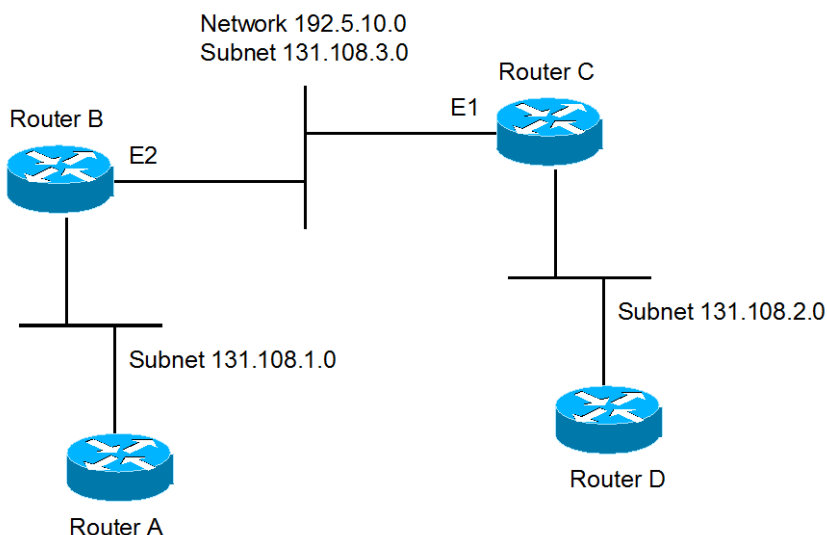


Figure 10. Network Configuration Example – multiple IP address

The following example shows how to set multiple IP configurations:

Router B configuration

```
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 configuration

```
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 is to show the contents of an ARP table:

Switch# **show arp**

IP Address	MAC Address	IPF	PORT	RefCnt	Flags
10.1.2.254	0007.7089.1123	vlan2	gi1/1	1	S
10.1.11.46	0006.2bfc.146e	vlan11	gi6/1	1	S
10.1.13.1	0001.0281.f775	vlan13	gi2/1	1	R
10.1.13.190	0000.f083.f6d4	vlan13	gi6/2	1	K

The following command is used to register a static ARP entry to an ARP table:

Switch(config)# **arp** 142.10.52.196 0010.073c.0514 vlan1 gi2/1

Switch# **show arp**

IP Address	MAC Address	IPF	PORT	RefCnt	Flags
142.10.52.196	0010.073c.0514	vlan1	gi2/1	1	P

The following command is used to delete a static ARP entry from the ARP table:

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

The following example shows how to configure a static route that allows the host connected to 20.1.1.0 network to communicate with a host in 192.168.2.0 network:

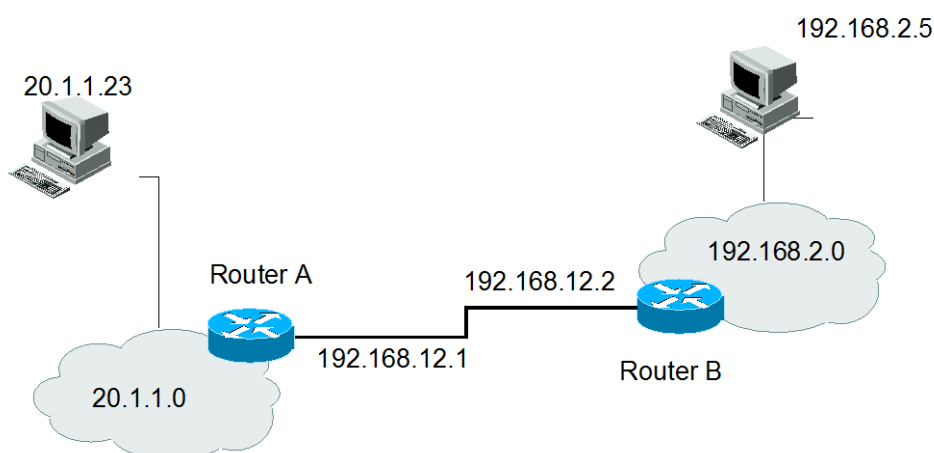


Figure 11. Network Configuration Example – Static route

Router A configuration

Switch(config)# **ip route** 192.168.2.0/24 192.168.12.2

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

Chapter 5. Utilities

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

Status dump command

Commands

“show tech-support” is used to dump the system logging messages of each module (system configuration, multicast, routing, driver, etc.).

show tech support

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.

Switch# show tech-support

--- Display the system information ---

```
MODEL-NAME      : U9016B
SERIAL-NO       :
System MAC-ADDRESS: 00:07:70:74:ff:01
```

--- Display the system version ---

```
UbiQuoss Switch Operating System Software
U9016B Software (U9016B), Version 1.1.0
Technical Support: http://www.ubiQuoss.com
Copyright © 2001-2010 by UbiQuoss Inc.
```

BOOTLDR: U9016B Software (u92h_bsp.r005), Version 1.3.5

```
Router uptime is 6 minutes
Time since Router switched to active is 4 minutes
System restarted at 1970:01:01-00:08:59
System image file is "tftp://192.168.0.9/u92h.r110_ss1"
```

If you require further assistance, contact us by sending email to spot.team@ubiQuoss.com.

```
Router Router processor with RouterM bytes of memory.
Processor board ID
460EX CPU at 1000Mhz, Rev 24.162 (pvr 1302 18a2), 1024KB L2 Cache
Last reset from h/w reset
131072K bytes of Flash internal SIMM (Sector size 256K).
```

--- Show current system's time ---

14:26:50 UTC Thu Feb 18 2010

--- Display elapsed time since boot ---

0 days, 5 hours, 11 mins, 39 secs since boot

--- CPU information ---

...

Command History Function

This function shows the commands used by the administrator in order or in reverse order based on time. This function can be used to retrieve the commands used by the administrator, thus helping to identify the cause of any problem and to recover after a system malfunction.

Table 52 Command history Function

Command	Description	Mode
show history	Shows the commands used.	Privileged
show history back	Show the commands in reverse time order.	Privileged
show history detail	Shows additional information including the time of command used/User/Access IP.	Privileged

When a command is used repeatedly, it is saved just once.

Output Post Processing

Overview of output post processing

Most of the commands that show the current status or setting of a system begin with 'show'. The show commands generally show the results on a single page, but there are cases where the list of results 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 results are 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 53 Overview of output post processing

Commands	Description
include WORD	Shows the string containing a specific word.
exclude WORD	Shows the string without a specific word.
begin WORD	Shows the lines after a string containing a specific word.

'show mac-address-table' outputs a large amount of results. You should use 'include' to get the mac addresses containing the desired part only.

```
Switch#
Switch# show run | inc service
service password-encryption
service dhcp
```

'show ip interface' outputs a large amount of results. You should use 'begin' to get the result after a specific VLAN interface.

```
Switch#show ip interface | begin Vlan1
...skipping
Vlan1 is up, line protocol is up
  Internet protocol processing disabled
  IP Flow switching is disabled
Vlan33 is administratively down, line protocol is down
  Internet address is 20.1.3.2/24
  Broadcast address is 20.1.3.255
  MTU is 1500 bytes
  Ingress service-policy is not set.
  Egress service-policy is not set.
  IP Flow switching is disabled
Vlan200 is down, line protocol is down
  Internet address is 200.1.1.236/24
  Broadcast address is 200.1.1.255
  MTU is 1500 bytes
  Ingress service-policy is not set.
  Egress service-policy is not set.
  IP Flow switching is disabled
```


DDM (Digital Diagnostic Monitoring)

U9016B supports the commands that show the status of SFP with DDM in detail. The monitoring items are as follows:

Table 54 IP OPTION command

Item	Description
Temperature	SFP Port Temp
Voltage	SFP Port Voltage
Current	SFP Port Current
RxPower	SFP Port Optic Input Power
TxPower	SFP Port Optic Output Power

SFP DDM Monitoring

The following commands are used to check the status of the SFP with DDM:

Table 55 SFP DDM Monitoring

Commands	Mode	Description
show interface transceiver	Privileged	Checks the status of DDM supporting SFP.

Switch# show interface transceiver

If device is externally calibrated, only calibrated values are printed.

++ : high alarm, + : high warning, - : low warning, -- : low alarm.

NA or N/A: not applicable, Tx: transmit, Rx: receive.

mA: milliamperes, dBm: decibels (milliwatts).

				Optical		Optical	
Port	Temperature (Celsius)	Voltage (Volts)	Current (mA)	Tx Power (dBm)	Rx Power (dBm)		
Gi2/3	42.6	3.32	17.4	-7.7	-40.0	--	
Gi2/4	41.5	3.32	15.5	-6.7	-40.0	--	

gi3	SFP	ddm	50.6°C	3.5 V	14.0 mA	-6.08 dBm	-
40.00 dBm							
			Normal	Normal	Normal	Alarm(L)	
Alarm(L)		(warn)	100.0	-10.0	4.0	1.0	131.0
0.00							0.0
		(alarm)	100.0	-10.0	4.0	1.0	131.0
0.00							0.0

					gi1/2		
		Normal		Normal	Normal	Normal	Normal
	(warn)	128.0	-128.0	6.6	0.0	131.0	0.0
							8.20
	(alarm)	128.0	-128.0	6.6	0.0	131.0	0.0
							8.20
							-40.00
							8.00
							-40.00
							-40.00

Chapter 6. OS Image and Configuration Files

This chapter describes Flash File System management and using USB or Compact Flash (CF) memory. OS Image and Configuration File are saved in the File System provided by U9016B. When you boot the system, the system load the saved OS Image and Configuration file. This chapter describes the following commands:

- File system commands for operation
- OS Image and Configuration File management
- Booting Mode Setting

The function described in this manual can be changed because of our condition.

File System

The system provides a flash file system for saving OS images and configuration files. Moreover, the system supports USB Ports. This chapter describes several file system of this product. The flash file system is used for saving OS images and configuration files.

USB memory can connect or disconnect on the system. When it is connected on the system, you can manage it like flash file system.

The basic commands for management system file are as follows:

Table 56 File Management Command

Command	Description	Mode
show flash:	Shows flash file status.	Privileged
show usbflash: <0-9>	Shows USB memory status.	Privileged
dir (usbflash: flash:) (<0-9>) directory	Shows relevant file system.	Privileged
erase (flash:) filename	Erase the saved file in flash memory.	Privileged
erase (usbflash:) (<0-9>) filename	Erases the file in CF memory, USB memory.	Privileged
rename (usbflash: flash:) (<0-9>) filename (usbflash: flash:) (<0-9>) change	Renames file name and changes the place of file system.	Privileged

The following example shows how to show the file system:

```
Router#show flash:
-length- -----type/info----- CN path
1260    text file                -- dconfig
616     text file                B* igmp_cpuha
3571    text file                -- econfig
1893    text file                -- igmp_MVLAN_final
2048    text file                -- igmp_cpuha_bk
50274956 [U9016B] 1.1.0         -- u92h.r110
59537056 [U9016B] 1.1.1         -- u92h.r111
1196    text file                -- lacp_test

19060 Kbytes available (112012 Kbytes used, 86% used)
Router#
```

The following example shows how to erase file in USB memory:

shu#show usbflash:

-----filename-----	-----type/info-----	CN	-length-
1.avi	binary data file	--	732508160
2.avi	binary data file	--	731899904
.....			

1474004 Kbytes available (2147920 Kbytes, 28 % used)

shu#**erase usbflash: 1.avi**

shu#show usbflash:

-----filename-----	-----type/info-----	CN	-length-
2.avi	binary data file	--	731899904
.....			

2189344 Kbytes available (1432580 Kbytes, 19 % used)

shu#

Image/Configuration/BSP Down/Upload

You can download the Image and configuration file from a remote TFTP or FTP server. You can upload the image and configuration file to a remote FTP (TFTP) server.

To download or upload software from a remote TFTP or FTP server to the System, perform the following tasks:



Warning

Do not select image for upgrading without permission because images are different as system model and version. Follow our introduction.



Warning

The configuration applied via FTP/TFTP is added or changed on the configuration of current system. In other words, the configuration of current system is not deleted perfectly and changed with the downloaded configuration perfectly.



Notice

For the security to access the system or server, the some specific system can only use the SFTP with the accessing way.

Download/Upload with the FTP

The following table shows the download/upload commands with using the FTP @

Table 57 Download/Upload with the FTP

Command	Description	Mode
copy ftp: (usbflash: disk1: flash:) (<0-9>)	Saves OS image file from FTP to Flash, USB, and CF.	Privileged
copy (usbflash: disk1: flash:) (<0-9>) ftp	Saves OS image from Flash, USB, and CF to FTP.	Privileged
copy ftp: config-file	Saves Configuration file from FTP to Flash.	Privileged
copy ftp: running-config	Applies Configuration file with the current running-config from FTP	Privileged
copy running-config (usbflash: disk1: flash:) (<0-9>) filename	Saves running-config with file filename to relevant file system.	Privileged
copy running-config ftp:	Saves current running-config to FTP server.	Privileged
copy ftp: bootloader		Privileged

The following example shows how to download a file with using FTP:

```
Switch# copy ftp: flash
IP address of remote host ? 10.1.13.4
User ID ? evolution
Password ?
Source file name ? 0621
Destination file name ? 0621
Warning: There is a file already existing with this name
Do you want to over-write [yes/no]? y
Over-writing 0621 file to flash memory
```

```
Switch# copy ftp bootloader
IP address of remote host ? 192.168.0.1
```

```
User ID ? Ins
Password ?
Source file name ? E7xg.bsp
Bootloader key (0xaabb) ? 0x860011
FTP:: 10.1.13.4/E7xg.bsp --> bootloader
Continue [yes/no]? yes
!
```

The following example shows how to save running-config file in the USB memory:

```
shu#copy running-config usbflash: evol.cfg
shu#show usbflash:

-----filename----- type/info----- CN -length-
2.avi                  binary data file      -- 731899904
evol.cfg              text file              --    7131
.....
2189336 Kbytes available (1432588 Kbytes, 19 % used)

shu#
```



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.

Down/UpLoading File with the TFTP

To download and upload the file with the TFTP, use the following commands:

Table 58 Down/UpLoading File with TFTP

Command	Description	Mode
copy tftp: (usbflash: disk1: flash:) (<0-9>)	Saves OS image file from TFTP to Flash, USB, and CF.	Privileged
copy (usbflash: disk1: flash:) (<0-9>) tftp:	Saves OS image from Flash, USB, and CF to TFTP.	Privileged
copy tftp: config-file	Saves Configuration file from TFTP to Flash.	Privileged
copy tftp: running-config	Applies Configuration file with the current running-config from TFTP	Privileged
copy running-config tftp:	Saves running-config with file filename to relevant file system.	Privileged
copy tftp: bootloader	Saves current running-config to TFTP server.	Privileged

The following example shows how to download a file from TFTP:

```
shu#copy tftp: usbflash:
IP address of remote host ? 10.1.13.4
Source file name ? evol.r137
Destination file name ? evol.r137

TFTP::10.1.13.4/evol.r137 --> usbflash: 0 [evol.r137]
Proceed [yes/no]? y

Switch# copy tftp bootloader
IP address of remote host ? 10.1.13.4
Source file name ? E7x.bsp
Bootloader key (0xaabb) ? 0x860011
```

```
TFTP:: 10.1.13.4// E7x.bsp --> bootloader
Proceed [yes/no]? yes
( )
```

Download/Upload through SFTP

The following table shows the commands used to download or upload files through SFTP.

Table 59. Download/Upload Command through SFTP

Command	Description	Mode
copy sftp: flash:	Saves the OS image file in the SFTP server to the flash.	Privileged
copy flash: sftp	Saves the OS image file in the flash to the SFTP server.	Privileged
copy sftp: config-file	Saves the Configuration file in the SFTP server to the flash.	Privileged
copy sftp: running-config	Applies the Configuration file in the SFTP server as the current running-config.	Privileged
copy running-config flash: filename	Saves the running-config to the file system as filename.	Privileged
copy running-config sftp:	Saves the current running-config being used not to the SFTP server.	Privileged
copy sftp: bootloader	Saves the BSP file in the SFTP server to the flash.	Privileged

The following example shows how to download a file through FTP.

```
Switch# copy sftp: flash
IP address of remote host ? 1.2.3.4
User ID ? abcd
Password ?
Source file name ? U9016B.r101
Destination file name ? U9016B.r101
Warning: There is a file already existing with this name
Do you want to over-write [yes/no]? y
Over-writing U9016B.r101 file to flash memory
!
```

```
Switch# copy sftp bootloader
IP address of remote host ? 1.2.3.4
User ID ? abcd
Password ?
Source file name ? u-boot_U9016B1.0.6.kwb_os
Bootloader key (0xaabb) ? 0x3400106
FTP:: 1.2.3.4// u-boot_U9016B1.0.6.kwb_os --> bootloader
Continue [yes/no]? yes
!
```

Configuration File Management

The system configuration file is a text file that has commands for system configuration when the system is booting. It is convenient that you do not need to input commands manually for the system configuration, whatever the system booting.

The system contains two types of configuration files: the running (current operating) configuration and the startup (last saved) configuration.

The feature of the files is as follows:

Running configuration

The running configuration is the current (unsaved) configuration that reflects the most recent configuration changes. When a user changes the system configuration, the system configuration is saved in the running configuration file of DRAM and is applied immediately to the system. You can upload or download the running configuration file via FTP or TFTP.

Startup configuration

The startup configuration is the saved configuration in DRAM and is used when the system initializes. The startup configuration is not removed when the system power is turned off. You can upload or download the startup configuration file via FTP or TFTP.

Table 60 Configuration Management Command

Command	Description	Mode
show startup-config	Shows the configuration of Booting config File saved in the flash memory	Privileged
show running-config	Shows the current configuration.	Privileged
copy running-config startup-config	Saves running-config as startup-config in the flash memory.	Privileged
erase startup-config	Deletes startup configuration file saved in the flash memory.	Privileged

Saving Configuration File

If you apply the current running configuration file when the next system's booting, save the current running configuration file to the startup configuration file before the system is reset or powered off.

To save the current running configuration file to the startup configuration file, use the following commands:

```
Switch# show running-config
!
no service dhcp
!
no logging console
!
ip domain-lookup
!
spanning-tree mode rstp-VLAN-bridge
... < > ....
SWITCH#
SWITCH# copy running-config startup-config
Overwrite 'system.cfg'? [yes/no] y
SWITCH# show startup-config
!
```

```
no service dhcp
!
no logging console
!
ip domain-lookup
!
spanning-tree mode rstp-VLAN-bridge
... < > ....
SWITCH#
```

Configuration File Erase

When the system restarts, the system reload startup-config file in the flash memory. If you want to use another configuration file, you must erase the startup-config. After you set another configuration file, restart the system.

```
SWITCH# erase flash: System1.cfg
Warning: System1.cfg is booting config file
Do you want to erase it [yes/no]? y
SWITCH# boot config System2.cfg
SWITCH# reload
```

Boot Mode Setting and System Restart

You can set OS image and config files to the system for applying on the next boot. Care must be taken in doing so as, when you restart the system, the set OS image and config file are applied to the system.

The following table shows how to set OS image and config file for next booting:

Table 61 Boot Mode Setting and System Restart

Command	Description	Mode
boot system flash <i>filename</i>	Sets OS image applied when next booting.	Privileged
boot system tftp <i>filename</i> A.B.C.D	Sets OS image applied when next booting.	Privileged
boot config <i>filename</i>	Sets filename as Start-up configuration file.	Privileged
reload	Restarts the system.	Privileged

Boot Mode Setting

Care must be taken in the following situations:

- When you execute boot flash command, you must use OS image only for U9016B.
- When you execute boot config command, you must use Config file only for U9016B.

```
Switch#
Switch# boot system flash u92h.r111
Switch#
Switch# boot config lns.cfg
Switch#
```

System Reload

You can restart the system with the power switch on/off or reload command. Moreover, you can reserve restarting time with the following commands:

Table 62 Boot Mode Setting and System Reload

Command	Description	Mode
reload	Restarts the system.	Privileged
reload {in <i>time</i> at <i>time</i> [<i>day</i>] [<i>month</i>]} [<i>reason</i>]	Reserves time for system restart. <ul style="list-style-type: none"> ▪ in: in time ▪ at: at time ▪ time: HH:MM ▪ day: 1 - 31 ▪ month: (ex. Jan or January) ▪ reason: reason for restart 	Privileged
reload cancel	Cancels the reserved system restart.	Privileged
show reload	Shows the reserved information that the system restarts.	Privileged

The following example shows how to restart system with the reload at command and cancel the schedule with reload cancel command:

```
Switch# show clock
23:52:01 UTC Thu Sep 14 2010
Switch# reload at 13:00 19 Feb For reload test
```

```
System configuration has been modified. Save? [y/n]: y
Building configuration...
[OK]
Reload scheduled for 13:00:00 KST Fri Feb 19 2010 in ( 13 hours 7 minutes )
Reload Reason: For reload test
```

```
continue to reboot ? [yes/no]: y
```

```
Switch# show reload
Reload scheduled for 13:00:00 KST Fri Feb 19 2010 in ( 13 hours 7 minutes 28 seconds ) on vty/0
(10.1.20.99)
Reload reason: For reload test
Switch#
Switch# reload cancel
```

```
***
*** --- SHUTDOWN ABORTED ---
***
```

```
Switch# show reload
No reload is scheduled.
Switch#
```



Warning

Before you restart the system, you must save the current configuration in flash memory. When you execute the reload command in config mode, you always make sure if you have saved the file as follows:

System configuration has been modified. Save? [y/n]: y



Warning

Do not restart system by force when the system is saving a file in the flash file system.

Chapter 7. NTP

This chapter describes the NTP configuration of the system.

U9016B provides time-of-day service. NTP (Network Time Protocol) synchronizes timekeeping among a set of distributed time servers and clients. This synchronization allows events to be correlated when system logs are created and other time-specific events occur.

Understanding Time Sources

The system has two clocks. One is a hardware clock (Refer to “calendar” Command), which is maintained by the battery. The other is a software clock (Refer to “clock” Command). These two clocks are managed separately.

The default time source is the software clock. The software clock maintains the current time from the system’s start time. The software clock can be set from variable source and sent with various ways to another system. When system initializes or restarts, the software clock initializes with using the hardware clock. You can make changes by using the following sources:

- Network Time Protocol (NTP)
- Passive Setting (Hardware clock)

Software clock manages time information based on Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT). You can set time zone and daylight savings time for supporting time information of the place where the system run in.

Network Time Protocol

NTP (Network Time Protocol) synchronizes timekeeping among a set of distributed time servers and clients. This synchronization allows events to be correlated when system logs are created and other time-specific events occur.

Hardware Clock

Even if the system is restarted or turned off, the system has hardware clock maintained by battery for maintaining current time. When the system is restarted, you use the hardware clock for initializing software clock.

Configuring NTP

This chapter describes how to configure NTP with the following procedure:

- Configuring Poll-Based NTP Associations
- Configuring NTP Authentication
- Configuring the Source IP Address for NTP Packets
- Configuring the System as an Authoritative NTP Server
- Updating the Hardware Clock

Configuring Poll-Based NTP Associations

The network system using NTP provides various modes in order to synchronize between the time source and system clock. There are two ways for obtaining the time information from the network. One is a poll-based association from the host server and the other is by listening to NTP information from broadcast network. This section describes the server request mode from server.

The following modes are server request modes used by users:

- Client mode
- Symmetric active mode

In the case of client mode, the system researches time servers to gain current time information. The system synchronizes one of them. In this case, because the system and time servers are in a client and server relationship, the system does not use the time information sent from another-client's equipment. This mode is useful for a system that does not provide time information to another local client. You can use `ntp server` command to set time for a server that you want to have time synchronized to client mode.

In the case of symmetric active mode, the system researches the time servers to gain current time information and provides time information to a local host. As this mode is peer- to-peer relation, the system also saves the time information of local network equipment on networking. This mode must use when mutual crossing servers exist via complex network path. Most stratum 1 and stratum 2 servers use this type of network setting. When you set symmetric active mode, use `ntp peer` command.

To decide NTP mode depend on equipment's role (server or client) and stratum 1 server setting.

Table 63 Setting NTP Server

Command	Purpose
Switch(config)# ntp server <i>ip-address</i>	Sets NTP with Client mode.
Switch(config)# ntp peer <i>ip-address</i>	Sets NTP with Symmetric active

Configuring NTP Authentication

Before you use NTP, you must perform an authentication procedure. This procedure starts with creating an NTP packet.

After NTP authentication is set correctly, the system synchronizes a reliable time source and time. When you send or receive the encrypted NTP packet, use the following commands in the global configuration mode:

Table 64 Configuring NTP Authentication

Step	Command or Action	Purpose
Step 1	ntp authenticate	Enables NTP authentication.
Step 2	ntp authentication-key <i>key-number</i> md5 <i>value</i>	Defines authentication key.
Step 3	ntp trusted-key <i>key-number</i>	Defines trusted-key. If authentication key is trusted key, the system attempts to synchronize time with the system using this key in NTP packet.
Step 4	ntp server <i>ip-address</i> key <i>key-number</i>	Enables to synchronize software clock and NTP time server.

Configuring the Source IP Address for NTP Packets

When the system sends an NTP packet, the source IP address of the NTP packet is set with an interface address that sends an NTP packet. If you want to set a specific interface IP address, execute the following commands.

Table 65 Configuring the Source IP Address for NTP Packets

Command	Purpose
ntp source <i>interface</i>	Assign interface to get ip address.

Configuring the System as an Authoritative NTP Server

When you synchronize the hardware clock with NTP time, execute the following commands in the config mode:

Table 66 Configuring the System as an Authoritative NTP Server

Command	Purpose
ntp master [<i>stratum</i>]	Sets the system as NTP server.

The system provides stratum 1 service. However, we do not recommend this service because there is no RF or atomic clock that can connect to this equipment.

Updating the Hardware Clock

You can set to update hardware clock by software clock from equipment having hardware clock. We recommend the NTP because software clock is more accurate than a hardware clock.

When you synchronize the hardware clock with NTP time, execute the following commands in the config mode:

Table 67 Updating the Hardware Clock

Command	Purpose
Switch(config)# ntp update-calendar	Sets update calendar with software clock periodically.

Configuring Time and Date Manually

If you have not available time source, you can set current time directly after system runs.

Configuring the Time Zone

When you set timezone information, execute the following commands in the config mode:

Table 68 Configuring the Time Zone

Command	Purpose
Switch(config)# clock timezone <i>zone hours-offset [minutes-offset]</i>	Sets timezone. Zone: name of timeband. Minutes-offset: interval minutes with UTC.

Configuring Summer Time (Daylight Savings Time)

If you set daylight savings time, execute the following commands in the config mode:

Table 69 Configuring Summer Time (Daylight Savings Time)

Command	Purpose
Switch(config)# clock summer-time <i>zone recurring [week day month hh:mm week day month hh:mm [offset]]</i>	Sets recurring start and end summer time. Offset: minute

If daylight saving time does not repeat per every year, you can set the exact day when daylight saving time starts. The following command shows how to set it:

Table 70 Configuring Summer Time

Command	Purpose
Switch(config)# clock summer-time <i>zone date month date year hh:mm month date year hh:mm [offset]</i>	Sets specific start and end summer time. Offset: minute
or	
Switch(config)# clock summer-time <i>zone date date onth date year hh:mm date month year hh:mm [offset]</i>	

Manually Setting the Software Clock

If the system has hardware clock or synchronizes effective way like NTP, you do not need set software clock. If you have not useful time source, use the following command:

When you set software clock directly, use the following commands:

Table 71 Manually Setting the Software Clock

Command	Purpose
Switch# clock set <i>hh:mm:ss day month year</i>	Sets software clock.
or	
Switch# clock set <i>hh:mm:ss month day year</i>	

Using the Hardware Clock

The system has a hardware clock. The hardware clock is a chip that has a chargeable battery. Even though you restart the system, the system can maintain the time information.

The software clock must receive the time information from reliable time source for maintaining exact time information. The software clock must update hardware clock time periodically while the system runs.

The following tasks are for setting hardware clock:

- Setting the Hardware Clock
- Setting the Software Clock from the Hardware Clock
- Setting the Hardware Clock from the Software Clock

Setting the Hardware Clock

The hardware clock manages the time separately. The hardware clock runs continuously even if the system is restarted or turned off. The hardware clock is only set once when the system is set up.

If you have reliable external time source, you must not set the hardware clock directly. The time will synchronize with using NTP.

If you have no external time source, execute the following command in EXEC mode in order to set the hardware clock:

Table 72 Setting the Hardware Clock

Command	Purpose
Switch# calendar set <i>hh:mm:ss day month year</i> or Switch# calendar set <i>hh:mm:ss month day year</i>	Sets Hardware Clock

Setting the Software Clock from the Hardware Clock

When you set software clock with new hardware clock setting, execute the following commands in EXEC mode:

Table 73 Setting the Software Clock from the Hardware Clock

Command	Purpose
Switch# clock read-calendar	Sets software clock with hardware clock.

Setting the Hardware Clock from the Software Clock

When you set hardware clock with new software clock setting, execute the following commands in EXEC mode:

Table 74 Setting the Hardware Clock from the Software Clock

Command	Purpose
Switch# clock update-calendar	Sets hardware clock with softwareclock.

Monitoring Time and Calendar Services

When you show clock, calendar, and NTP information, use the following commands:

Table 75 Monitoring Time and Calendar Services

Command	Purpose
show calendar	Shows current hardware clock information.
show clock	Shows current software clock information.
show ntp associations [detail]	Shows NTP association status.
show ntp status	Shows ntp status.

Configuration Examples

Clock, Calendar, and NTP Configuration Examples

The system that has hardware clock connects with two server system and update hardware clock periodically. Clock timezone KST 9

```
ntp update-calendar
ntp server 192.168.13.57
    ntp server 192.168.11.58
```

Chapter 8. DHCP

This chapter describes the DHCP configuration of the system.

DHCP Server Features and 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 an IP network. DHCP is designed for the configuration of large-scale networks and complex TCP/IP software to reduce 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 the two:

- 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.

U9016B 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 of DHCP Server

DHCP supports three ways for IP address allocation as follows:

- 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 the main parameters are as follows:

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

U9016BSwitch as a DHCP Server

The following figure shows the basic steps that occur when a DHCP client request an IP address from a DHCP server (U9016B):

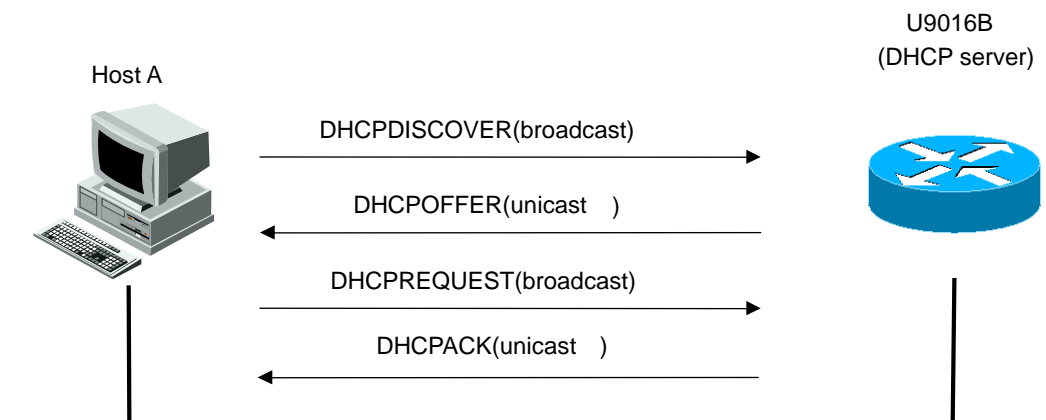


Figure 12. U9016BSwitch as a DHCP server

1. The Client Host A sends broadcast message *DHCPDISCOVER* to the DHCP server.
2. DHCP server sends 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 more than one DHCP server 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.

Advantages of DHCP Server

The features of the U9016B server have 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** – As the DHCP server maintains configurations for several subnets, an administrator only needs to update a single, central server when configuration parameters change.

Enabling DHCP Server Function

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:

Table 76 Enabling DHCP Server Function

Command	Description
service dhcp	Enables the DHCP server functions of the switch. To disable the DHCP server dunctions, use no command.

The following example shows how to enable DHCP server function:

```
Router# configure terminal
Router(config)# service dhcp
Router# show running-config
!
...
service dhcp server
...
!
```

DHCP Address Pool

U9016B server support Network Pool and Host Pool.

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

DHCP Network Pool Configuration

You can configure a DHCPNetwork Pool with a name that is a symbolic string (such as “ubiQuoss”) or an integer (such as “0”). For DHCP network pool settings, 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 complete required tasks illustrated in the following section.



Notice

Different network pools can be configured into a single 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:

Table 77 IP DHCP Pool

Commnad	Description
ip dhcp pool name	Generates a name for DHCP Network Pool Enters the DHCP network pool configuration mode identified as “config-dhcp#” prompt.

The following example shows setting a DHCP Network Pool name as ‘network_pool1’. You can use up to 31 characters.


```
Router# configure terminal
Router(config)# ip dhcp pool network_pool1
Router(config-dhcp)# exit
Router# show running-config
...
!
ip dhcp pool network_pool1
!
...
```

DHCP Subnet and Network Mask Configuration

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

Table 78 DHCP Subnet and Network Mask Configuration

Command	Description
network <i>network-number/prefix-length</i>	Specifies the sub network number and mask for DHCP address pool.

The following shows an example where setting DHCP Subnet and Network mask for 100.0.0.0/24:

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

Setting IP Address Range to be assigned in Network Pool

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

Table 79 Setting IP Address Range to be Assigned in Network Pool

Command	Description
<code>range lowest-address highest-address</code>	Sets the IP address range to be assigned to clients in a subnet. This command should be used after DHCP subnet and network mask are set.

The following example shows setting IP address range, from 100.0.0.1 to 100, which will be assigned in network pool:

```
Router# configure terminal
Router(config)# ip dhcp pool network_pool1
Router(config-dhcp)# range 100.0.0.1 100.0.0.100
Router# show running-config
...
!
ip dhcp pool network_pool1
network 100.0.0.0/24
range 100.0.0.1 100.0.0.100
!
```

Setting the 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:

Table 80 Setting the Default Router for Client

Command	Description
<code>default-router address</code>	Shows the IP address of a default router for the DHCP client

The following example shows setting the default router for 100.0.1 for a client in DHCP server:

```
Router# configure terminal
Router(config)# ip pool network_pool1
Router(config-dhcp)# default-router 100.0.0.1
Router(config-dhcp)# exit
Router# show running-config
...
!
ip dhcp pool network_pool1
default-router 100.0.0.1
network 100.0.0.0/24
range 100.0.0.1 100.0.0.100
```

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:

Table 81 Setting DNS IP Server for Client

Command	Description
---------	-------------

dns-server <i>address</i>	Specifies the IP address of the DNS server that the DHCP client can use. A new DNS server IP will be added when a command is entered.
---------------------------	--

The following is an example of setting DNS Server for 200.0.0.1, 200.0.0.2 in DHCP server for the client:

```
Router# configure terminal
Router(config)# ip dhcp pool network_pool1
Router(config-dhcp)# dns-server 200.0.0.1
Router(config-dhcp)# dns-server 200.0.0.2
Router(config-dhcp)# exit
Router# show running-config
...
!
ip dhcp pool network_pool1
dns-server 200.0.0.1
dns-server 200.0.0.2
default-router 100.0.0.1
network 100.0.0.0/24
range 100.0.0.1 100.0.0.100
!
...
```

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:

Table 82 Setting the Domain Name for Client

Command	Description
domain-name <i>domain</i>	Specifies the domain name for a client

The following is an example of setting a domain name as “ubiQuoss.com” in a DHCP server for the client.

```
Router# configure terminal
Router(config)# ip dhcp pool network_pool1
Router(config-dhcp)# domain-name ubiQuoss.com
Router(config-dhcp)# exit
Router# show running-config
...
!
ip dhcp pool network_pool1
dns-server 200.0.0.1 200.0.0.2
domain-name ubiQuoss.com
default-router 100.0.0.1
network 100.0.0.0/24
range 100.0.0.1 100.0.0.100
!
...
```

Setting Group for Network Pool

Network group includes multiple DHCP network pools, and network pools in the same group share the IP pool.

Table 83 Setting Group for Network Pool

Command	Description
group <i>group-name</i>	Displays group name

**Notice**

In the case that one interface consists of multiple IP addresses, network pool of each IP address should be configured with the same group name.

The following is an example of binding different network pools into “ubiQuoss pool”.

```
Router# configure terminal
Router(config)# ip dhcp pool network_pool1
Router(config-dhcp)# group ubiQuoss_pool
Router(config-dhcp)# exit
Router# show running-config
...
!
ip dhcp pool network_pool1
 dns-server 200.0.0.1 200.0.0.2
 domain-name ubiQuoss.com
 default-router 100.0.0.1
 network 100.0.0.0/24
 range 100.0.0.1 100.0.0.100
 group ubiQuoss_pool
```

Setting the Address Lease Time

By default, each IP address assigned by a DHCP server comes with a 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:

Table 84 Setting the Address Lease Time

Command	Description
lease {days [hours] [minutes]}	Specifies the lease period Default : one hour Infinite: Use automatic allocation system leasing IP address permanently to the host.

The following is an example of setting the lease time for 20 minutes:

```
Router(config)# ip dhcp pool network_pool1
Router(config-dhcp)# lease 0 0 20
Router(config-dhcp)# exit
Router# show running-config
...
!
ip dhcp pool network_pool1
dns-server 200.0.0.1 200.0.0.2
lease 0 0 20
domain-name ubiQuoss.com
default-router 100.0.0.1
network 100.0.0.0/24
range 100.0.0.1 100.0.0.100
group ubiQuoss_pool
!
...
```

DHCP Host Pool Configuration

A manual binding is a mapping between the IP address and MAC (Media Access Control) 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 configuration mode to set parameters such as IP and MAC.

To set a DHCP host pool, you should complete the required tasks illustrated in the following section:



Notice

A host pool is designed for clients who want to apply common parameters. You can set multiple hosts to a host pool. You can apply the parameter to all hosts in the pool by a single setting.

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 global config mode:

Table 85 Setting DHCP Host Pool Name and Entering DHCP Configuration Mode

Command	Description
<code>ip dhcp pool <i>name</i></code>	Generates a name for DHCP host pool Enters the DHCP host pool configuration mode identified as "config-dhcp#" prompt.

The following is an example of setting the DHCP Host Pool Name as 'host_pool1'. You can use up to 31 characters.

```
Router# configure terminal
Router(config)# ip dhcp pool host_pool1
Router(config-dhcp)# exit
Router# show running-config
...
!
ip dhcp pool host-pool
!
...
```

Table 86 Host Pool Configuration Command

Command	Description
<code>default-router <i>address</i></code>	Shows IP address of a default router for DHCP client
<code>dns-server <i>address1 address2 address3</i></code>	Specifies the IP address of the DNS Server that the DHCP client can use One IP address is required, but you can specify up to three IP addresses in the command line.
<code>domain-name <i>domain</i></code>	Specifies a domain name for a client
<code>host <i>ipaddr/prefix-len</i></code>	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 the network command. Configurations of other commands are the same.

Client Configuration for DHCP Manual Binding

It configures clients to provide manual binding in host pool.

Table 87 Client Configuration for DHCP Manual Binding

Command	Description
host <i>ip-address netmask</i>	Generates an IP address and network mask for a client Enters the DHCP Host Configuration mode identified as "config-dhcp #"

Table 88 Manual Binding Command

Command	Description
hardware-address <i>hardware-address</i>	Specifies the hardware address of the client

The following example shows that allocating IP 110.0.0.1 to a user with a MAC address of 00:11:22:33:44:55. The command should be set after 'network A.B.C.D' command is set.

```
Router# configure terminal
Router(config)# ip dhcp pool host_pool1
Router(config-dhcp)# host 110.0.0.1/24
Router(config-dhcp)# hardware-address 0011.2233.4455
Router(config-dhcp)# exit
Router# show running-config
!
ip dhcp pool host_pool1
  host 110.0.0.1/24
  hardware-address 0011.2233.4455
!
```

Other Global Commands

Table 89 Global Command List

Command	Description
ip dhcp max-lease {days [hours] [minutes]]infinite}	When DHCP client requests for the lease time, DHCP server allocates time, which does not exceed max-lease time to DHCP client. Switch has the default value of one day.

The following is an example of setting max-lease time for 2 days:

```
Router(config)# ip dhcp max-lease 2
Router# show running-config
!
ip dhcp max-lease 2
```

DHCP relay agent Features and Configuration

DHCP relay agent Overview

DHCP relay is the host forwarding DHCP packet between DHCP client and DHCP server in each different sunet.

DHCP relay agent records (DHCP packet's giaddr field) value on gateway address and insert relay agent information to DHCP packet. Then you can set to send it to server.

If you set U9016B as DHCP relay agent, DHCP client and DHCP server forwards DHCP packet each other.

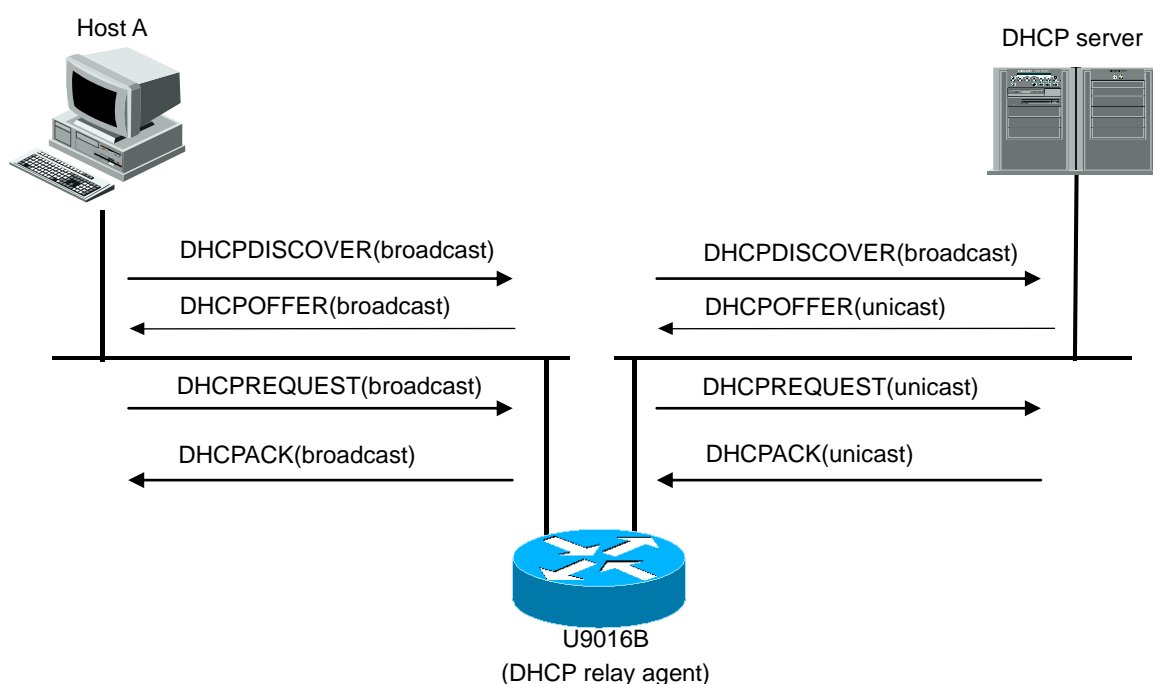



Figure 13. Message transmissions of DHCP server as a DHCP relay agent

1. DHCP client sends broadcast message, *DHCPDISCOVER* to the IP requested.
2. DHCP relay agent receives the IP request message from DHCP client, and sent the message to DHCP server by unicast.
3. When the DHCP server receives a message from the DHCP relay agent, it sends the *DHCPOFFER* message to the DHCP relay agent by unicast. The message contains information including IP address, default gateway etc. of the client (an IP address recorded in giaddr field is used as a destination IP).
4. The DHCP relay agent sends the *DHCPOFFER* message to the client.
5. *DHCPREQUEST* and *DHCPACK* messages are transferred by the DHCP relay agent in a same manner between the DHCP server and the client.

Enabling DHCP Relay Function

By default, the DHCP replay agent functions are not enabled. To enable the DHCP relay agent, use the following command in global configuration mode:

Table 90 Enabling DHCP Relay Function

Command	Description
service dhcp relay	<p>Enables DHCP Relay function of router</p> <p>Use no format of this command to disable the DHCP relay.</p> <hr/> <div>  <div> <p>Note</p> <p>You may not set DHCP relay and DHCP server together.</p> </div> </div>

If system forward DHCP packet via DHCP relay agent, the switching chip of a router does not forward the packet and traps a packet with the CPU. Then you need to set the relay agent to precede the packet.

The following example shows how to enable a DHCP relay agent when a user is connected to the port of Vlan10 and to DHCP server through vlan20:

```

Router#config terminal
Router(config)#class-map dhcp_user_class
Router(config-cmap)#match protocol udp
Router(config-cmap)#match layer4 source-port 68
Router(config-cmap)#exit
Router(config)#class-map dhcp_server_class
Router(config-cmap)#match protocol udp
Router(config-cmap)#match layer4 source-port 67
Router(config-cmap)#end
Router#show class-map

CLASS-MAP-NAME: dhcp_user_class (match-all)
  Match Source Port: 68
  Match Protocol: udp

CLASS-MAP-NAME: dhcp_server_class (match-all)
  Match Source Port: 67
  Match Protocol: udp

Router#config terminal
Router(config)#policy-map dhcp_user_map
Router(config-pmap)#class dhcp_user_class
Router(config-pmap-c)#trap-cpu
Router(config-pmap-c)#exit
Router(config-pmap)#exit
Router(config)#policy-map dhcp_server_map
Router(config-pmap)#class dhcp_server_class
Router(config-pmap-c)#trap-cpu
Router(config-pmap-c)#exit
Router(config-pmap)#exit
Router(config)#int vlan10
Router(config-if-Vlan10)#service-policy input dhcp_user_map
Router(config-if-Vlan10)#int vlan20
Router(config-if-Vlan20)#service-policy input dhcp_server_map
Router(config-if-Vlan20)#end
Router#show policy-map

POLICY-MAP-NAME: dhcp_user_map
  State: attached

CLASS-MAP-NAME: dhcp_user_class (match-all)
  Trap-cpu

POLICY-MAP-NAME: dhcp_server_map
  State: attached

CLASS-MAP-NAME: dhcp_server_class (match-all)
  Trap-cpu

```

```
Router#show service-policy
Interface    Vlan20 : input  dhcp_server_map
Interface    Vlan10 : input  dhcp_user_map
Router# configure terminal
Router(config)# service dhcp relay
Router(config)# exit
Router# show ip dhcp relay
```

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

DHCP helper-address is configured on following servers:
none

DHCP Server Configuration on DHCP Relay Agent

To run DHCP relay agent, you set DHCP server to DHCP discover/request message from DHCP client. Relay agent can set server to per interface receiving DHCP packet or server to forward regardless to interface receiving the packet.

To set DHCP server for each interface that received a DHCP message, use the following command:

Table 91 DHCP Server Configuration on DHCP Relay Agent

Command	Description
ip dhcp helper-address <i>address</i>	Sets the IP address of a DHCP server which will forward the DHCP discover/request message that the interface has received. Only DHCP packets received on the interface are forwarded to the assigned server. To delete the DHCP server functions, use no command.

When you set DHCP server regardless of interface with setting DHCP message with RX, use the following command:

Table 92 DHCP Server Configuration on DHCP Relay Agent

Command	Description
ip dhcp-server <i>address</i>	Sets an IP address of the DHCP server that a DHCP relay agent will forward a DHCP discover/request message to. To delete the setting, use no command.



Notice

DHCP relay Agent of U9016B can have up to 256 helper-addresses.

The following example shows how to set a server address in DHCP relay agent:

```
Router#configure terminal
Router(config)#service dhcp relay
Router(config)#ip dhcp-server 192.168.0.254
Router(config)#exit
Router#show ip dhcp relay
```

```

DHCP relay                : Enabled
DHCP Smart Relay feature  : Disabled
DHCP Smart Relay retry count : 3
DHCP server-id based relay : Disabled
Verification of MAC address : Enabled
Insertion of option 82    : Disabled
DHCP Option82 Management-IP : 0.0.0.0
DHCP maximum hop count    : 10
DHCP helper-address is configured on following servers:
    192.168.0.254
Router#configure terminal
Router(config)#interface vlan1
Router (config-if-vlan1)#ip dhcp helper-address 100.0.0.1
Router(config)#end
Router#show ip dhcp relay
DHCP relay                : Enabled
DHCP Smart Relay feature  : Disabled
DHCP Smart Relay retry count : 3
DHCP server-id based relay : Disabled
Verification of MAC address : Enabled
Insertion of option 82    : Disabled
DHCP Option82 Management-IP : 0.0.0.0
DHCP maximum hop count    : 10

DHCP helper-address is configured on following servers:
    192.168.0.254, 100.0.0.1(vlan1)

```

DHCP Relay Agent Information option (OPTION82) Configuration

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

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

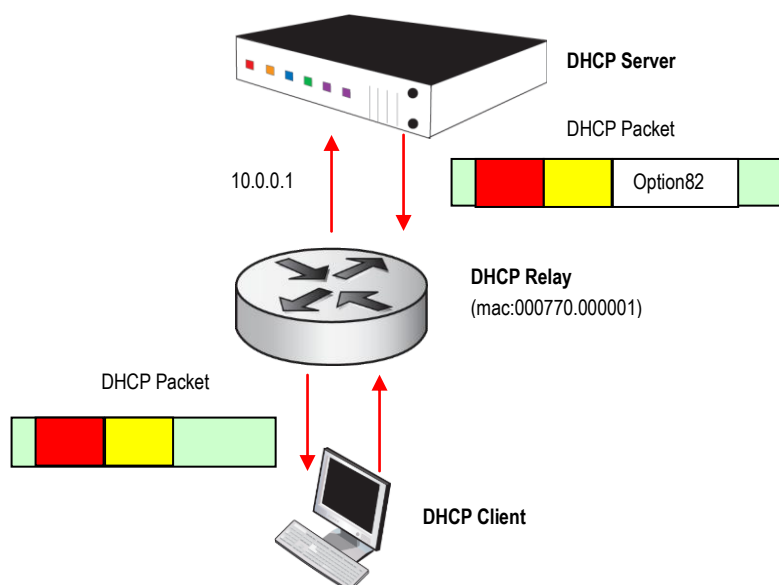


Figure 14. DHCP Relay Option82

Enabling DHCP relay agent information option

To enable the relay information option function of U9016B DHCP Relay Agent, use the following command:

Table 93 Enabling DHCP relay agent information option

Command	Description
ip dhcp relay information option	Enables DHCP relay agent information option By default, the feature is not enabled. Use no format to exclude relay agent information option in router.

The following shows an example of adding the relay agent information option function of DHCP relay agent:

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

```
DHCP relay : Enabled
```

```

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

DHCP helper-address is configured on following servers:
192.168.0.254

Relay agent information option reforwarding Policy Configuration

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

Table 94 Relay agent information option reforwarding Policy Configuration

Command	Description
ip dhcp relay information option policy {drop keep replace}	<p>The default is set to replace.</p> <p>Drop: deletes packets with relay information option</p> <p>keep: maintains the existing relay information option; and adds relay information option if no relay agent information option in router.</p> <p>replace: Replaces the relay information option in router with relay information option.</p> <p>Use no format command to go back to default.</p>

In the following example, DHCP Relay Information Option reforwarding is set to “drop”.

```

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

```

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

DHCP helper-address is configured on following servers:
192.168.0.254

DHCP Smart Relay Configuration

The system forward packet to DHCP server with configuring primary IP address of interface received DHCP packet from DHCP client with giaddr field of DHCP packet.

Normally, a DHCP relay agent forwards DHCP_DISCOVER message to a DHCP server only with a primary IP address on an interface, even if there is more than one IP address on the interface.

If the smart relay forwarding is enabled, a DHCP relay agent will retry sending DHCP discover message with a secondary IP address, in the case of no response from the DHCP server.

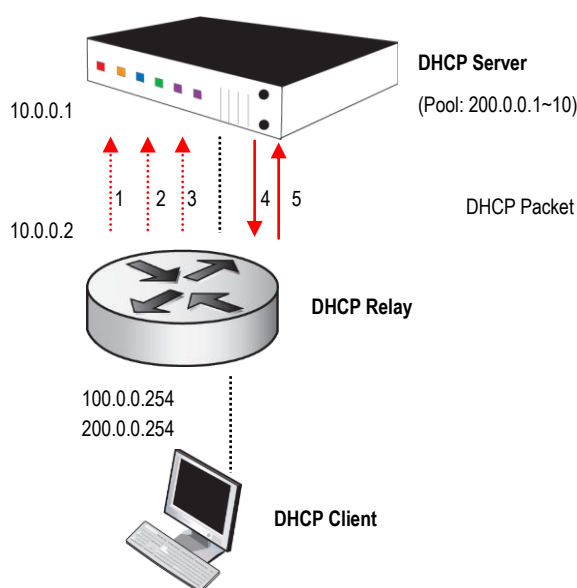


Figure 15. DHCP Smart-Relay running procedure

To enable DHCP smart-relay, use the following command.

Table 95 enabling DHCP smart-relay

Command	Description
ip dhcp smart-relay	Enables DHCP smart-relay function By default, the feature is set to disabled. Use no format command to disable the function.

To set the number of trials that a client can change IP address which a DHCP relay agent sets in the giaddr field, use the following command:

Table 96 the number of trials that a client can change IP address

Command	Description
ip dhcp smart-relay retry <1-10>	Sets the number of trials that a relay agent sets in <1-10> giaddr field. The default is 3. To go back to the default, use no command.

The following is an example of Setting up DHCP Smart-Relay:

```
Router# configure terminal
Router(config)# ip dhcp smart-relay
Router(config)# ip dhcp smart-relay retry 5
```

```
Router(config)# exit
Router# show ip dhcp relay
```

```
DHCP relay : Enabled
DHCP Smart Relay feature : Enabled
DHCP Smart Relay retry count : 5
DHCP server-id based relay : Disabled
Verification of MAC address : Enabled
Insertion of option 82 : Enabled
DHCP relay agent information option policy : drop
DHCP Option82 Management-IP : 0.0.0.0
DHCP maximum hop count : 10
```

DHCP helper-address is configured on following servers:
192.168.0.254

DHCP Relay Agent Verify MAC-Address Configuration

DHCP relay agent uses the following items among fields of DHCP packets to recognize DHCP client that requests for IP.

1. source MAC address
2. client hardware address(chaddr field)
3. client identifier option (option61)

To block IP assigning request from vicious client, the DHCP relay agent check above three fields of DHCP discover message. In case that the three fields are not the same, you can set not to forward DHCP discover message to the server.

To drop the DHCP discover message whose client hardware address or client identifier option has been changed, use the following command:

Table 97 DHCP Relay Agent Verify MAC-Address Configuration

Command	Description
ip dhcp relay verify mac-address	When a client hardware address or client identifier option of DHCP discover message has been changed it does not forward the message to the server. By default this is enabled. To disable the function, use no command

The following is an example of deleting the function of “DHCP relay agent verifies MAC-address”:

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

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

DHCP helper-address is configured on following servers:
192.168.0.254

DHCP Class based DHCP packet forwarding

This function is for selection of message receiving from client like `ip dhcp-server` and `ip dhcp helper-address` commands.

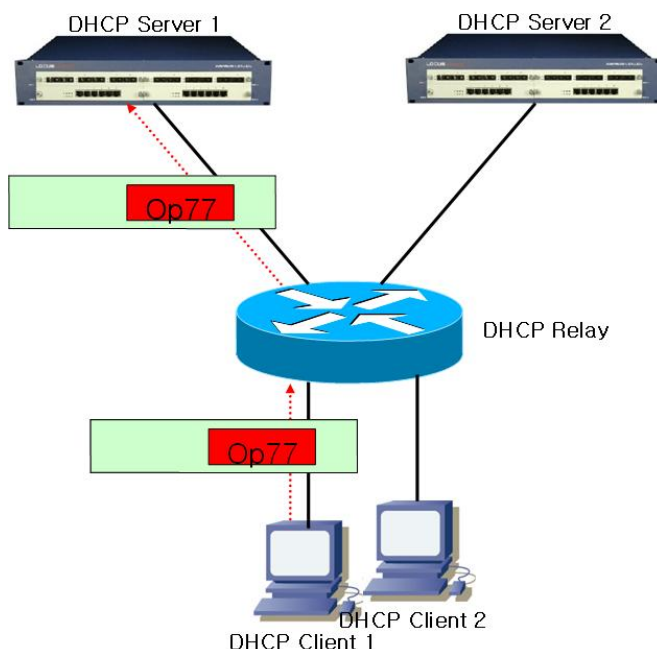


Figure 16. DHCP Class based on DHCP packet Relay

DHCP Class Configuration

To set DHCP class in U9016B DHCP relay agent, use the following command.

Table 98 DHCP Class Configuration

Command	Description
ip dhcp class <i>class-name</i>	Assigns DHCP Class Name. Enters DHCP class setting mode which is recognized as "(dhcp-class) #". To delete the class, use no command.
option <1-255> {ascii hex} WORD	Set option-option value so that the DHCP message sent from a client can be categorized into this class. <1-255>: DHCP option number {ascii hex}: DHCP option value format (ascii string variable, hexadecimal) WORD: option value,
<div style="display: flex; align-items: center;"> <div style="margin-right: 10px;"> </div> <div> <p>Notice</p> <p>For a hexadecimal format, you must use even number of digits. e.g. <code>ip dhcp option 60 hex 1 (x)</code> <code>ip dhcp option 60 hex 01 (o)</code></p> </div> </div>	

The following example shows how to set "test".

```
Router(config)# configure terminal
Router(config)# ip dhcp class test
Router(dhcp-class)# option 77 ascii ubiQuoss
```


DHCP Relay-Pool Configuration

To set DHCP Relay-Pool, use the following commands:

Table 99 DHCP Relay-Pool Configuration

Command	Description
ip dhcp relay-pool <i>WORD</i>	Generates a DHCP relay-pool and enters DHCP relay-pool which is recognized as "(dhcp-pool)#". WORD: name of relay-pool To delete relay-pool, use no command.
relay source <i>A.B.C.D/M</i>	Sets the subnetwork of relay-pool. To disable the function, use no command.
class <i>class-name</i>	Sets the DHCP class of a DHCP DISCOVER/REQUEST message that a client has sent so the message can be forwarded to the assigned server in the relay-pool. You can assign more than one class. To disable the function, use no command.
relay target <i>A.B.C.D/M</i>	Sets a server which will forward a DHCP DISCOVER/REQUEST message. To disable the function, use no command.

If you set "test" DHCP class and DHCP relay-pool "test-pool", DHCP relay agent forwarding message included "ubiQuoss" of ascii characters.

```
Router(config)# ip dhcp relay-pool test
Router(config-dhcp)# relay source 100.0.0.0/24
Router(config-dhcp)# exit
Router(config-dhcp)# class test
Router(config-class)# relay target 200.0.0.254
Router(config-class)# exit
Router(config)# service dhcp relay
```

DHCP Snooping Function

DHCP Snooping Function Overview

The DHCP snooping compiles an address binding table that is similar to the one made in the DHCP server based on DHCP messages exchanged between DHCP client and DHCP server.

The binding table is used as database to prevent malicious users. Snoop can also control messages between client servers. It can be enabled in the same way as DHCP agent and it cannot be used with DHCP server simultaneously.

Trust and Untrust Source

The DHCP Snooping classifies traffic sources into trusted and untrusted. Untrusted sources can do traffic attack and other conflict behaviors. To prevent these obstacles, the DHCP Snooping can filter messages from untrusted sources.

DHCP Snooping Binding Database

The DHCP Snooping makes a dynamic database using DHCP Message and maintains it. The database includes an entry of untrusted host of VLAN which has DHCP Snooping enabled. The database entry adds every DHCP message from DHCP server and client after Validation check. It reports the result of validation check in state items. For a series of normal DHCP messages started from the same DHCP client, only the latest message is recorded in the database entry. When the IP address lease time has passed or when receiving a DHCP release message from a host, it is recorded as time expired or released on the state list. When the database entry has exceeded the max-value the oldest invalid entry will be deleted, a new entry will be added.

The DHCP Snooping binding database includes MAC Address, Client Hardware Address, Client Identifier, leased IP address, lease time, received time, State, VLAN ID, information of interface port connected to the host.

Packet Validation

A switch verifies the validity of the DHCP packet received from the untrusted interface of VLAN which has DHCP Snooping enabled. In the following case a switch records each item in the state list of DHCP Snooping binding table.

A switch receives a DHCP discover packet that has a source MAC address not correspond with a DHCP client identifier or DHCP client hardware address from an untrusted interface.

Packet Rate-limit

The DHCP Snooping applies rate-limit to DHCP packets from the same DHCP client. It allows up to two packets per second sent from the same type of DHCP client.

DHCP Snooping Function Activation

By default, DHCP Snooping of a switch is disabled. To enable the DHCP Snooping, use the following command in the global mode.

**Notice**

As in the relay agent setting, to enable the DHCP Snooping you must use class-map and policy-map so that a DHCP packet can be trapped to the CPU. Refer to the Section 6.2.2 for the configuration.

Table 100 DHCP Snooping Function Activation

Command	Description
ip dhcp snooping	Activates DHCP Snooping function Use no format command to disable DHCP Snooping function.

The following is an example of enabling DHCP Snooping function:

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

DHCP Snooping VLAN Configuration

In the DHCP Snooping VLAN Configuration, you will set a VLAN that will snoop DHCP packets. Packets passing by VLANs other than the one you have set will not be snooping.

Table 101 DHCP Snooping VLAN Configuration

Command	Description
ip dhcp snooping VLAN <i>VLAN_ID</i>	Sets a VLAN which will snoop DHCP packets. To delete the DHCP Snooping VLAN, use no command.



Notice

When you use DHCP Snooping and DHCP Relay simultaneously, DHCP Relay will forward a packet.



Notice

When you use DHCP Snooping and DHCP Relay simultaneously, you must set both VLANs connected to DHCP server and to DHCP client as Snooping VLANs.

The following example shows how to enable DHCP Snooping of vlan1.

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

DHCP Snooping Information option (OPTION82) Configuration

When DHCP Snooping snoops a DHCP request received from a DHCP client, it provides DHCP Snooping information option so the information the interface and switch connected to a DHCP client can be included.

Enable DHCP Snooping Information Option Function

To enable information option of U9016B Snooping, use the following command:

Table 102 Enable DHCP Snooping information option function

Command	Description
ip dhcp snooping information option	Enables DHCP Snooping information (option-82 field). By default, this is disabled.

The following example shows how to enable DHCP Snooping Information Option:

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

DHCP snooping information option reforwarding policy Configuration

By default, DHCP Snooping information policy of U9016B drops packets with information option sent by DHCP client.

To change default policy of U9016B, use the following command in global mode:

Table 103 DHCP Snooping information option reforwarding policy Configuration

Command	Description
ip dhcp snooping information policy {drop keep replace}	The default is set to drop. drop: deletes packets with DHCP Snooping information. keep: maintains the existing DHCP Snooping information. replace: replaces the existing DHCP Snooping information with the DHCP Snooping information of router.

The following example shows how to set DHCP Snooping information option reforwarding policy as keep.

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

DHCP Snooping Trust Port Configuration

To set a Trust Port (e.g. a DHCP server direction port), use the following command. When you set a Trust Port, a request packet will be forwarded as a trust port only.

Table 104 DHCP Snooping Trust Port Configuration

Command	Description
ip dhcp snooping trust	Sets an assigned port as a Trust Port. It will not conduct a Validation check for a DHCP packet received at the Trust Port. Requested packets from the host will be forwarded only to the Trust Port. By default, all ports are untrusted ports.

The following is an example of setting port 'gi1/1' on Trust Port:

```
Router(config)# interface gi1/1
Router(config-if-Giga1/1)# ip dhcp snooping trust
Router(config-if-Giga1/1)# end
Router# show ip dhcp snooping interface
```

Interface	Trust State	Max Entry
Giga1/1	Trusted	2000

DHCP snooping max-entry Configuration

To set the number of DHCP Snooping max-entry for each port, use the following command:

Table 105 DHCP snooping max-entry Configuration

Command	Description
ip dhcp snooping max-entry <10-1000>	Sets the number of DHCP Snooping max-entry for each port. It does not delete any entry that is valid (and in use of an IP) even when binding entries are generated because it exceeds the max-entry. By default, each port has 2000 Max-entries.

The following example shows how to set DHCP Snooping Max-Entry of gi 1/1 with 100:

```
Router# configure terminal
Router(config)# interface gi1/1
Router(config-if-Giga1/1)# ip dhcp snooping max-entry 100
Router(config-if-Giga1/1)# end
Router# show ip dhcp snooping interface
```

Interface	Trust State	Max Entry
Giga1/1	Trusted	100

DHCP Snooping Entry Time Configuration

To set the time restoring a DHCP Snooping binding entry that is not invalid (not in use of an IP address), use the following command:

Table 106 DHCP Snooping Entry Time Configuration

Command	Description
ip dhcp snooping entry-time <5-65535>	Sets the time for an Invalid DHCP Snooping Binding Entry (not in use of an IP address) to be stored. The time is set in minutes. By default, entry time is 14400 minutes (10 days).

The following example shows how to set entry time DHCP Snooping with 10 seconds:

```
Router# configure terminal
Router(config)# ip dhcp snooping entry-time 10
Router(config)# exit
Router# show ip dhcp snooping
Router DHCP Snooping is enabled
Invalid entry keep time: 10 mins
DHCP Packet rate-limit per client: 100 pps
Verification of hwaddr field is enabled
Insertion of option 82 is enabled [keep]
DHCP snooping is configured on following VLANs:
vlan1
```

DHCP Snooping Rate-Limit Configuration

To set the rate-limit of the DHCP packet from the same DHCP client, use the following command:

Table 107 DHCP Snooping Rate-Limit Configuration

Command	Description
ip dhcp snooping rate-limit	Sets the number of DHCP Packets, which are the same type, to be accepted sent from the same DHCP client per second. By default, it accepts two packets per second.

The following example shows how to set DHCP Snooping rate-limit with 100:

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

DHCP Snooping Verify MAC-Address Configuration

To drop a packet whose DHCP client Identifier or Client HW Address has changed, use the following command:

Table 108 DHCP Snooping Verify MAC-Address Configuration

Command	Description
ip dhcp snooping verify mac-address	Drops the packet whose DHCP client Identifier or Client HW Address has been changed. By default, this is enabled.

The following example shows how to disable DHCP Snooping Verify Mac-Address:

```
Router# configure terminal
Router(config)# no ip dhcp snooping verify mac-address
Router(config)# exit
Router# show ip dhcp snooping
Router DHCP Snooping is enabled
Invalid entry keep time: 10 mins
```

DHCP Packet rate-limit per client: 100 pps
Verification of hwaddr field is disabled
Insertion of option 82 is enabled [keep]
DHCP snooping is configured on following VLANs:
vlan1

DHCP Snooping Manual Binding Configuration

To set DHCP Snooping Binding Entry manually, use the following command:

Table 109 DHCP Snooping Manual Binding Configuration

Command	Description
ip dhcp snooping binding <i>H.H.H</i> VLAN <1-4094> <i>A.B.C.D</i> interface <i>IFNAME</i>	Assigns IP A.B.C.D to a DHCP client whose MAC address is H.H.H in the assigned interface. Lease time is infinite.

The following example shows the subscriber who has MAC address 1111.2222.3333 uses IP 100.0.0.10 connected with gi 1/1 of VLAN 1.

```
Router# configure terminal
Router(config)# ip dhcp snooping binding 1111.2222.3333 VLAN 1 100.0.0.10 interface gi1/1
Router(config)# exit
Router#
Router#
Router# show ip dhcp snooping binding
State Codes: © - Invalid Client Identifier, (E) - Lease Time Expired
              (H) - Invalid Client HW Address, ® - Rate Limit Dropped
              (M) - Mac Validation Check Dropped
```

Mac Address	IP Address	State	Lease(sec)	interface
1111.2222.3333	100.0.0.10	Manual	Infinite	Giga1/1
total 4 bindings found				

DHCP server Monitoring and Management

DHCP server Pool Information Inquiry

To inquire DHCP address pool information in DHCP server, use the following command in the privileged EXEC mode:

Table 110 DHCP server Pool Information Inquiry

Command	Description
show ip dhcp pool	Shows the DHCP address of the DHCP server information.
show ip dhcp pool [pool_name]	Shows network pool information of the DHCP server.

DHCP Server Binding Information Search

To search the binding information of addresses provided by the DHCP server to the client, use the following command in privileged EXEC mode:

Table 111 DHCP Server Binding Information Search

Command	Purpose
show ip dhcp binding	Displays all bindings on DHCP server.
show ip dhcp binding detail	Displays all bindings on DHCP server in more detailed format

DHCP Server Statistics Search

Table 112 DHCP Server Statistics Search

Command	Purpose
show ip dhcp server statistics	Displays the statistics of the server and the information of counters of sent/ received messages.

DHCP Server Conflict Search

Table 113 DHCP Server Conflict Search

Command	Purpose
show ip dhcp conflict {poolname}	Displays all address conflicts recorded in the DHCP server.

DHCP Server Variables Initialization Command

Table 114 DHCP Server Variables Initialization Command

Command	Purpose
clear ip dhcp binding {address *}	Deletes the automatic address binding function from the DHCP database. When you specify an address it will automatically bind of the specified address; when you use "*" it will delete all automatic bindings.
clear ip dhcp server statistics	Initializes all statistic counters of the DHCP server

DHCP relay Monitoring and Control

Table 115 DHCP relay Monitoring and Control Command

Command	Description
show ip dhcp helper-address	Shows the DHCP server list
show ip dhcp relay information option	Enables DHCP relay agent information option and shows reforwarding policy
show ip dhcp relay statistics	Shows relay statistics and counted information of received messages
debug ip dhcp relay {events packets:pal}	Enables debugging of DHCP relay

DHCP Snooping Monitoring and Control

Table 116 Showing DHCP Snooping and Control

Command	Description
show ip dhcp snooping	Shows global DHCP Snooping configuration
show ip dhcp snooping binding {IFNAME invalid manual VLAN}	Shows DHCP Snooping binding entry
show ip dhcp snooping interface	Shows DHCP Snooping configuration to interface.
show ip dhcp snooping statistics	Shows DHCP Snooping statistica; information.
show debugging ip dhcp snooping	Shows DHCP Snooping debugging.
debug ip dhcp snooping	Enables DHCP Snooping debugging function.

DHCP Configuration Examples

This section provides examples as follows:

- DHCP network pool configuration example
- DHCP host pool configuration example
- DHCP server monitoring and management example
- DHCP relay agent configuration example
- DHCP relay agent monitoring and management example

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 one 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.

```
Router(config)# configure terminal
Router(config)# ip dhcp pool marketing
Router(config-dhcp)# domain-name ubiQuoss.com
Router(config-dhcp)# lease 1 0 0
Router(config-dhcp)# network 192.168.1.0/24
Router(config-dhcp)# default-router 192.168.1.1
Router(config-dhcp)# range 192.168.1.10 192.168.1.100
Router(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 and 192.168.3.0/24 network. The default-router of 192.168.2.0/24 network is 192.168.2.1 and the address range is 192.168.2.10~192.168.2.240. 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. Each client is guaranteed up to 12 hours of IP address lease.

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

Example of DHCP Host Pool Configuration

The following shows an example of the host pool configuration in 192.168.4.0/24 network. The default-router is 192.168.4.1 and ubiQuoss.com is used as the domain name. This is host pool for clients using

192.168.4.10 and 192.168.4.11 as DNS-server. And, an IP address of 192.168.4.114 and netmask of 255.255.255.0 are allocated to the client whose MAC address is 00:01:02:94:77:d7.

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

```
Router(config)# ip dhcp pool mars
Router(config-dhcp)# default-router 192.168.4.1
Router(config-dhcp)# dns-server 192.168.4.10
Router(config-dhcp)# dns-server 192.168.4.11
Router(config-dhcp)# domain-name ubiQuoss.com
Router(config-dhcp)# host 192.168.4.114/13
Router(config-dhcp)# hardware-address 00:01:02:94:77:d7
Router(config-dhcp)# exit
```



Notice

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

DHCP server Monitoring and Control

The following example shows how to display DHCP address pool on the DHCP server:

```
shu# show ip dhcp pool
Pool network :
  network: 44.1.1.0/24
  address range(s):
    add: 44.1.1.1 to 44.1.1.200
  lease <days:hours:minutes> <0:0:1>
  no domain is defined
  no dns-servers
  no default-routers

Pool host:
  host 3.1.1.1/24
  hardware Ethernet 11:11:11:11:11:11
  no domain is defined
  no dns-servers
  no default-routers
shu#
```



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 DHCP server assigned to the client:

```
Router# show ip dhcp binding
```

IP address	Hardware address	Lease expiration	Type
192.168.4.114	00:01:02:94:77:d7	Infinite	Manual
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 assigned to the client in detail:

```
Router(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 how to delete 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 another client).

```
Router(Config)# clear ip dhcp binding 192.168.3.10
Router(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 how to display the statistics of DHCP server:

Router# 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

DHCP relay agent Configuration

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

DHCP Client

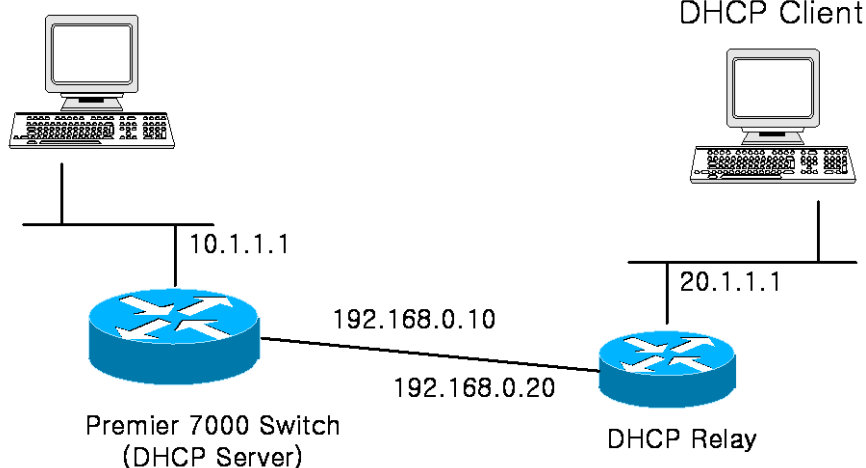


Figure 17. Network – DHCP Relay Agent Configuration

```

Router(config)# configure terminal
Router(config)# ip dhcp-server 10.1.1.2
Router(config)# service dhcp relay
Router (config)# end
Router# show ip dhcp helper-address
IP address      Interface
-----
10.1.1.2
  
```

```

Router #
Router # show ip dhcp relay statistics
  
```

```

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

```

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



Notice

To transfer a 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.

Item	Description
Client-packets relayed	Successfully done forwarding a packet sent from a DHCP client to DHCP server.
Client-packets errored	Failed to forward a packet sent from a DHCP client to DHCP server.

Server-packets relayed	Failed to forward a packet sent from a DHCP server to DHCP client.
Server-packets errored	Failed to forward a packet sent from a DHCP server to DHCP client.
Giaddr errored	A DHCP packet sent from a DHCP server does not have a giaddr.
Corrupt agent options	When the insertion function of the DHCP relay agent or DHCP information option of snoop is enabled, the Option82 of DHCP packet, sent from a DHCP server, has an error (The Length field and the actual DHCP Option82 Length are different).
Missing agent options	When the insertion function of a DHCP relay agent or DHCP information option of snoop is enabled, the DHCP packet sent from a DHCP server does not have the information of Option82.
Bad circuit id	When the insertion function of a DHCP relay agent or DHCP information option of snoop is enabled, the circuit id (interface information of a member) from the information of DHCP packet Option82, sent from a DHCP server, has an error. (The port corresponding to the circuit id cannot be found by using the circuit id of option82 in a DHCP packet.)
Missing circuit id	When the insertion function of a DHCP relay agent or DHCP information option of snoop is enabled, the circuit id (interface information of a member) from the information of DHCP packet Option82, sent from a DHCP server, has an missing. (The port corresponding to the circuit id cannot be found by using the circuit id of option82 in a DHCP packet.)

DHCP Snooping Configuration

The following example shows how to use U9016B as a DHCP Snoop located in between a DHCP Server and DHCP Client. The system DHCP Snoop generates a DHCP Snooping Binding Entry by Snooping the DHCP packet passing by the switch. The following example shows that the DHCP Client (0000.864a.c185), connected to the gi1/1 port, receives the IP 100.0.0.100 after sending a DHCP Request packet to the DHCP Server 100.0.0.254.

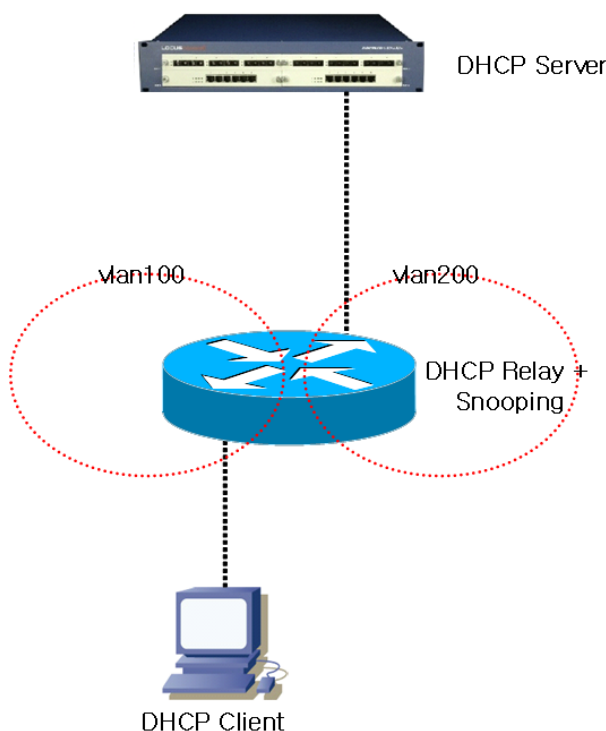


Figure 18. DHCP Snooping Configuration

```
Router# configure terminal
Router(config)# ip dhcp snooping VLAN 100
Router(config)# ip dhcp snooping VLAN 200
Router(config)# ip dhcp snooping
Router(config)# ip dhcp-server 100.0.0.254
Router(config)# service dhcp relay
Router# show ip dhcp snooping binding
State Codes: © - Invalid Client Identifier, (E) - Lease Time Expired
              (H) - Invalid Client HW Address, (D) - Rate Limit Dropped
```

MacAddress	IpAddress	State	Lease(sec)	VlanId	Port
0000.864a.c185	100.0.0.100	Ack	87	100	Giga1/1

Functions and Configuration of DHCPv6 Relay

DHCPv6 Relay Function Overview

DHCPv6 Relay is a protocol that relays the DHCPv6 from the network where the DHCPv6 server does not exist to one or more DHCPv6 servers on the other network.

The following steps show that U9016B ONU, as a DHCPv6 Relay Agent, sends the IP request message from the DHCPv6 client to the DHCPv6 server:

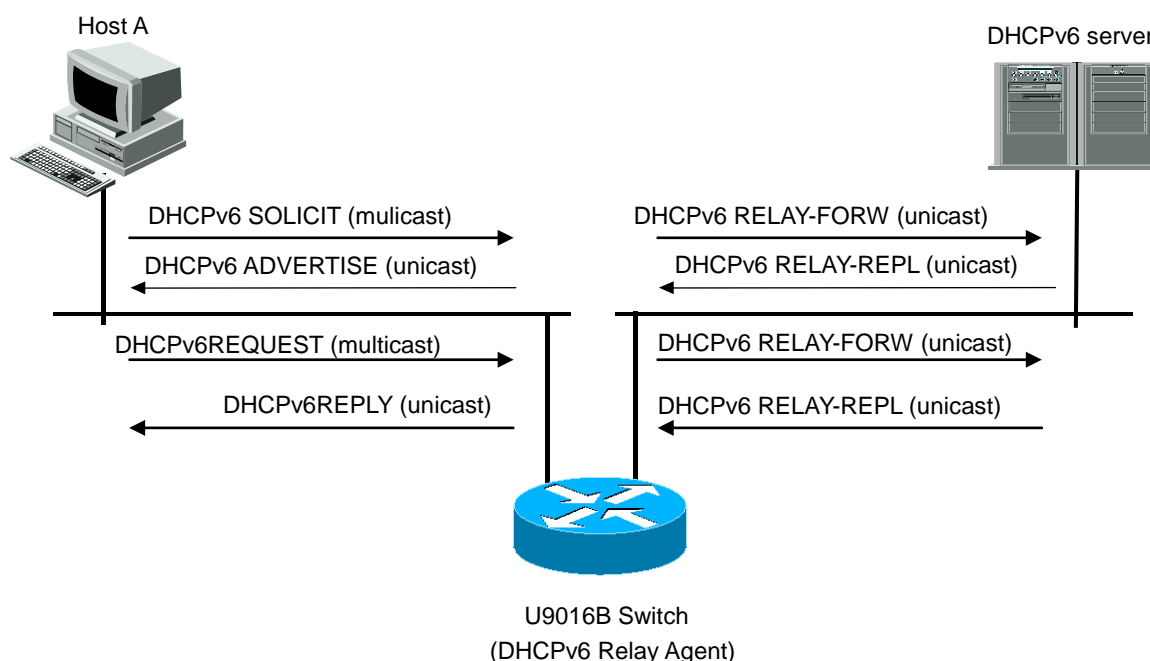


Figure 19. DHCPv6 Relay Agent sends a message to DHCPv6 Server

1. The DHCPv6 client multicasts the DHCPv6 Solicit message to request for an IP.
2. The DHCPv6 Relay Agent receives the DHCPv6 client message requesting for an IP. Then it writes the DHCPv6 RELAY-Forw message including the DHCPv6 Solicit message and then unicasts the message to the DHCPv6 server.
3. The DHCPv6 server receives the message from the DHCPv6 Relay Agent. Then it writes the DHCPv6 RELAY-REPL message including the DHCPv6 Advertise with information on the IP address and the default router and then unicasts the message to the DHCPv6 Relay Agent.
4. The DHCPv6 Relay Agent receives the DHCPv6 RELAY-Repl message. Then it unicasts the DHCPv6 Advertisement message included in the received message to the client.
5. The DHCPv6 Request and the DHCPv6 Reply between the DHCPv6 server and the client are sent to the DHCPv6 Relay Agent in the same way.

Configuring DHCPv6 Relay Agent

When U9016B is used as a DHCPv6 Relay Agent, it relays the DHCPv6 request from the DHCPv6 client to the specified DHCPv6 server.

Enabling U9016B DHCPv6 Relay Function

By default, the DHCPv6 relay function in the switch is disabled. The following table shows how to enable DHCPv6 relay function by using the following commands in global configuration mode:

Table 117. Enabling U9016B DHCPv6 Relay Function

Command	Description
service ipv6 dhcp-relay	Enables U9016B DHCPv6 relay function. To disable the DHCPv6 relay function, use No-type of this command.

The following example shows how to enable the DHCPv6 relay function.

```
Switch# configure terminal
Switch (config)# service ipv6 dhcp-relay
Switch (config)# exit
```

Setting Outgoing Interface on DHCPv6 Relay Agent

The following table shows how to set the outgoing interface on the DHCPv6 relay agent to forward the DHCPv6 message. The outgoing interface is set by global, interface, and destination. The priority is in the order of destination, interface, and global.

Table 118. Setting Outgoing Interface on DHCPv6 Relay Agent

Command	Description
ipv6 dhcp relay source-interface IFNAME	Sets the outgoing interface in global configuration mode and the interface mode. To delete the DHCPv6 server, use No -type of this command

The following example shows how to specify the server address from the DHCPv6 relay agent:

```
Switch# configure terminal
Switch (config)# ipv6 dhcp source-interface vlan50
Switch (config)# interface vlan100
Switch (config-if-vlan100)# ipv6 dhcp relay source-interface vlan100
Switch (config-if-vlan100)# end
```

Setting Server from DHCPv6 Relay Agent

To set the DHCPv6 server from the DHCPv6 relay agent, use the following command in Interface mode.

Table 119. Setting Server from DHCPv6 Relay Agent

Command	Description
ipv6 dhcp relay destination X::X:X [IFNAME]	Sets the IP address of the DHCPv6 server used when the DHCPv6 relay agent relays the DHCPv6 request packet. (Optional) To specify the outgoing interface per destination by entering IFNAME. To delete the DHCPv6 server, use No -type of this command

**Notice**

U9016B DHCPv6 relay agent allows 100 destinations per interface.

The following example shows how to specify the server address from the DHCPv6 relay agent:

```
Switch# configure terminal
Switch (config)# interface vlan100
Switch (config-if-vlan100)# ipv6 dhcp relay destination 3ffe:501:ffff:100::ffe vlan50
Switch (config-if-vlan100)# end
Switch#
```

Monitoring and Managing DHCPv6 Relay

Table 120. Commands to Monitor and Manage DHCPv6 Relay

Command	Description
show ipv6 dhcp relay statistics	Shows the counter related to the relay statistics and the transmitted messages.
debug ipv6 dhcp relay on	Enables DHCPv6 relay debugging.
no debug ipv6 dhcp relay on	Disables DHCPv6 relay debugging.

Examples of Configuring DHCPv6 Relay

This section provides following examples, describing how to configure the DHCPv6 relay agent, including:

Examples of configuring DHCPv6 Relay Agent
Examples of monitoring and managing DHCPv6 Relay Agent

The following example shows how the DHCPv6 relay agent of the switch relays the client DHCPv6 request packet to the DHCPv6 server.

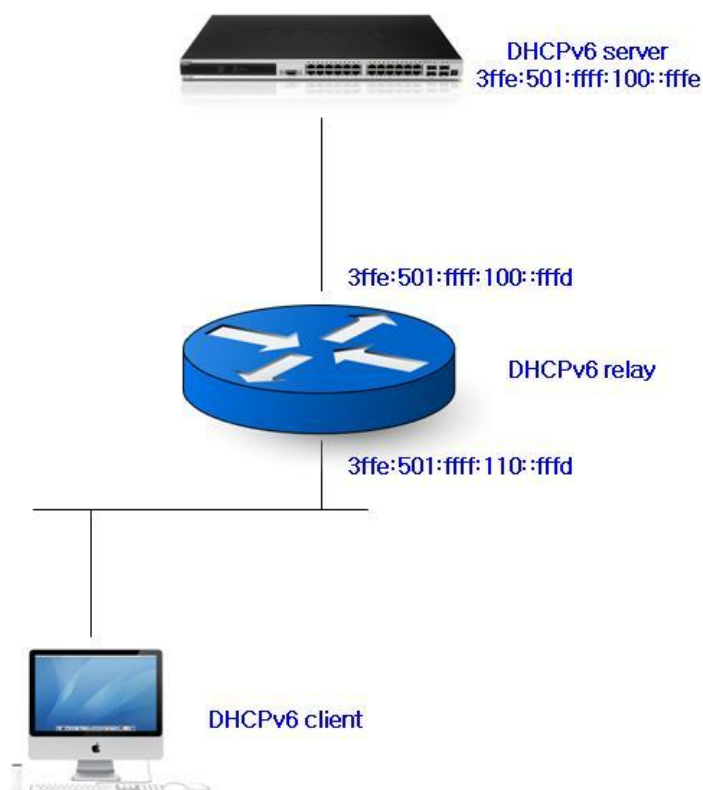


Figure 20. Example Network – Configuring DHCPv6 Relay Agent

```

Switch (config)# configure terminal
Switch (config)# interface vlan100
Switch (config-vlan100)# ipv6 dhcp relay destination 3ffe:501:ffff:100::ffe
Switch (config)# end
Switch#
  
```

Switch # show ipv6 dhcp relay statistics

```

<Client-packet relay>      Count
Client-packets relayed      8
Client-packets errors      0
  Invalid MSG Type          0
  HOP count exceed          0
  Unknown Interface         0

<Server-packet relay>      Count
Server-packets relayed      6
Server-packets errors      0
  Invalid MSG               0
  Invalid MSG Type          0
  
```

Out Interface not found 0

Table 121. Description on Input Message

Client-packets relayed	Succeeded in forwarding the packet received from the client to the server
Client-packets errors	Failed in forwarding the packet received from the client to the server
Server-packets relayed	Succeeded in forwarding the packet received from the server to the client
Server-packets errors	Failed in forwarding the packet received from the server to the client
Client Invalid msg type	When the type of a message sent from the client is the type except solicit, request, confirm, renew, rebind, release, decline, information-request, relay-forw, or lease-query
Server Invalid msg	When the relay-repl message sent by the server does not include the RELAY_MSG option
Server Invalid msg type	When the type of a message included in the relay-repl message is the type except advertise, reply, reconfigure, or leasequery-reply
Unknown Interface	When there is no information on the interface which has received the message from the client
Hop count exceed	When the hop count of the message from the client is 32 or more
Out Interface not found	When there is no information on the interface which will receive the message included in the relay-repl sent by the server

Chapter 9. IGMP Snooping

This chapter introduces IGMP Snooping Configuration.

IGMP Snooping Overview

Multicast traffic is processed as an 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 interface.

The procedure of IGMP Snooping in brief is as follows:

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

IGMP Snooping Configuration

IGMP Snooping operates in a global configuration.

Enable IGMP Snooping on a VLAN

To enable VLAN for IGMP Snooping, use the following command in the global configuration mode:

Table 122 Enable IGMP Snooping on a VLAN

Command	Description
ip igmp snooping	Enables IGMP Snooping of VLAN
no ip igmp snooping	Disables IGMP Snooping of VLAN

```
Router# configure terminal
Router(config)# interface vlan22
Router(config-if-Vlan22)# ip igmp snooping
Router(config-if-Vlan22)# end
Router# show ip igmp interface
.....
Interface Vlan22 (Index 2022)
  IGMP Enabled, Active, Non-Querier, Version 2 (default)
  Internet address is 220.1.1.222
  IGMP interface has 10 group-record states
  IGMP activity: 0 joins, 0 leaves
  IGMP querying router is 0.0.0.0
  IGMP query interval is 125 seconds
  IGMP querier timeout is 262 seconds
  IGMP max query response time is 25 seconds
  Last member query response interval is 1000 milliseconds
  Group Membership interval is 275 seconds
  IGMP Snooping is enabled on this interface
  IGMP Snooping fast-leave is not enabled
  IGMP Snooping querier is not enabled
  IGMP Snooping report suppression is enabled
.....
Router#
```

Enabling IGMP Snooping.

To configure the functionality of IGMP Snooping, use the following procedure.

IGMP Report-Suppression

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

To set IGMP Report-Suppression, use the following command in the interface configuration mode:

Table 123 IGMP Report-Suppression

Command	Description
ip igmp snooping report-suppression	Sets IGMP report-suppression to VLAN interface
no ip igmp snooping report-suppression	Disables the IGMP report-suppression of VLAN interface.

```
Router# configure terminal
Router(config)# interface vlan22
Router(config-if-Vlan22)# no ip igmp snooping report-suppression
Router(config-if-Vlan22)# end
Router# show ip igmp interface
```

```
.....
Interface Vlan22 (Index 2022)
  IGMP Enabled, Active, Non-Querier, Version 2 (default)
  Internet address is 220.1.1.222
  IGMP interface has 10 group-record states
  IGMP activity: 0 joins, 0 leaves
  IGMP querying router is 0.0.0.0
  IGMP query interval is 125 seconds
  IGMP querier timeout is 262 seconds
  IGMP max query response time is 25 seconds
  Last member query response interval is 1000 milliseconds
  Group Membership interval is 275 seconds
  IGMP Snooping is enabled on this interface
  IGMP Snooping fast-leave is not enabled
  IGMP Snooping querier is not enabled
  IGMP Snooping report suppression is disabled
```

```
.....
Router#
```

IGMP Fast-Leave

After enabling the fast-leave function of IGMP Snooping and receiving IGMPv2 Leave message from the host, delete the port in the forwarding table at once.

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

Table 124 IGMP Fast-Leave

Command	Description
ip igmp snooping fast-leave	Sets Fast-leave function to the specific VLAN
no ip igmp snooping fast-leave	Disables the Fast-leave function of the VLAN

```

Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface vlan22
Router(config-if-Vlan22)# ip igmp snooping fast-leave
Router(config-if-Vlan22)# end
Router# show ip igmp interface
.....
Interface Vlan22 (Index 2022)
  IGMP Enabled, Active, Non-Querier, Version 2 (default)
  Internet address is 220.1.1.222
  IGMP interface has 10 group-record states
  IGMP activity: 0 joins, 0 leaves
  IGMP querying router is 0.0.0.0
  IGMP query interval is 125 seconds
  IGMP querier timeout is 262 seconds
  IGMP max query response time is 25 seconds
  Last member query response interval is 1000 milliseconds
  Group Membership interval is 275 seconds
  IGMP Snooping is enabled on this interface
  IGMP Snooping fast-leave is enabled
  IGMP Snooping querier is not enabled
  IGMP Snooping report suppression is enabled
.....

```

Router#

IGMP Mrouter-Port

Multicast traffic and IGMP messages received from all member ports, excluding the Mrouter port in the VLAN interface, must be forwarded to the multicast router. Accordingly, the Mrouter port of the VLAN interface connected to the multicaster router is added to all multicast forwarding table entries as a traffic forwarding port.

In other words, IGMP snooping detects IGMP messages and the Mrouter port connected to the multicast router.

Whenever a new multicast forwarding table entry is created, the Mrouter port is always added as the traffic forwarding port, and the IGMP messages sent from the IGMP host are forwarded, as well as multicast traffic.

To set Multicast Router Port with static, use the following command in the interface configuration mode.

Table 125 IGMP Mrouter-Port

Command	Description
ip igmp snooping mrouter interface IFNAME	Sets Mrouter port manually. IFNAME should be a Member-Port in VLAN.
no ip igmp snooping mrouter interface IFNAME	Disables the Mrouter port of VLAN

```
Router# configure terminal
Router(config)# interface vlan22
Router(config-if-Vlan22)# ip igmp snooping mrouter interface gi2/5
Router(config-if-Vlan22)# end
Router# show ip igmp snooping mrouter vlan22
VLAN    Interface
22      Giga2/5
```

Router#

IGMP Access-Group

To set IGMP Access-Group, use the following command in the interface configuration mode:

Table 126 IGMP Access-Group

Command	Description
ip igmp snooping access-group <access-list>	Sets IGMP access group.
no ip igmp snooping access-group <access-list>	Disables IGMP access group.

```
Router# configure terminal
Router(config)# access-list 10 permit 225.1.1.1
Router(config)# access-list 10 deny any
Router(config)# interface gi1/2
Router(config-if-Giga1/2)# ip igmp snooping access-group 10
Router(config-if-Giga1/2)# end
Router#
Giga3/1/2)# end
Router#
```

In the case that relevant interface is the member of various VLAN interface, you can limit Multicast Group of IGMP Host only to a specific VLAN interface.

To limit Multicast Group of IGMP Host to a specific VLAN interface set IGMP access-group, use the following command in the interface configuration mode:

Table 127 Multicast Group of IGMP Host only to specific VLAN interface

Command	Description
ip igmp snooping access-group <access-list> VLAN <VLAN-id>	Limits multicast group of the IGMP host only to a specific VLAN interface.
no ip igmp snooping access-group <access-list> VLAN <VLAN-id>	Disables the setting.

```
Router# configure terminal
Router(config)# access-list 10 permit 225.1.1.1
Router(config)# access-list 10 deny any
Router(config)# interface gi1/2
Router(config-if-Giga1/2)# ip igmp snooping access-group 10 VLAN 22
Router(config-if-Giga1/2)# end
Router#
```

IGMP Group-Limit

IGMP Snooping can limit Multicast Group number per each interface.

To limit the multicast group number, use the following command in the interface configuration mode.

Table 128 IGMP Group-Limit

Command	Description
ip igmp snooping limit <count>	Limits multicast group number received to the relevant port.
ip igmp snooping limit <count> except <access-list>	Limits multicast group number received to the relevant port. In the case of no limitation of the group, designate with an access-list.
no ip igmp snooping limit <count>	Disables the setting.

```
Router# configure terminal
Router(config)# interface gi1/2
Router(config-if-Giga1/2)# ip igmp snooping limit 10
Router(config-if-Giga1/2)# end
Router#
```

In the case that the relevant interface is a member of the various VLAN interface, you can limit multicast group number to a specific VLAN interface only. To limit the multicast group number to a specific VLAN interface only, use the following command in the interface configuration mode:

Table 129 Multicast Group number only to specific VLAN interface

Command	Description
ip igmp snooping limit <count> VLAN <VLAN-id>	Limits multicast group received from relevant port

<i>id</i> >	to relevant VLAN.
ip igmp snooping limit <count> VLAN <VLAN-id> except <access-list>	Limits multicast group received from relevant port to relevant VLAN. In the case of no limitation Group, designate with an access-list.
no ip igmp snooping limit <count> VLAN <VLAN-id>	Disables multicast group number only to relevant VLAN interface.

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface gi1/2
Router(config-if-Giga1/2)# ip igmp snooping limit 10 VLAN 22
Router(config-if-Giga1/2)# end
Router#
```

Display System and Network Statistics

Table 130 IGMP Snooping-related Monitoring Command

Command	Description
show ip igmp snooping mrouter <IFNAME>	Displays Mrouter Port of VLAN
show ip igmp statistics	Displays the statistics of IGMP snooping

Chapter 10. Multicast Routing

This chapter describes IP multicast routing elements and IP multicast routing setting.

IP Multicast Routing Overview

IP Multicasting transmits packet in one host group with many IP hosts. This group includes a 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.

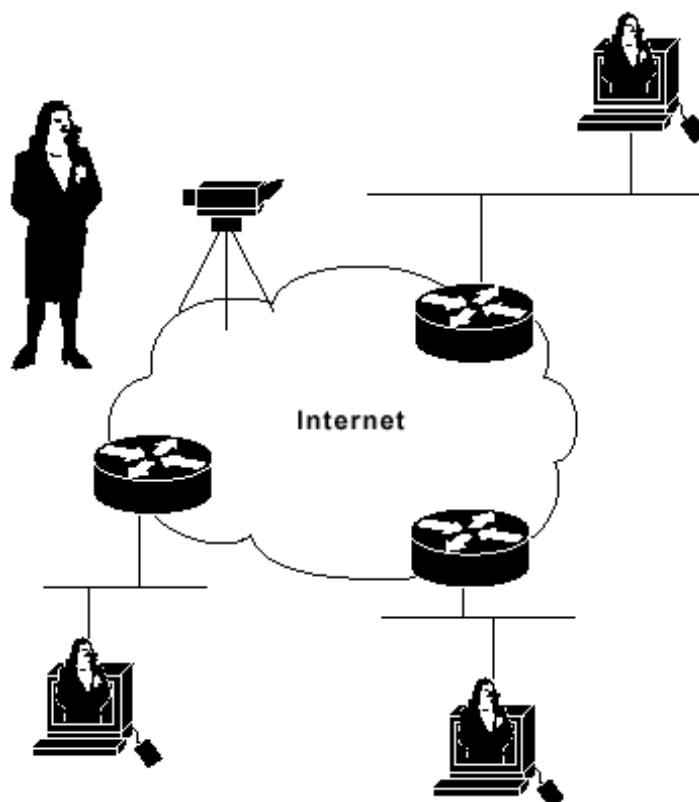


Figure 21. Multicasting to Transmit Traffic to Many Destinations

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. Table 125 below summarizes the requirements for each protocol unicast and flooding algorithm.

Table 131 Multicast Protocol

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

IGMP Proxy Overview

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

IP multicast uses Class D IP address for multicast group address. This is defined in RFC2236.

If IGMP (Internet Group Management Protocol) proxy receives the IGMP join/leave message from the host, it sends the IGMP join/leave message to the router instead of the host.

If it receives the IGMP query from the IGMP router, it transmits the IGMP query to the host instead of the router. In other words, it functions as IGMP router for the host and as IGMP host for IGMP router.

The limitation items when running IGMP Proxy configuration are as follows:

- Supports only IGMP v2. IGMP v3 is not supported and mutual setting is not acceptable.
- One upstream interface and the others of many downstream interfaces are set at first.
- You can not set PIM-SM setting on upstream or downstream interface after Proxy setting is done.
- Upstream interface setting use Proxy-Service and downstream interface use Mroute-Proxy.
- You can not IGMP Snooping on the interface set with Proxy-Service.

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 rendezvous point and then, to the recipient.

PIM-SM includes the following improvements of PIM-SM v1.

- Boot Router (BSR) supports fault-tolerant and automatic RP discovery and distribution mechanism and maps group-to-RP dynamically without setting.
- Flexible encoding about Address family of PIM Join/Prune message is available.
- PIM packet is not included in IGMP packet any more.

Many Candidate BSRs can be set in PIM domain to prevent Single point of failure, and BSR is monitored among the candidate BSR. The router informs the prior BSR with the Bootstrap message and monitored BSR notifies to all routers in PIM domain as BSR.

Router that is set as the Candidate RP informs the group range to BSR with the unicast. BSR includes this information in the Bootstrap message and transmits it to PIM message in the domain. So all router get RP information about the specific multicast group. To say, if the router gets the Bootstrap message, router has the current RP map.

MVLAN Overview

In multicast VLAN networks, subscribers to a multicast group can exist in more than one VLAN. If the VLAN boundary restrictions in a network consist of Layer 2 switches, it might be necessary to replicate the multicast stream to the same group in different subnets, even if they are on the same physical network. Multicast VLAN routes packets received in a multicast source VLAN to one or more received VLANs. Clients are in the received VLANs and the multicast server is in the source VLAN. Multicast routing has to be disabled when Multicast VLAN is enabled.

To use MVLAN on status set PIM-SM or IGMP Proxy, care should be taken when taken the necessary procedures set out below:

- You must set Multicast VLAN. After MVLAN setting, all OIF belongs to relevant VLAN.
- You set Local IP for VLAN interface of MVLAN and enable MVLAN function after MVIF is made.
- The using of MVLAN is useful when necessary of reducing resource in the environment that many outgoing interface need.
- You may use MVLAN when the system is L3 Multicast Routing environment.

IP Multicast Routing Configuration

Enable IP Multicast Routing

To forward multicast packet, IP multicast routing should be enabled basically. The following shows the commands in global configuration mode:

Table 132 Enable IP Multicast Routing

Command	Description
ip multicast-routing	Enables IGMP, IGMP Snooping, PIM-SM for Multicast Routing.
no ip multicast-routing	Disables IGMP, IGMP Snooping, PIM-SM for Multicast Routing.

```
Router# configure terminal
Router(config)# ip multicast-routing
Router(config)#
```

Enable IGMP and PIM on an interface

If PIM-SM protocol is enabled in the interface, IGMP querier functionality is also automatically enabled. To enable PIM, use the following command in interface configuration mode:

Table 133 Enable IGMP and PIM on an interface

Command	Description
ip pim sparse-mode	Enables PIM Sparse-Mode of the interface
no ip pim sparse-mode	Disables PIM Sparse-Mode of the interface

```
Router# configure terminal
Router(config)# interface vlan22
Router(config-if-Vlan22)# ip pim sparse-mode
Router(config-if-Vlan22)# end
Router# show ip pim sparse-mode interface
Address      Interface  VIFindex  Mode  Ver/  Nbr  Query  DR  DR
Count       Intvl  Prior
v2/S        0      30
2.1.1.1      Vlan22    0          2.1.1.1
Router#
Router# show ip igmp interface
Interface Vlan22 (Index 2022)
IGMP Active, Querier, Version 2 (default)
```

```

Internet address is 2.1.1.1
IGMP interface has 0 group-record states
IGMP activity: 0 joins, 0 leaves
IGMP query interval is 125 seconds
IGMP querier timeout is 262 seconds
IGMP max query response time is 25 seconds
Last member query response interval is 1000 milliseconds
Group Membership interval is 275 seconds
IGMP Snooping is not enabled on this interface
IGMP Snooping fast-leave is not enabled
IGMP Snooping querier is not enabled
IGMP Snooping report suppression is enabled
Router#

```

Configure Multicast Functionality

To configure features of Multicast, follow the steps below.

Router-Guard IP Multicast

Router-guard IP multicast blocks packets that can be generated at the multicast router among multicast control packets sent to the interface of the user's network; it then compiles statistics.

Router-guard IP multicast blocks multicast control packets as follows:

- IGMP Query Message
- PIM Message
- DVMRP Message

To set the router-guard IP multicast, use the following commands in the interface configuration mode.

Table 134 Router-Guard IP Multicast

Command	Description
router-guard ip multicast	Sets router-guard IP multicast in the corresponding interface.
router-guard ip multicast VLAN <1-4093>	Sets router-guard IP multicast only to specific members' interfaces of VLAN.
no router-guard ip multicast	Disables router-guard IP multicast of the interface.
no router-guard ip multicast VLAN <1-4093>	Sets router-guard IP multicast to specific members' interface of the VLAN.

```

Router# configure terminal
Router(config)# interface GigabitEthernet 1/3
Router(config-if-Giga1/3)# router-guard ip multicast
Router(config-if-Giga1/3)# interface GigabitEthernet 1/2
Router(config-if-Giga1/2)# router-guard ip multicast VLAN 22
Router(config-if-Giga1/2)# end
Router# show router-guard ip multicast

```

```

Globally enabled on interface gi1.3
Drop statistics
  IGMP Queries           : 0
  PIM Messages           : 0
  DVMRP Messages         : 0
  Invalid Messages       : 0

```

Enabled on interface gi1.2, vlan22

```
Drop statistics
  IGMP Queries      : 0
  PIM Messages     : 0
  DVMRP Messages   : 0
  Invalid Messages  : 0
Router#
```

Multicast Traffic Forwarding-TTL-Limit

Multicast traffic forwarding controlled at the multicast router diminishes one TTL transmitting multicast traffic, received from RPF interface, to downstream interface. When the diminished TTL is 0, it is dropped.

You can set the TTL of multicast traffic, forwarded from the multicast router, not to forward by setting a specific TTL value. Under this setting, when multicast traffic that has a TTL value of less than the specific value comes in from the RPF interface, it will not be forwarded. To prevent multicast traffic to be forwarded, you must apply TTL to the RPF interface.

To set the TTL of multi traffic forwarding, use the following commands in the interface configuration mode:

Table 135 Multicast Traffic Forwarding-TTL-Limit

Command	Description
ip multicast ttl-threshold <1-255>	Applies TTL restriction on multicast traffic
no ip multicast ttl-threshold	Disables the TTL restriction on multicast traffic

```
Router# configure terminal
Router(config)# interface GigabitEthernet 1/3
Router(config-if-Giga1/3)# ip multicast ttl-threshold 10
Router(config-if-Giga1/3)# end
```

Static Multicast Route Path

PIM operates based on the unicast routing table. However, depending on the network environment and router management, you can statistically apply multicast route path, which has the higher priority than unicast routing table, to the specific RP or source. The multicast route path is valid only in the PIM, and is always applied to in advance of the unicast routing path.

To set the static multicast route path, use the following commands in the global configuration mode:

Table 136 Static Multicast Route Path

Command	Description
ip mroute A.B.C.D/M [A.B.C.D bgp isis ospf rip static] A.B.C.D	Sets static multicast route path
no ip mroute A.B.C.D [bgp isis ospf rip static]	Disables assigned static multicast route path

```
Router# configure terminal
Router(config)# ip mroute 100.1.1.1/32 static 20.1.1.2
Router(config)# exit
Router#
```

Global Multicast Group-Limit

You can set the global multicast group range to allow or block the multicast traffic of specific groups. The global multicast group range simultaneously applies to all multicast protocols such as IGMP or PIM of a router.

To set the global multicast group range, use the following commands in the global configuration mode:

Table 137 Global Multicast Group-Limit

Command	Description
ip multicast group-range <i>access-list</i>	Sets a multicast group range
no ip multicast group-range	Disables the multicast group range

```
Router# configure terminal
Router(config)# access-list 20 permit 224.1.1.0 0.0.0.255
Router(config)# access-list 20 deny any
Router(config)# ip multicast group-range 20
Router(config)# exit
Router#
```

Multicast Load-Split

PIM Router can have more than one RPF interfaces with the same metric of SPT. For multiple RPF interfaces of a source, PIM selects an upstream interface and splits multicast traffic based on the hash value determined by the hash function of (S, G) entry. The load-split is different from the load-balance. Dealing with many multicast entries, each (S, G) entry has a RPF interface. So, it intensifies the RPF interface less than using only one interface, and increases the efficiency of network bandwidth.

To set the multicast load-split, use the following command in the global configuration mode:

Table 138 Multicast Load-Split

Command	Description
ip multicast multipath	Sets the multicast load-split
no ip multicast multipath	Disables the multicast load-split

```
Router# configure terminal
Router(config)# ip multicast multipath
Router(config)# exit
Router#
```

Multicast Route-Limit

Multicast router can limit the number of multicast routing entries in the system.

To set the number of multicast routing entries, use the following command in global configuration mode:

Table 139 Multicast Route-Limit

Command	Description
ip multicast route-limit <i><1-2147483647> [<1-2147483647>]</i>	Limits the number of multicast routing entry (Default : 1000)
no ip multicast route-limit	Disables the number of multicast routing entry

```
Router# configure terminal
Router(config)# ip multicast route-limit 10000 9000
Router(config)# exit
Router# show ip mroute sparse count

IP Multicast Statistics
Total 0 routes using 0 bytes memory
Route limit/Route threshold: 10000/9000
Total NOCACHE/WRONGVIF/WHOLEPKT rcv from fwd: 0/0/0
Total NOCACHE/WRONGVIF/WHOLEPKT sent to clients: 0/0/0
Immediate/Timed stat updates sent to clients: 0/0
Reg ACK rcv/Reg NACK rcv/Reg pkt sent: 0/0/0
Next stats poll: 00:00:19
Forwarding Counts: Pkt count/Byte count, Other Counts: Wrong If pkts
Fwd msg counts: WRONGVIF/WHOLEPKT rcv
Client msg counts: WRONGVIF/WHOLEPKT/Imm Stat/Timed Stat sent
Reg pkt counts: Reg ACK rcv/Reg NACK rcv/Reg pkt sent
Router#
```

Configuring IGMP Functionality

To configure IGMP features, follow the steps below.

IGMP Version

The IGMP version of IGMP querier, which operates by each network, works as the Default IGMPv2.

To change the IGMP Version, use the following command in the interface configuration mode:

Table 140 IGMP Version

Command	Description
ip igmp version <1-3>	Sets IGMP version of interface (Default: 2)
no ip igmp version	Sets the IGMP for default setting

```
Router# configure terminal
Router(config)# interface vlan22
Router(config-if-Vlan22)# ip igmp version 3
Router(config-if-Vlan22)# end
Router# show ip igmp interface
Interface Vlan22 (Index 2022)
IGMP Enabled, Active, Querier, Configured for version 3
Internet address is 2.1.1.1
IGMP interface has 0 group-record states
IGMP activity: 0 joins, 0 leaves
IGMP query interval is 125 seconds
IGMP querier timeout is 262 seconds
IGMP max query response time is 25 seconds
Last member query response interval is 1000 milliseconds
Group Membership interval is 275 seconds
IGMP Snooping is not enabled on this interface
IGMP Snooping fast-leave is not enabled
IGMP Snooping querier is not enabled
IGMP Snooping report suppression is enabled
Router#
```

IGMP Access-Group

Multicast router transmits IGMP host-query message to control multicast group that network hosts are in, and forwards packets to the member of this group. It can also configure a filter for each interface to limit the multicast group that subnets host by the interface.

To filter multicast group that interface permits, use the following command in the Interface configuration mode:

Table 141 IGMP Access-Group

Command	Description
ip igmp access-group <i>access-list</i>	Controls multicast group – subnet host that is serviced by the corresponding interface.
no ip igmp access-group	Disables multicast group – subnet host that is serviced by the corresponding interface.

```
Router# configure terminal
Router(config)# access-list 1 deny 225.1.1.0 0.0.0.255
Router(config)# interface GigabitEthernet 1/1
Router(config-if-Giga1/1)# ip igmp access-group 1
Router(config-if-Giga1/1)# end
```

IGMP Query-Interval

Multicast router sends a IGMP query message periodically for managing multicast membership.

To change IGMP query message interval, use the following command in interface configuration mode:

Table 142 IGMP Query-Interval

Command	Description
ip igmp query-interval <i><1-18000></i>	Sets igmp query-interval (Default: 125 seconds)
no ip igmp query-interval	Sets IGMP query interval as default.

```
Router# configure terminal
Router(config)# interface vlan22
Router(config-if-Vlan22)# ip igmp query-interval 60
Router(config-if-Vlan22)# end
Router# show ip igmp interface
Interface Vlan22 (Index 2022)
  IGMP Enabled, Active, Querier, Version 2 (default)
  Internet address is 2.1.1.1
  IGMP interface has 0 group-record states
  IGMP activity: 0 joins, 0 leaves
  IGMP query interval is 60 seconds
  IGMP querier timeout is 262 seconds
  IGMP max query response time is 25 seconds
  Last member query response interval is 1000 milliseconds
  Group Membership interval is 275 seconds
  IGMP Snooping is not enabled on this interface
  IGMP Snooping fast-leave is not enabled
  IGMP Snooping querier is not enabled
  IGMP Snooping report suppression is enabled
Router#
```


IGMP Last-Member-Query-Count

IGMP last-member-query-count assigns the number of occurrence of IGMP group-specific queries when finding another host of a multicast group by a IGMP querier.

To set IGMP last-member-query-count, use the following commands in interface configuration mode:

Table 143 IGMP Last-Member-Query-Count

Command	Description
ip igmp last-member-query-count <2-7>	Sets the number of occurrence of IGMP group-specific query (Default : 2 times)
no ip igmp last-member-query-count	Sets the number of occurrence for default

```
Router# configure terminal
Router(config)# interface GigabitEthernet vlan22
Router(config-if-Vlan22)# ip igmp last-member-query-count 3
Router(config-if-Vlan22)# end
```

IGMP Last-Member-Query-Interval

Last-member-query-interval is available with IGMPv2 and has a max response time for group-specific query messages from a IGMP querier, as a response to 'IGMP Leave' message. It is an interval for group-specific query message and the default is "1". This value is to control leave latency of network, and network can sense the last member existence of group faster with smaller value.

To set the interval, use the following commands in the interface configuration mode:

Table 144 IGMP Last-Member-Query-Interval

Command	Description
ip igmp last-member-query-interval <i><1000-25500></i>	Sets the IGMP last-member-query-interval (Default : 1000ms)
no ip igmp last-member-query-interval	Sets the IGMP last-member-query-interval for default

```
Router# configure terminal
Router(config)# interface GigabitEthernet vlan22
Router(config-if-GigaVlan22)# ip igmp last-member-query-interval 2000
Router(config-if-GigaVlan22)# end
Router# show ip igmp interface
Interface Vlan22 (Index 2022)
  IGMP Enabled, Active, Querier, Version 2 (default)
  Internet address is 2.1.1.1
  IGMP interface has 0 group-record states
  IGMP activity: 0 joins, 0 leaves
  IGMP query interval is 125 seconds
  IGMP querier timeout is 262 seconds
  IGMP max query response time is 25 seconds
  Last member query response interval is 2000 milliseconds
  Group Membership interval is 275 seconds
  IGMP Snooping is not enabled on this interface
  IGMP Snooping fast-leave is not enabled
  IGMP Snooping querier is not enabled
  IGMP Snooping report suppression is enabled
Router#
```

IGMP Immediate-Leave

Normally, a querier sends a group-specific or group-source-specific query message upon receipt of a leave message from a host. If you set a leave latency as 0 (zero), you can omit the querying procedure. When the querying procedure is omitted, the router immediately removes the interface from the IGMP cache for that group, and informs the multicast routing protocols.

To set the IGMP immediate-leave, use the following commands in the interface configuration mode:

Table 145 IGMP Immediate-Leave

Command	Description
ip igmp immediate-leave group-list <i>access-list</i>	Enables IGMP immediate-leave on relevant interface.
no ip igmp immediate-leave	Disables IGMP immediate-leave on the relevant interface.

```
Router# configure terminal
Router(config)# access-list 2 permit 225.1.1.0 0.0.0.255
Router(config)# interface vlan22
Router(config-if-Vlan22)# ip igmp immediate-leave group-list 2
```

```
Router(config-if-Vlan22)# end
```

IGMP Group Limit

You can use a IGMP group limit to limit the number of IGMP states that can be joined to a router on an interface or global level. Membership reports exceeding the configured limits are not entered into the IGMP cache and traffic for the excess membership reports is not forwarded.

To set the IGMP Group Limit, use the following command in the interface configuration mode:

Table 146 IGMP Group Limit

Command	Description
ip igmp limit <1-2097152>	Sets IGMP group limit on the relevant interface. (Default : unlimited)
no ip igmp limit	Disables IGMP group limit on the relevant interface.

```
Router# configure terminal
Router(config)# interface vlan22
Router(config-if-Vlan22)# ip igmp limit 100
Router(config-if-Vlan22)# end
```

IGMP Global Limit

To set the IGMP Global Limit, use the following commands in configuration mode:

Table 147 IGMP Global Limit

Command	Description
ip igmp limit <1-2097152>	Sets IGMP group limit to global (Default: unlimited)
no ip igmp limit	Disables the IGMP group limit set to global

```
Router# configure terminal
Router(config)# ip igmp limit 100
Router(config)# end
```

IGMP Minimum-Version

You can limit a version of IGMP message be received. In the case of setting IGMP minimum-version with 2, the received IGMPv1 message is limited and IGMPv2, IGMPv3 message is allowed. In the case of IGMPv3 message, decide processing or not by IGMP version of the set interface.

To set the IGMP minimum-version, use the following commands in interface configuration mode:

Table 148 IGMP Minimum-Version

Command	Description
ip igmp minimum-version <2/3>	Sets IGMP minimum-version to relevant interface.
no ip igmp minimum-version	Disables IGMP minimum-version.

```
Router# configure terminal
Router(config)# interface vlan22
Router(config-if-Vlan22)# ip igmp minimum-version 2
```

```
Router(config-if-Vlan22)# end
```

IGMP Querier-Timeout

There should be a single querier on a network segment to prevent duplicating multicast traffic for connected hosts. When there are several routers, if the router has the lowest IP address or if the router hears no queries during the timeout period, it becomes the querier.

To set the IGMP querier-timeout, use the following commands in the interface configuration mode:

Table 149 IGMP Querier-Timeout

Command	Description
ip igmp querier-timeout <60-300>	Sets IGMP querier timeout (Default : 262 seconds)
no ip igmp querier-timeout	Sets IGMP querier timeout to default

```
Router# configure terminal
Router(config)# interface vlan22
Router(config-if-Vlan22)# ip igmp querier-timeout 300
Router(config-if-Vlan22)# end
Router# show ip igmp interface
Interface Vlan22 (Index 2022)
  IGMP Enabled, Active, Querier, Version 2 (default)
  Internet address is 2.1.1.1
  IGMP interface has 0 group-record states
  IGMP activity: 0 joins, 0 leaves
  IGMP query interval is 125 seconds
  IGMP querier timeout is 300 seconds
  IGMP max query response time is 25 seconds
  Last member query response interval is 1000 milliseconds
  Group Membership interval is 275 seconds
  IGMP Snooping is not enabled on this interface
  IGMP Snooping fast-leave is not enabled
  IGMP Snooping querier is not enabled
  IGMP Snooping report suppression is enabled
Router#
```

IGMP Query-Max-Response-Time

In IGMP version 2 and 3, membership query messages include the maximum query response time field. This field specifies the maximum time allowed before sending a responding report. The maximum query response time allows a router to quickly detect that there are no more directly connected group members on a network segment.

To set the IGMP query max-response-time, use the following commands in the interface configuration mode.

Table 150 IGMP Query-Max-Response-Time

Command	Description
ip igmp query-max-response-time <1-240>	Designates max-response-time. (Default : 25 second)
no ip igmp query-max-response-time	Returns to default setting.

```
Router# configure terminal
Router(config)# interface vlan22
Router(config-if-Vlan22)# ip igmp query-max-response-time 10
Router(config-if-Vlan22)# end
Router# show ip igmp interface
Interface Vlan22 (Index 2022)
  IGMP Enabled, Active, Querier, Version 2 (default)
  Internet address is 2.1.1.1
  IGMP interface has 0 group-record states
  IGMP activity: 0 joins, 0 leaves
  IGMP query interval is 125 seconds
  IGMP querier timeout is 262 seconds
  IGMP max query response time is 10 seconds
  Last member query response interval is 1000 milliseconds
  Group Membership interval is 275 seconds
  IGMP Snooping is not enabled on this interface
  IGMP Snooping fast-leave is not enabled
  IGMP Snooping querier is not enabled
  IGMP Snooping report suppression is enabled
Router#
```

IGMP Rate

Multicast Router can limit PPS about IGMP packet incoming to CPU. IGMP packet over set IGMP rate drop from CPU.

To limit IGMP packet to PPS, use the following commands in the interface configuration mode.

Table 151 IGMP Rate

Command	Description
ip igmp rate <500-6000>	Sets the IGMP rate in pps units.
no ip igmp rate	Disables the IGMP rate.

```
Router# configure terminal
Router(config)# interface vlan22
Router(config-if-Vlan22)# ip igmp rate 100
Router(config-if-Vlan22)# end
Router# show ip igmp rate-limit statistics
```

```
IGMP Message Ratelimit (pps) for IP Multicast
Ifname      Incoming rate  Rate-limit  Permit  Drop    Rx-Total
-----+-----+-----+-----+-----+-----+
vlan22                0      100      0       0         0
Router#
```

IGMP Robustness-Variable

You can statically configure the querier's robustness variable (QRV) field in the membership query message for IGMP version 2 and 3. The QRV allows tuning for the expected packet loss on a network. If a network is expected to be lossy, the QRV value may be increased. When receiving the query message that contains a certain QRV value from a querier, a host returns the report message as many as the specified QRV value.

To set the IGMP Robustness-Variable, use the following commands in the interface configuration mode:

Table 152 IGMP Robustness-Variable

Command	Description
ip igmp robustness-variable <2-7>	Sets the IGMP robustness variable (Default: 2)
no ip igmp robustness-variable	Sets the IGMP robustness variable to default

```
Router# configure terminal
Router(config)# interface GigabitEthernet 2/1/1
Router(config-if-Giga2/1/1)# ip igmp robustness-variable 5
Router(config-if-Giga2/1/1)# end
```

IGMP Static-Group

When there are no more group members on a network segment or a host cannot report its group membership using IGMP, multicast traffic is no longer transmitted to the network segment. However, you may want to pull down multicast traffic to a network segment to reduce the time from when an IGMP join request is made to when the requested stream begins arriving at a host, which is called the *zapping time*.

The IGMP-Group reduces the zapping time by statically creating a virtual host that behaves like a real one on a port, even if there is no group member in the group where the port belongs. As a result, a multicast router realizes there is still group member, allowing multicast traffic to be permanently reachable on the group.

To set an IGMP Static-Group, use the IGMP Class-Map. To generate an IGMP Class-Map, use the following commands in the global configuration mode:

Table 153 IGMP Static-Group

Command	Description
class-map type multicast-flows <i>name</i>	Makes an IGMP class-map.
no class-map type multicast-flows	Deletes the IGMP class-map.

To set IGMP Class-Map, use the following command.

Table 154 IGMP Class-Map

Command	Description
group A.B.C.D	Assigns an IGMPv2 group (*, G).
group A.B.C.D source A.B.C.D	Assigns an IGMPv3 group and source (S, G).
group A.B.C.D to A.B.C.D	Assigns multiple IGMPv2 groups (*, Gn).

group <i>A.B.C.D to A.B.C.D source A.B.C.D</i>	Assigns multiple IGMPv3 groups and a source(S, Gn).
no group <i>A.B.C.D</i>	Deletes the assigned IGMPv2 group (*, G).
no group <i>A.B.C.D source A.B.C.D</i>	Deletes the assigned IGMPv3 and source (S, G).
no group <i>A.B.C.D to A.B.C.D</i>	Deletes the assigned multiple IGMPv2 groups (*, Gn).
no group <i>A.B.C.D to A.B.C.D source A.B.C.D</i>	Deletes the assigned multiple IGMPv3 groups and a source(S, Gn).

The source setting, assigned in IGMP class-map, is valid only in IGMPv3.

```
Router# configure terminal
Router(config)# class-map type multicast-flows igmp_static
Router(config-mcast-flows-cmap)# group 225.1.1.1 to 225.1.1.10
Router(config-mcast-flows-cmap)# group 225.1.2.1
Router(config-mcast-flows-cmap)# end
Router# show ip igmp static-group class-map
```

```
Class-map igmp_static
  description : -
    Group address range 225.1.1.1 to 225.1.1.10
    Group address 225.1.2.1
Router#
```

To set IGMP static-group, use the following command in interface configuration mode:

Table 155 IGMP Rate

Command	Description
ip igmp static-group <i>A.B.C.D</i>	Sets the IGMPv2 static-group not using the IGMP class-map.
ip igmp static-group <i>A.B.C.D interface IFNAME</i>	For the VLAN interface with enabled IGMP Snooping, it sets the member port of VLAN interface when setting IGMPv2 static-group.
ip igmp static-group <i>A.B.C.D source A.B.C.D</i>	Sets an IGMPv3 static-group not using the IGMP class-map.
ip igmp static-group <i>A.B.C.D source A.B.C.D interface IFNAME</i>	For the VLAN interface with IGMP Snooping enabled, it sets the member port of VLAN interface when setting IGMPv3 static-group.
ip igmp static-group class-map <i>name</i>	Sets a static-group based on the information of the assigned group in the IGMP class-map using IGMP class-map.
no ip igmp static-group <i>A.B.C.D</i>	Disables the IGMPv2 static-group.
no ip igmp static-group <i>A.B.C.D interface IFNAME</i>	Disables the IGMPv2 static-group that is set in the VLAN interface with enabled IGMP Snooping.
no ip igmp static-group <i>A.B.C.D source A.B.C.D</i>	Disables the IGMPv3 static-group.
no ip igmp static-group <i>A.B.C.D source A.B.C.D interface IFNAME</i>	Disables the IGMPv3 static-group that is set in the VLAN interface with enabled IGMP Snooping.
no ip igmp static-group class-map <i>name</i>	Disables the static-group of IGMP Class-Map.

```

Router# configure terminal
Router(config)# interface vlan22
Router(config-if-Vlan22)# ip igmp static-group igmp_static
Router(config-if-Vlan22)# end
Router# show ip igmp group
IGMP Connected Group Membership
Group Address      Interface      Uptime        ExpiresLast Reporter
225.1.1.1 Vlan22      00:01:42      static        0.0.0.0
225.1.1.2 Vlan22      00:01:42      static        0.0.0.0
225.1.1.3 Vlan22      00:01:42      static        0.0.0.0
225.1.1.4 Vlan22      00:01:42      static        0.0.0.0
225.1.1.5 Vlan22      00:01:42      static        0.0.0.0
225.1.1.6 Vlan22      00:01:42      static        0.0.0.0
225.1.1.7 Vlan22      00:01:42      static        0.0.0.0
225.1.1.8 Vlan22      00:01:42      static        0.0.0.0
225.1.1.9 Vlan22      00:01:42      static        0.0.0.0
225.1.1.10 Vlan22      00:01:42      static        0.0.0.0
225.1.2.1 Vlan22      00:01:42      static        0.0.0.0
Router# show ip igmp static-group class-map interface vlan22

Vlan22
Class-map attached : igmp_static
Group address range 225.1.1.1 to 225.1.1.10
Group address 225.1.2.1
Router#

```

IGMP SSM-MAP

The purpose of static SSM mapping is to provide SSM service on IGMPv1 and IGMPv2 messages. It means that it enables a multicast host to signal to a router which groups it wants to receive multicast traffic from, and from which sources this traffic is expected. You can specify a source address of multicast server to receive the multicast traffic from specified sources. If the system receives IGMPv1

or IGMPv2 report message from the host when static SSM mapping is enabled, it handles as if it receives IGMPv3 report messages.

By default, the PIM SSM is enabled. To disable the PIM SSM, use the following commands in the global configuration mode:

Table 156 IGMP SSM-MAP

Command	Description
no ip igmp ssm-map enable	Disables the SSM-MAP
ip igmp ssm-map enable	Enables SSM-MAP

```
Router# configure terminal
Router(config)# no ip igmp ssm-map enable
Router(config)# exit
Router# show ip igmp ssm-map
SSM Mapping : Disabled
Database    : None configured
Router#
Router# configure terminal
Router(config)# ip igmp ssm-map enable
Router(config)# exit
Router# show ip igmp ssm-map
SSM Mapping : Enabled
Database    : None configured
```

A group joined with IGMPv2 processes assigned source with mapping group assigned from database of IGMP SSM-MAP.

To generate database of IGMP SSM-Map, use the following commands in the global configuration mode:

Table 157 IGMP SSM-MAP

Command	Description
ip igmp ssm-map static access-list A.B.C.D	Adds ssm-map database using access-list.
no ip igmp ssm-map static access-list A.B.C.D	Deletes the added ssm-map database using access-list.

```
Router# configure terminal
Router(config)# access-list 20 permit 224.1.1.0 0.0.0.255
Router(config)# access-list 21 permit 224.1.3.0 0.0.0.255
Router(config)# ip igmp ssm-map static 20 179.1.1.200
Router(config)# ip igmp ssm-map static 21 179.1.1.201
Router(config)# exit
Router# show ip igmp ssm-map
SSM Mapping : Enabled
Database    : Static mappings configured
Router#
Router# show ip igmp ssm-map 224.1.1.1
Group address: 224.1.1.1
Database    : Static
Source list : 179.1.1.200
Router#
Router# show ip igmp ssm-map 224.1.2.1
```

Can't resolve 224.1.2.1 to source-mapping

```
Router#
Router# show ip igmp ssm-map 224.1.3.1
Group address: 224.1.3.1
Database      : Static
Source list   : 179.1.1.201
Router#
```

IGMP Proxy-Service

To enable IGMP Proxy service, you must set upstream in the Single Tree structure. The interface disperses traffic and works at the host side.

To set IGMP proxy-service, use the following commands in the interface mode:

Table 158 IGMP Proxy-Service

Command	Description
ip igmp proxy-service	Sets the selected interface for a proxy upstream interface.
no ip igmp proxy-service	Disables the setting of proxy upstream interface.

```
Router# configure terminal
Router(config)# interface vlan10
Router(config-if-Vlan10)# ip igmp proxy-service
```

```
Router# show ip igmp interface
Interface Vlan10 (Index 2010)
  IGMP Enabled, Active, Non-Querier, Version 2 (default) proxy-service
  IGMP host version 2
  Internet address is 10.0.1.114
  IGMP interface has 0 group-record states
  IGMP activity: 0 joins, 0 leaves
  IGMP querying router is 10.0.1.111
  IGMP query interval is 125 seconds
  IGMP querier timeout is 262 seconds
  IGMP max query response time is 25 seconds
  Last member query response interval is 1000 milliseconds
  Group Membership interval is 275 seconds
  IGMP Snooping is not enabled on this interface
  IGMP Snooping fast-leave is not enabled
  IGMP Snooping querier is not enabled
  IGMP Snooping report suppression is enabled
```

IGMP Mroute-Proxy

To do IGMP proxy service, the setting about downstream in single tree structure is needed. The relevant interface take part in role of router side like receiving report or sending query.

To set IGMP Mroute-proxy, use the following commands in the interface mode.

Table 159 IGMP Mroute-Proxy

Command	Description
ip igmp mroute-proxy IFNAME	Sets the interface as a proxy downstream interface. Enter upstream interface for IFNAME.
no ip igmp mroute-proxy	Disables the setting of proxy downstream interface.

```
Router# configure terminal
Router(config)# interface vlan30
Router(config-if-Vlan30)# ip igmp mroute-proxy vlan10
```

```
Router# show ip igmp interface
Interface Vlan30 (Index 2030)
  IGMP Enabled, Active, Version 2 (default)
  IGMP mroute-proxy interface is Vlan10
  IGMP interface has 0 group-record states
  IGMP activity: 0 joins, 0 leaves
  IGMP query interval is 125 seconds
  IGMP querier timeout is 262 seconds
  IGMP max query response time is 25 seconds
  Last member query response interval is 1000 milliseconds
  Group Membership interval is 275 seconds
  IGMP Snooping is not enabled on this interface
  IGMP Snooping fast-leave is not enabled
  IGMP Snooping querier is not enabled
  IGMP Snooping report suppression is enabled
```

Configuring MVLAN Functionality

When MVLAN is set, actually the displaying information of MFDB table is the same with previous display. By MVLAN MFDB, it runs internally and does not change externally.

Making MVLAN

To enable MVLAN, use the following commands in the VLAN database.

Table 160 PIM SSM

Command	Description
VLAN <i>vlanid</i> MVLAN	Makes a MVLAN id
no VLAN <i>vlanid</i>	Deletes the generated MVLAN id

```
Router# configure terminal
Router(config)# VLAN database
Router(config-VLAN)# VLAN 300 MVLAN
Router# show VLAN
```

VLAN Name	Status	Ports
1 default	active	
10 VLAN0010	active	
20 VLAN0020	active	
30 VLAN0030	active	
40 VLAN0040	active	
50 VLAN0050	active	
60 VLAN0060	active	
70 VLAN0070	active	
80 VLAN0080	active	
300 VLAN0300	active	Multicast VLAN

Enabling MVLAN

To generate an IP interface of a MVLAN ID, use the following commands.

The generated and enabled MLAN interface unifies all outgoing interfaces in the Internal MFWD and saves system resource.

You can set an IP address as a local address. To set MVLAN, use the following commands in the config mode:

Table 161 Enable MVLAN

Command	Description
ip MVLAN <i>Vlanid A.B.C.D/M</i>	Generates a MVLAN interface and enables it
no ip MVLAN	Deletes the MVLAN interface and disables it

```
Router(config)# ip MVLAN 300 182.1.2.3/24
```

MVLAN Status Information

To check the creation and status of activation of MVLAN, use the following commands:

Table 162 MVLAN Status Information

Command	Description
show ip MVLAN	Check configuration and status of MVLAN

```
Router# show ip MVLAN
IP Multicast Mvlan
Status      : Enabled
Mvlan Id    : 300
Mvlan Vif   : 7
Mvlan IP    : 180.1.2.3/24
```

Display System and Network Statistics

Table 163 Monitoring Commands of IP Multicast Routing

Command	Description
show ip igmp groups	Displays the multicast group that hosts are in.
show ip igmp interface	Displays the multicast-related information.
show ip igmp rate-limit statistics	Displays the statics of multicast packet of an interface with the rate-limit.
show ip igmp ssm-map	Displays configuration of ssm-map
show ip igmp static-group class-map	Displays the status of class-map to assign a static group.
show ip mcache	Displays the Routing cash of Multicast.
show ip mroute	Displays contents of the routing table of multicast.
show ip mvif	Displays the information of the multicast interface.
show ip pim sparse-mode anycast-rp	Displays the information of PIM anycast RP.
show ip pim bsr-router	Displays the information of BSR router.
show ip pim sparse-mode interface	Displays the information of an interface with PIM.
show ip pim sparse-mode local-members	Displays the information of PIM local membership.
show ip pim sparse-mode mroute	Displays contents of the routing table of multicast, managed by PIM.
show ip pim neighbor	Displays PIM neighbor.
show ip pim rp	Displays information of RP.
show ip pim rp-hash	Displays information of RP-HASH.

show ip rpf	Displays information of RPF.
show ip rpf event	Displays the information of received RPF events.

Chapter 11. Statistics Monitoring

This chapter describes the monitoring function for the system and statistics of U9016B OLT systems:

- System Status Monitoring
- Interface Statistics
- Logging setting
- RMON (Remote Monitoring)
- Setting threshold value

The Statistics that U9016B system provide help system administrator to grasp the current status of network operation quickly. If you pay attention to statistical data then you will be able to forecast future operations and prevent possible issues from arising.

Status Monitoring

The status monitoring provides information about U9016B. With show and its sub-commands, it provides status information, which will be displayed on your terminal screen.

Table 164 Status Monitoring Command

Command	Description	Mode
show logging	Displays the current snapshot of the log	Privileged
show memory usage	Shows the status of the system memory usage	Privileged
show cpu usage	Shows the current CPU usage	Privileged
show environment [cooling temperature status scu]	Displays status of the system, FAN, and temperature cooling: FAN information temperature: shows the temperature status: shows information of Power, FAN, Temperature scu: the current SCU voltage Information	Privileged
show version	Displays the version of the system	Privileged

System Threshold Configuration

You can set the threshold for the values of system module temperature, CPU and memory usage ratio. The threshold will have either upper limit or lower limit. If the value cross the limit it will induce syslog and SNMP trap.

Temperature Configuration

You can set the upper and lower thresholds of the temperature of the system.

Table 165 Temperature Configuration Command

Command	Description	Mode
temperature threshold <i>HIGHVAL LOWVAL</i>	Sets the threshold value for temperature. If the value cross the limit it will induce syslog and SNMP trap.	Config
show environment temperature	Displays current temperature and temperature threshold. In case FAN is available in the system, it also displays the status of FAN.	Privileged

The example below shows setting a threshold for the temperature of the system:

```
Switch# configure terminal
Switch(config)# temperature threshold 80 20
Switch(config)# exit
Switch# show environment temperature
```

```
Temperature   : 74.2 (°C)
Threshold     : High 80 (°C) Low 20 (°C)
```

CPU Usage Configuration

You can set the threshold for CPU usage ratio. If the value crosses the threshold the system will notify the violation by syslog and SNMP trap.

Table 166 CPU Usage Threshold Command

Command	Description	Mode
cpu usage threshold low <30-100> high <40-100>	Sets the threshold value for CPU usage ratio. If CPU usage ratio will rise above the threshold or go down below the threshold the system will produce syslog.	Config
cpu usage time-period (<300> <5> <60>)	Sets the reference value for CPU usage in terms of time.	Config
show cpu usage	Shows current CPU usage.	Privileged

Memory Usage Configuration

You can set the threshold for memory usage. If the remaining memory is lower than the threshold value the system will notify the violation by syslog and SNMP trap.

Table 167 Memory Usage Command

Command	Description	Mode
memory free low-watermark <10-70>	Sets the threshold value for the memory size to be kept. If the remaining memory is lower than the threshold or go up above the threshold again, the system will produce syslog.	Config
show memory usage	Shows current memory usage.	Privileged

Application Memory Usage Display

To show the memory related information which are used by individual applications, use the following command:

Table 168 Memory Display Command

Command	Description	Mode
show memory (bfd bgp imi mstp nsm ospf pimd rip)	Shows memory-related information used by individual applications.	Privileged

Port Statistics

U9016B system provides the statistics for individual ports of the system. To view the statistics, use the following commands.

```
show interface [ifname]
```

U9016B provides information of the port statistics as follows:

- **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.

The following shows a display of the port information including statistical data by the show interface command.

```
Switch# show interface GigabitEthernet 5/1
```

```
Giga5/1 is up, line protocol is up (connected)
Hardware is Ethernet, address is 0007.709e.2914 (bia 0007.709e.2914)
index 1111 metric 1 mtu 1500 arp ageing timeout 7200
Full-duplex, A-1000Mb/s, media type is 1000BaseLX
<UP,BROADCAST,RUNNING,MULTICAST>
VRF Binding: Not bound
Bandwidth 1g
inet 3.44.1.230/24 broadcast 3.44.1.255
VRRP Master of : VRRP is not configured on this interface.
Last clearing of "show interface" counters never
60 seconds input rate 88 bits/sec, 0 packets/sec
60 seconds output rate 72 bits/sec, 0 packets/sec
L2/L3 in Switched: ucast 30 pkt - mcast 20,532 pkt
L2/L3 out Switched: ucast 36 pkt - mcast 20,871 pkt
20,565 packets input, 1,782,898 bytes
Received 3 broadcast pkt (20,532 multicast pkt)
0 CRC, 0 oversized, 0 dropped
20,918 packets output, 1,790,946 bytes
0 collisions
0 late collisions, 0 deferred
```

Table 169 Commands for Port Statistics Check

Command	Description	Mode
show port counter [detail]	For the items below, it displays the accumulated	Privileged

	statistics of all the interfaces. I-Kbps/ O-Kbps InOctets/ OutOctets InPkts/ OutPkts	
show port statistics {all IFNAME}	For the items below, it displays the accumulated statistics of the interface by unit of 5 seconds/1 minute/5 minutes. TX: bits/s, pkts/s RX: bits/s, pkts/s	Privileged
show port statistics avg type [IFNAME]	For the items that are classified per traffic types, it displays the accumulated statistics of the interface by unit of 5 seconds/1 minute/5 minutes. TX: Unicast/Multicast/Broadcast s RX: Unicast/Multicast/Broadcast	Privileged
show port statistics interface [IFNAME]	For the items below, it displays the statistics of the interfaces. InOctets/ OutOctets InUcastPkts/ OutUcastPkts InMcastPkts/ OutMcastPkts InBcastPkts/ OutBcastPkts IfInDiscards IfInErrors	Privileged
show port-mib IFNAME	It displays current statistics and the accumulated statistics of the interface in detail.	Privileged
show interface counters	For the items below, it displays the accumulated statistics of the interface. InOctets/ OutOctets InUcastPkts/ OutUcastPkts InMcastPkts/ OutMcastPkts InBcastPkts/ OutBcastPkts	Privileged
show interface counters errors	It displays the accumulated errors of the interface.	Privileged

The following is the displayed content brought by show interface counter command, which shows the accumulated statistics of all the ports:

Router#show interface counters

Port	InOctets	InUcastPkts	InMcastPkts	InBcastPkts
Gi5/1	0	0	0	0
Gi5/2	0	0	0	0
Gi5/3	0	0	0	0
Gi5/4	0	0	0	0
Gi5/5	0	0	0	0
Gi5/6	0	0	0	0
Gi5/7	2,560	0	20	0
Gi5/8	2,560	0	20	0
Port	OutOctets	OutUcastPkts	OutMcastPkts	OutBcastPkts
Gi5/1	0	0	0	0
Gi5/2	0	0	0	0
Gi5/3	0	0	0	0
Gi5/4	0	0	0	0
Gi5/5	37,466	0	305	0
Gi5/6	37,220	0	303	0
Gi5/7	36,974	0	301	0
Gi5/8	36,605	0	298	0
Router#				

The following is the displayed content brought by show port statistics command, which shows the accumulated statistics of a port in the unit of 5 seconds/1 minute/5 minutes:

```
Router#show port statistics gi5/5
```

```
Last clearing of counters 00:14:24
```

```
=====
```

Port	TX		RX	
	bits/s	pkts/s	bits/s	pkts/s

Gi5/5				
5 sec.	392	0	0	0
1 min.	488	0	0	0
5 min.	488	0	0	0

```
=====
```

The statistics of any interface have an average value and accumulated value. By use of the following commands, you can change the interval time to which the system refer, when it calculates the average value. Also, by setting high and low threshold values toward any interface, you can monitor whether it works out fine or not for the set duration of time.

Table 170 Commands for Port Statistics Configuration

Command	Description	Mode
load-interval <i>interval</i>	Sets the interval value - the system updates the average statistics of the interface for the period of the interval.	interface
no load-interval	Returns the interval value to default one.	interface
input-load-monitor <i>interval</i> <i>low-threshold high-threshold</i>	It sets High and Low threshold values which will be effective for the period of interval so that you can monitor whether it crosses the threshold.	interface
no input-load-monitor	Clears the monitoring setting.	interface
show port input-load-monitor	Shows the current monitoring setting.	interface

You can use the following commands to initialize the accumulated statistic values.

Table 171 Command for Initialization of Port Statistic

Command	Description	Mode
clear counters	Initializes the accumulated statistic values of all the interfaces.	privileged
clear counters <i>IFNAME</i>	Initializes the accumulated statistic values of the specified interface.	privileged



Notice

For the statistics which are displayed toward SNMP, you cannot initialize them by using of clear counter command.

RMON (Remote MONitoring)

Using the Remote Monitoring (RMON) capabilities of U9016B allows network administrators to improve system efficiency and reduce the network load.

The following sections explain more about RMON and the features that U9016B supports.

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 keeps collecting statistics about a LAN segment or VLAN.
- The probe transfers the information to a management workstation upon 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.

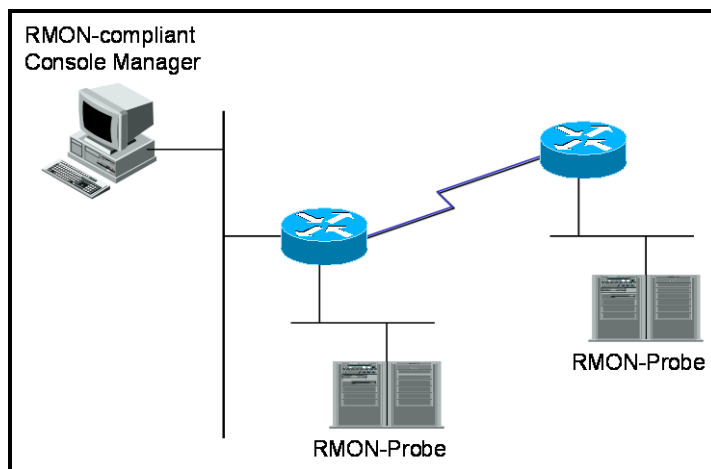


Figure 22. RMON Manager and RMON Probe

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 statistical data, history data, host-related data, host matrix and as well as the alarming function that warns when the threshold, which is set to predict and remove certain packets for filtering, is reached.

U9016B supports only statistics, history, alarm, and event groups among the nine RMON groups, as defined in Table 166. All the RMON functions are set as disabled by default.

Table 172 RMON Items

Item	Description
Statistics	Provides statistical 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	Provides information on the traffic and errors generated during the time span that the operation manager has set. Sets short-term/long-term time span and the interval is limited to 1-3,600 seconds. Displays of the usage by time and comparing the data with other segment data.
Alarm	Checks a particular value regularly and report to the manager when the value reaches the standard and the agent has its record. Sets 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	Finds 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	Collects 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 Configuration

The user can set RMON configuration through CLI or SNMP manager.

Table 173 Commands for RMON Alarm and Event Configuration

Command	Description	Mode
<code>rmon alarm index variable interval seconds {absolute delta} rising-threshold value event num falling-threshold value event num [owner string]</code>	Adds a RMON alarm to RMON alarm table <i>Index:</i> Alarm index <i>Variable:</i> As the target of Alarm, any SNMP mib instance is specified Interval: Sampling time period (Unit: second). Absolute: Indicates the sampled alarm value to be set and monitored as absolute value. Delta: Indicates the sampled alarm value to be monitored in terms of the difference between current and previous values. Rising-threshold, falling-threshold <i>value</i> : The configured value which is used as the reference while the system generates alarm. event: Indicates the specified event to be invoked when the sampled alarm value reaches either rising-threshold or falling-threshold. owner: Registers the owner of the alarm.	Config
<code>rmon event index [log] [trap community] [description string] [owner string]</code>	Adds an event to RMON event table <i>Index:</i> Event index. log: Sets the system to produce log when an Event happens. trap: Sets the system to transfer trap along with community when an Event happens. owner: Registers the owner of the Event. description: Registers the description about the Event.	Config
<code>no rmon alarm alarm-index</code>	Clears the setting of RMON alarm.	Config
<code>no rmon event event-index</code>	Clears the setting of RMON event.	Config
<code>show rmon alarms</code>	Prints out RMON alarm information.	Privileged
<code>show rmon events</code>	Prints out RMON event information.	Privileged

The following example demonstrates how to set rmon alarm with respect to GigabitEthernet 2/2. It shows that system will do sampling the inOctets value of GigabitEthernet 2/2 every 30 seconds and generate event whenever the value goes beyond the rising-threshold or under falling-threshold. When you set Rmon alarm you must set event or stats first.

```
Switch# configure terminal
Switch(config)# rmon event 1 log trap rmon_test description RisingAlarm
Switch(config)# rmon event 2 log trap rmon_test description FallingAlarm
Switch(config)# interface GigabitEthernet 2/2
Switch(config-if-Giga2/2)# rmon collection stats 1
Switch(config)# rmon alarm 1 etherStatsEntry.4.1158 interval 30 absolute rising-threshold
2000000 event 1 falling-threshold 1000000 event 2
Switch(config)# exit
Switch# show rmon alarm
Alarm 1 is active, owned by RMON_SNMP
Monitors etherStatsOctets.1158 every 30 second(s)
Taking Absolute samples, last value was 00
Rising threshold is 2000000, assigned to event 1
Falling threshold is 1000000, assigned to event 2
On startup enable rising or falling alarm alarmRisingThreshold : 15
alarmFallingThreshold : 0
alarmRisingEventIndex : 1
alarmFallingEventIndex : 1
alarmOwner : hong
Switch# show rmon event
```



```
event Index = 1
  Description RisingAlarm
  Event type Log & Trap
  Event community name rmon_test
  Last Time Sent = 5774:38:20
  Owner RMON_SNMP
```

```
event Index = 2
  Description FallingAlarm
  Event type Log & Trap
  Event community name rmon_test
  Last Time Sent = 00:00:00
  Owner RMON_SNMP
```

Switch# show rmon statistics

```
Collection 1 on Giga2/2 is active, and owned by RMON_SNMP,
Monitors ifEntry.1.1158 which has
Received 014354459 octets, 0195285 packets,
 03 broadcast and 021164 multicast packets,
 00 undersized and 00 oversized packets,
 00 fragments and 00 jabbers,
 00 CRC alignment errors and 00 collisions.
# of dropped packet events (due to lack of resources): 00
# of packets received of length (in octets):
64: 01585, 65-127: 0440336, 128-255: 0308
256-511: 04, 512-1023: 00, 1024-1518: 00
```

Table 174 Commands for RMON History Setting and Statistics

Command	Description	Mode
rmon collection stats <i>index</i> [owner <i>string</i>]	Collects the statistics of physical interface. <i>Index:</i> etherStats index	Interface
rmon collection history <i>index</i> [buckets <i>number</i>] [interval <i>seconds</i>] [owner <i>string</i>]	Collects the history of physical interface. <i>Index:</i> History index, buckets: The number of history, Interval: Collection period (Unit: second) owner: Registers the owner of the History.	Interface
no rmon collection stats <i>index</i>	Clears the setting so as not to collect the statistics of physical interface.	Interface
no rmon collection history <i>index</i>	Clears the setting so as not to collect the history of physical interface.	Interface
show rmon history	Prints out RMON history information.	Privileged
show rmon statistics	Prints out RMON statistics information.	Privileged
rmon clear counters	Initializes the statistics of the interface.	Interface

The following example shows how to set RMON with using maximum 30 numbers bucket per 10 seconds to gi 2/2

```
Switch# configure terminal
Switch(config)# interface GigabitEthernet 2/2
Switch(config-if-Giga2/2)# rmon collection stats 1
Switch(config-if-Giga2/2)# rmon collection history 1 buckets 30 interval 10
Switch(config-if-Giga2/2)# exit
Switch(config)#exit
Switch# show rmon history
Entry 1 is active, and owned by RMON_SNMP
Monitors ifIndex 1158 every 10 second(s)
Requested # of time intervals, ie buckets, is 30,
Sample # 1 began measuring   Received 14953616 octets, 203700 packets,
 3 broadcast and 21362 multicast packets,
 0 undersized and 0 oversized packets,
 0 fragments and 0 jabbers,
 0 CRC alignment errors and 0 collisions.
# of dropped packet events is 0
Sample # 2 began measuring   Received 14956451 octets, 203740 packets,
```

3 broadcast and 21363 multicast packets,
0 undersized and 0 oversized packets,
0 fragments and 0 jabbers,
0 CRC alignment errors and 0 collisions.
of dropped packet events is 0
Sample # 3 began measuring Received 14959509 octets, 203783 packets,
3 broadcast and 21364 multicast packets,
0 undersized and 0 oversized packets,
0 fragments and 0 jabbers,
0 CRC alignment errors and 0 collisions.
of dropped packet events is 0

Logging

U9016B log shows all information on configuration and alarms. 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 following:

- 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

U9016B 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.

U9016B has 0-7 severity levels as shown in the following table:

Table 175 U9016B Log Level

Severity Level	Description
Emergencies (0)	System is not available.
Alerts (1)	An Immediate action is required.
Critical (2)	Critical Status
Errors (3)	Error Message
Warnings (4)	Warning 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 U9016B contains 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.

Severity level

- Indicates the log message level defined in the < > as in Table 12.
- Integer between 1 and 7

Log description

- Text string including detailed information on event

The following is the log message for system booting:

```
May 6 11:53:48 [5] %REMOTE-CONNECT: login from console as Ins
May 6 11:54:01 [5] IFM-NOTICE: Rate limit ra creation
May 7 02:10:24 [5] %REMOTE-CONNECT: login from console as Ins
May 7 02:10:40 [5] IFM-NOTICE: Flow xx classified
May 7 02:10:48 [5] IFM-NOTICE: Flow xx match rate 10
May 7 05:17:56 [5] %REMOTE-CONNECT: login from console as Ins
May 7 05:23:10 [5] IFM-NOTICE: Service pa add interface fa1
```

Default Logging Value

Table 176 System Log Default

Configuration Parameter	Default
Display logging to console	disabled
Display logging to Telnet session	disabled
Logging buffer size	1MB
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	info (6)

Table 177 Commands for System Message Logging Configuration

Command	Description
logging console {<0-7> /alerts/critical/debugging/emergencies/errors/ informations/notifications/warnings}	Sets to print out the logging information toward console.
logging facility {auth/cron/daemon/kernel/local0/ local1/local2/local3/local4/local5/ local6/local7/lpr/mail/news/syslog/ user/uucp}	Sets the Facility parameter to which syslog messages are to be sent.
logging A.B.C.D	Sets to send syslog messages toward external syslog server.
logging monitor /alerts/critical/debugging/emergencies/errors/ informations/notifications/warnings}	Sets to print out the logging information toward current session.
logging source-ip A.B.C.D	Sets the source ip of syslog packet.
logging trap /alerts/critical/debugging/emergencies/errors/ informations/notifications/warnings}	Sets the logging level of syslog server.
show logging	Prints out logging buffer and its settings.

Examples of Logging Configuration

While accessing the console, if you want to have a log message with the log level notice (5) or below printed toward console, follow the example shown below. When you want to stop printing the log message toward console, use the no logging console command.

```
Switch# configure terminal
Switch(config)# logging console notifications
Switch(config)# end
Switch#
Switch# configure terminal
Switch(config)# no logging console
Switch(config)#
Switch#
Switch# configure terminal
Switch(config)# logging monitor warnings
Switch(config)# end
Switch#
Switch# configure terminal
Switch(config)# no logging session
Switch(config)#
```

While accessing via Telnet if you want to have the log message with log level warn (4) or below printed toward Telnet session, follow the example below. When you want to stop printing the log message toward Telnet session, use the logging session disable command.

```
Switch#
Switch# configure terminal
Switch(config)# logging monitor warnings
Switch(config)# end
Switch#
Switch# configure terminal
Switch(config)# no logging session
Switch(config)#
```

If you want to have the log message with Log level err (5) or below printed toward Log server 100.10.1.1, follow the example below. When you want to stop printing the toward log server, use the no logging A.B.C.D command. log message.

```
Switch# configure terminal
Switch(config)# logging 100.10.1.1
Switch(config)# logging trap errors
Switch(config)# end
Switch#
Switch# configure terminal
Switch(config)# no logging 100.10.1.1
Switch(config)#
```

sFlow

U9016B 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 U9016B. 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:

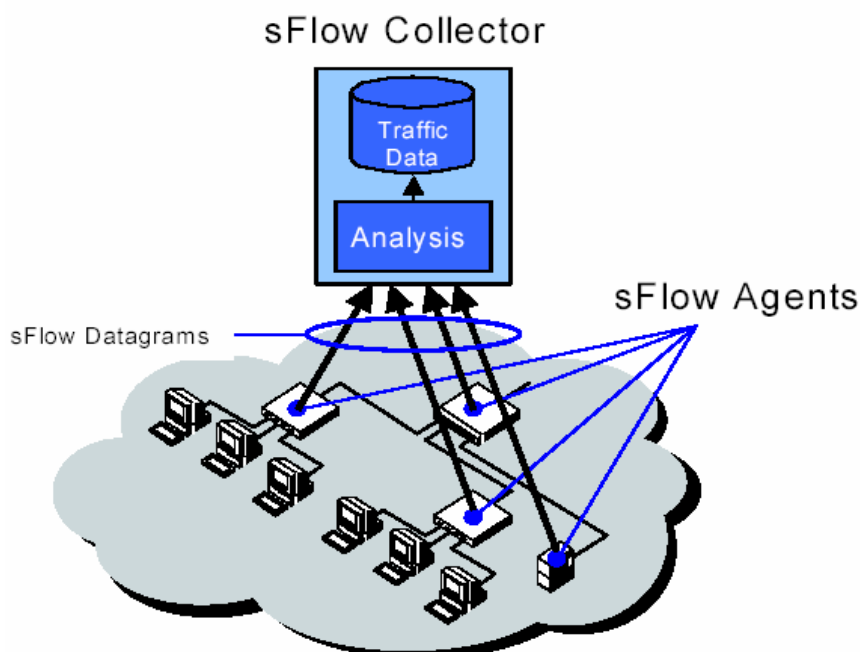


Figure 23 Key Map of sFlow (sFlow agent and collector)

sFlow Agent

This section introduces the function and commands for an sFlow agent. There are commands for setting the IP address of the 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. The flow sampling rate determines the number of packets which come through the interface before the system undertakes 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 the sFlow forward command, you can configure the physical interface (ex, gi1) for sampling upto maximum 4 interfaces. With the service sFlow command you can initiate the sFlow service.

Table 178 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 the 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 homepage <http://www.inmon.com/index.htm>. The following describes sflowtool and sFlowTrend setting.

sflowtool Configuration

1. You can show sFlow sampling packet in port 6343.with the following command:

```
[Ins:/home/Ins] 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 =====
```

- You can show sFlow sampling packet by line unit with the following command:

```
[Ins:/home/Ins] sflowtool -l
```

```
CNTR,10.0.0.254,17,6,100000000,0,2147483648,175283006,136405187,2578019,297011,0,3,0,0,0,0,0
```

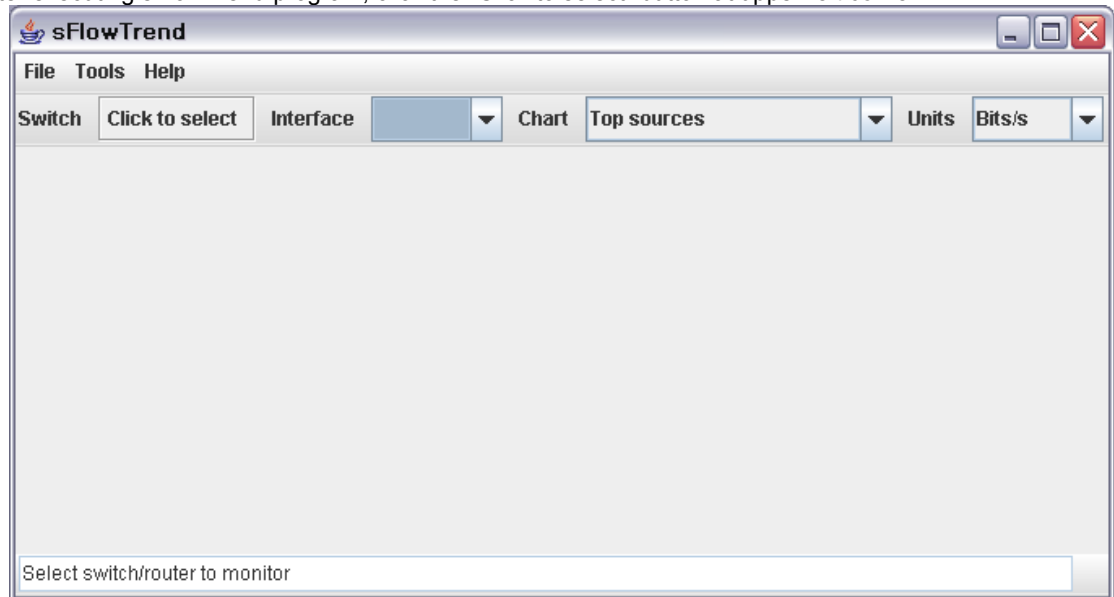
```
,0,0,1
```

```
FLOW,10.0.0.254,0,0,00902773db08,001083265e00,0x0800,0,0,10.0.0.1,10.0.0.254,17,0x00,64,3569
```

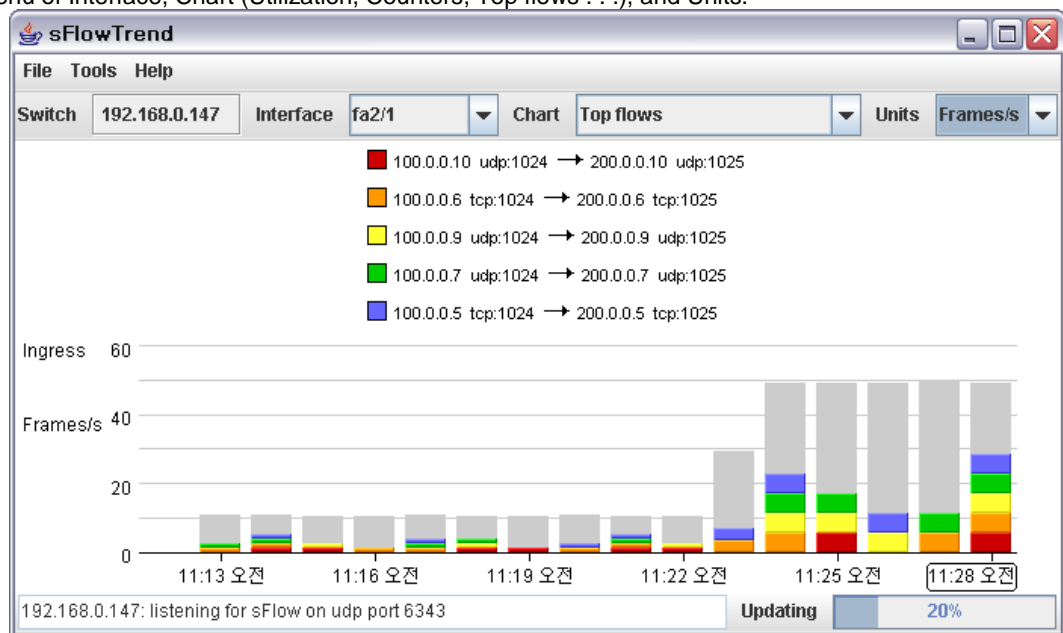
```
0,161,0x00,143,125,80
```

sFlowTrend Configuration

- After executing sFlowTrend program, click the "Click to select" button at upper-left corner.



- Type in the IP Address of sFlow Agent at the 'Select switch/router to monitor' dialog box.
- Once sFlowTrend has acquired sampling information, select the relevant option within the scroll down menu of Interface, Chart (Utilization, Counters, Top flows . . .), and Units.



sFlow Network Configuration

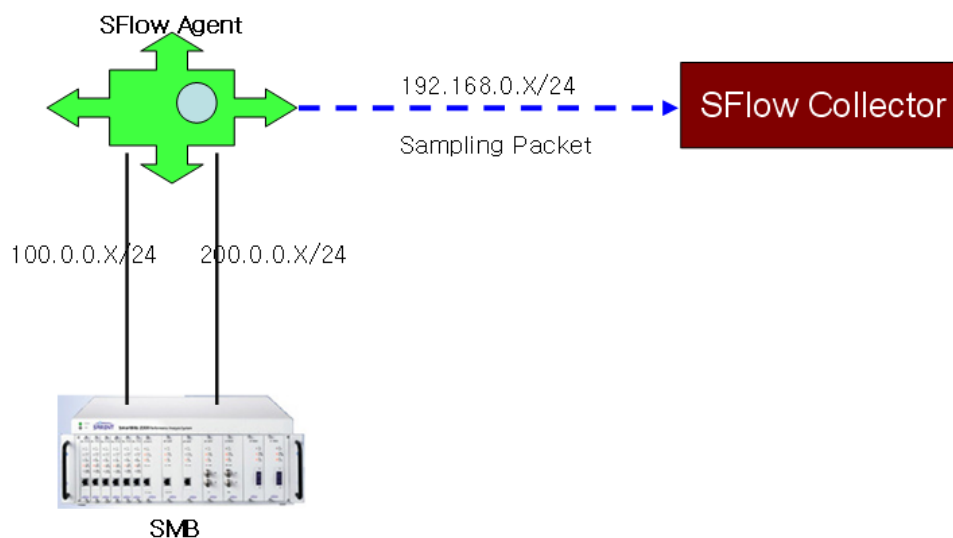


Figure 24. sFlow Network Configuration

sFlow Sampling Test

sFlow sampling has traffic flow sampling and interface statistics 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-Giga5/1)# sFlow forwarding
Switch(config-if-Giga5/1)# 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 there is traffic flow sampling and interface statistics sampling.

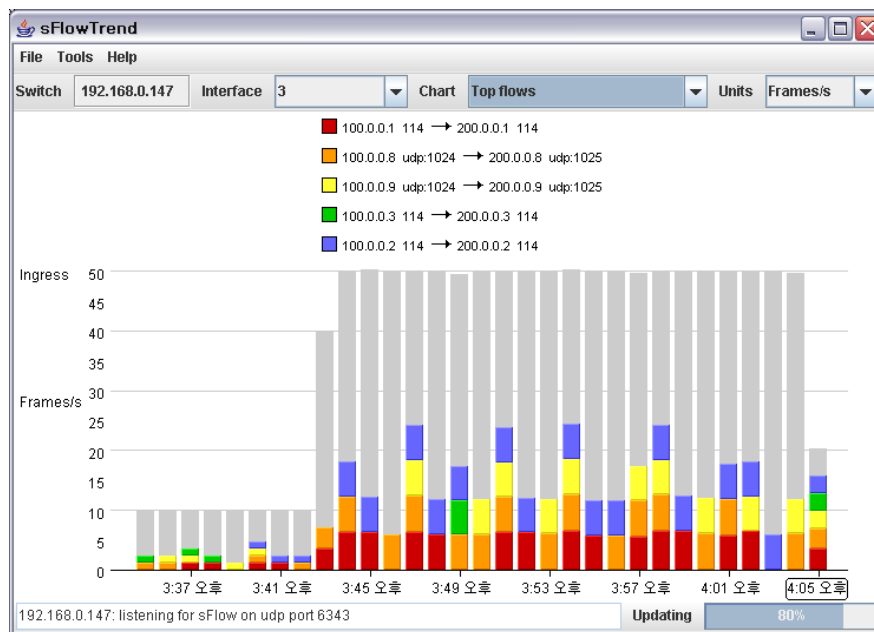


Figure 25. Traffic flow sampling

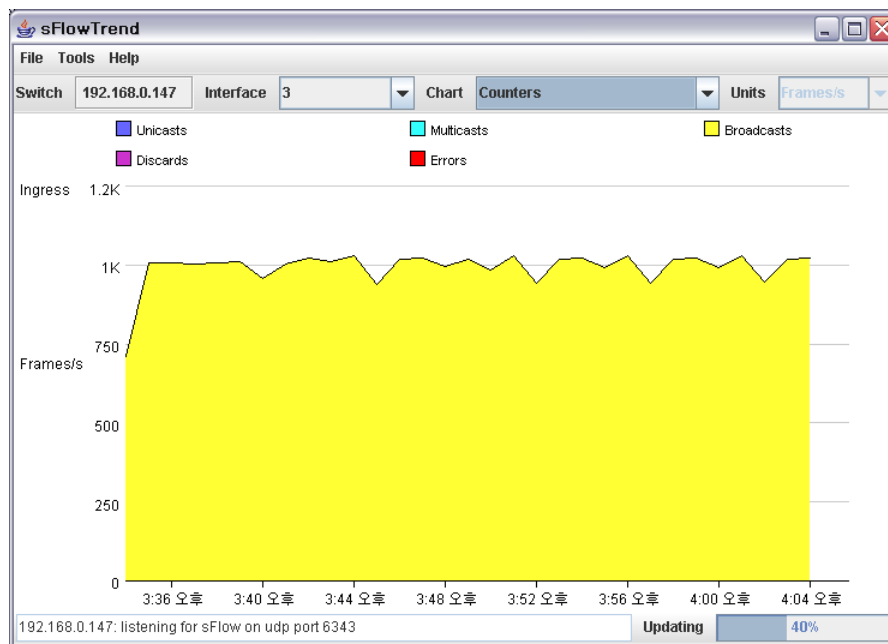


Figure 26. Interface statistics sampling

Chapter 12. STP, RSTP, MSTP, and SLD

This chapter introduces how to configure the Spanning Tree Protocol (STP) and Rapid Spanning Tree Protocol (RSTP) on the switch. It also explains frame transmission from the bridge.

**Note**

Refer to Command Reference for the complete format and instruction of commands mentioned in this chapter.

This chapter includes the following sections:

- Understanding Spanning-Tree Features
- Understanding RSTP
- Understanding MSTP
- Configuring Spanning-Tree Features
- Displaying the Spanning-Tree Status
- Configuring Bridge Mac Forwarding

Understanding Spanning-Tree Features

This chapter explains the following STP features:

- STP Overview
- Supported Spanning-Tree Instances
- 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 State

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 a 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 the 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 a loop, the spanning-tree port priority and path cost settings determine the forwarding and blocking states of these interfaces.

Bridge Protocol Data Units

The following shows elements provide stable active spanning-tree topology of a switched network:

- Unique bridgeID related to 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 the Root switch
- Spanning-tree path cost to the Root
- Switch BridgeID transmitting BPDU
- Message age
- Switch interface identifier transmitting BPDU
- hello, forward-delay, max-age protocol timer value

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 shows the result from BPDU exchange:

- A switch is chosen as root switch.
- Root port of each switch, except root switch, is chosen. This port provides the best path (the lowest cost) for the switch to transmit packets to the root switch.
- Designated switch for each LAN should be decided. The designated switch transmits the packet by the lowest path in which provides in the lowest cost.
- Designated switch, port or the designated switch connected to LAN, for each LAN is decided and provides the lowest path cost when LAN transmits packet to the root switch.
- Root ports and designated ports are configured in forwarding state.
- All interfaces not in the spanning-tree are blocked.

Election of Root Switch

All switches with spanning-tree gather information of other switches as exchanging BPDU, and the following shows results from message exchange:

- Only root switch first-out for each spanning-tree instance
- Designated switch first-out for all switched LAN segmentation
- Remove switched network loop by the block of L2 interface connected with redundant link

A switch with the highest priority (with the smallest value) in each VLAN is determined as the root switch. In the case that 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 addresses of the switch. U9016B 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 179 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	Bit4	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

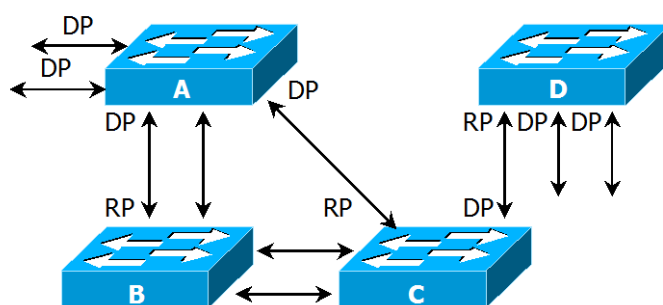
The following shows Spanning-tree timers that affect the spanning tree performance:

Table 180 Spanning-Tree Timers

Variable	Description
Hello timer	Decides the interval that the switch transmits Hello message to other switches
Forward-delay timer	Decides how long the interface is in listening and learning state before forwarding
Maximum-age timer	Decides the amount of time the switch stores received protocol information

Creating the Spanning-Tree Topology

Assuming that the 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).



RP = Root Port
DP = Designated Port

Figure 27. 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.

The following shows the states of each Layer 2 interface of the switch enabling spanning tree:

- 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 shows state transition of an interface.

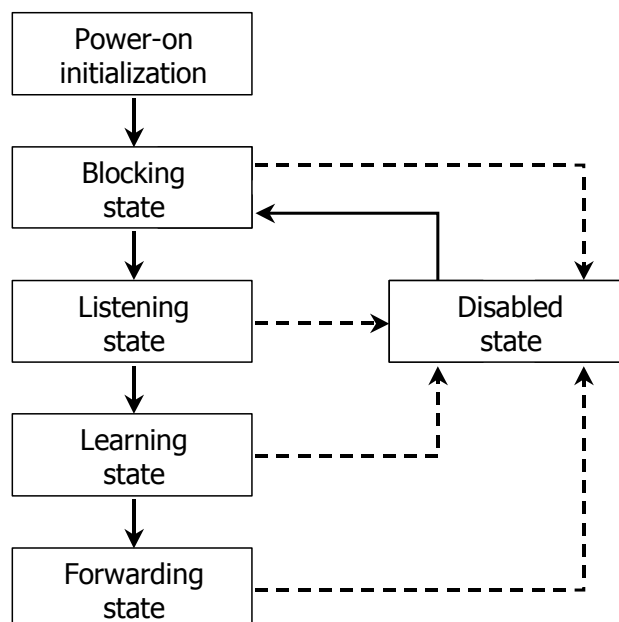


Figure 28. Spanning-Tree Interface States

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.

Item	Description
Blocking State	<p>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.</p> <p>An interface acts as following in blocking state: Drops the frames received through the port Drops the frames switched from other interfaces Does not perform address learning Receives BPDUs</p>
Listening State	<p>Listening state comes after the blocking state. If an interface decides to forward the frames, it goes into listening state.</p> <p>An interface acts as following in listening state: Drops the frames received through the port Drops the frames switched from other interfaces Does not perform address learning Receives BPDUs</p>
Learning State	<p>In learning state, a Layer 2 interface is ready to forward frames. The interface goes from listening state to learning state.</p> <p>In learning state, an interface acts as follows: Drops the frames received through the port Drops the frames switched from other interfaces Performs address learning Receives BPDUs</p>
Forwarding State	<p>In forwarding state, a Layer 2 interface forwards frames. The interface goes from learning state to forwarding state.</p> <p>In forwarding state, an interface acts as follows: Forwards the frames received through the port Forwards the frames switched from other interfaces Performs address learning Receives BPDUs</p>
Disable State	<p>In disabled state, a Layer 2 interface does not participate in frame forwarding or spanning tree.</p> <p>A disabled interface acts as follows: Drops the frames received through the port Drops the frames switched from other interfaces Does not perform address learning Does not receive BPDUs</p>

--	--

Understanding RSTP

RSTP supports rapid convergence of spanning tree for point-to-point connection, which takes less than 1 second (by contrast, 802.1D spanning tree takes 50 seconds maximum by default). This feature is efficient for a network which transmits traffic sensitive to delay such as voice and image.

This section explains the following operations of RSTP:

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

RSTP Overview

The operation of RSTP provides rapid recovery (in less than 1 second) of connectivity in the case of failure of a switch, switch port, or a LAN. A new root port can transit rapidly to the forwarding port state, and the use of explicit acknowledgements between the switches allows the designated ports to transit rapidly to the forwarding port 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 one of following port roles to each port:

- Root port – It provides the best path (the lowest cost) when the switch forwards packet to the root switch.
- Designated port – Designated port – It connects to the designated switch and provides the lowest cost when LAN forwards packet to the root switch. The designated switch port connected to LAN is called the designated port.
- Alternate port – It provides an alternative path to the root switch by current root port.
- Backup port – It act as a backup port for the path to the leaves of the spanning tree. Backup port exists when two ports are connected together in a loopback by a point-to-point link or if there are two or more connection to the designated VLAN.
- Disabled port – It has no role for spanning tree operation.

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

RSTP guarantees that root port and designated port transit to forwarding state when whole network has the consistent port role. But all alternate and backup ports are always in a discarding state (equivalent to blocking state). The following table compares 802.1D and RSTP port state:

Table 181 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 rapid convergence for the failure of switch, port, or LAN. It also provides rapid recovery for edge port, new root port, and ports linked by point-to-point.

- Edge ports – If a port is configured as an edge port in RSTP switch by using the spanning-tree admin-edge-port command, edge port immediately transits to forwarding state. Edge port should set in the port connected to one end station.
- Root ports – If the RSTP selects a new root port, the old root port is blocked and new root port is to be 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 nonedge 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.

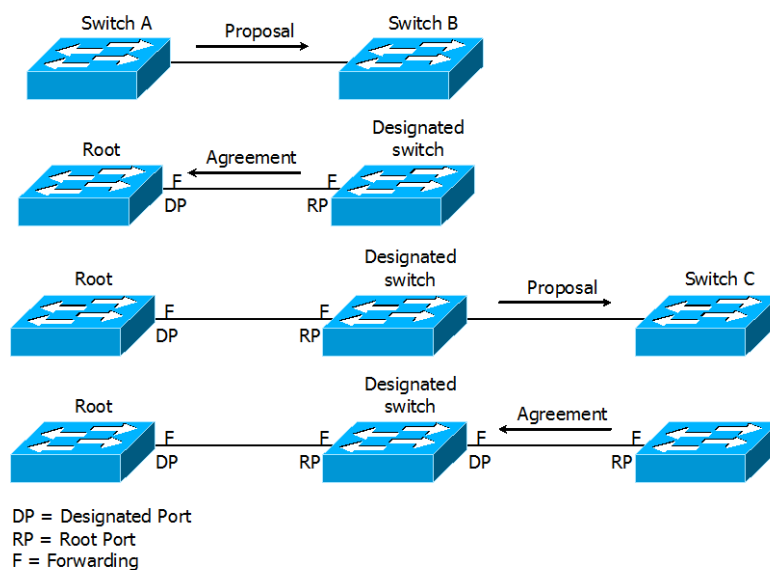


Figure 29. Proposal and Agreement Handshaking for Rapid Convergence

Bridge Protocol Data Unit Format and Processing

RSTP BPDU format is the same as IEEE 802.1D BPDU format except the protocol version field value is set to 2. The new 1 byte version 1 length field is set to 0, which does not include version 1 protocol information. The following table shows the RSTP flag field:

Table 182 RSTP BPDU Flags

Bit	Function
0	Topology change (TC)
1	Proposal
2-3:	Port role:
00	Unknown
01	Alternate port
10	Root port
11	Designated port
4	Learning
5	Forwarding
6	Agreement
7	Topology change acknowledgement (TCA)

The switch proposing itself as the designated switch sets the proposal flag of RSTP BPDU and transmits it. The port role of the message is always set as the designated port.

The switch agreeing the proposal from other switches sets the agreement flag of RSTP BPDU and transmits it. The port role of the message is always set as the root port.

RSTP does not use independent topology change notification (TCN) BPDU. To notice topology change, use topology change (TC) flag of RSTP BPDU flag. But generate and process TCN BPDU to interwork with 802.1D switch.

Learning and forwarding flag are set according to transmitting port state.

About MSTP

MSTP (Multiple Spanning Tree Protocol) is defined in IEEE 802.1s and binds multiple VLAN with one group. Then it make spanning tree work. As one spanning tree named instance in MSTP runs per VLAN group, the system need not to calculate a lot of spanning tree. The sytem thus has reduced load. For example, If you use PVST in network that uses 2000 numbers VLAN, the systems must calculate 2000 numbers spanning tree. But, If you divide 2000 numbers VLAN with 2 numbers group with using MSTP, the only 2 spanning trees are used. Forthermore if MSTP runs, BPDU transmmition quantity also reduses prograssively. By using MSTP, the reason why the system can reduce spanning tree number is that it needs spanning tree only as many as path number that can do load balancing.

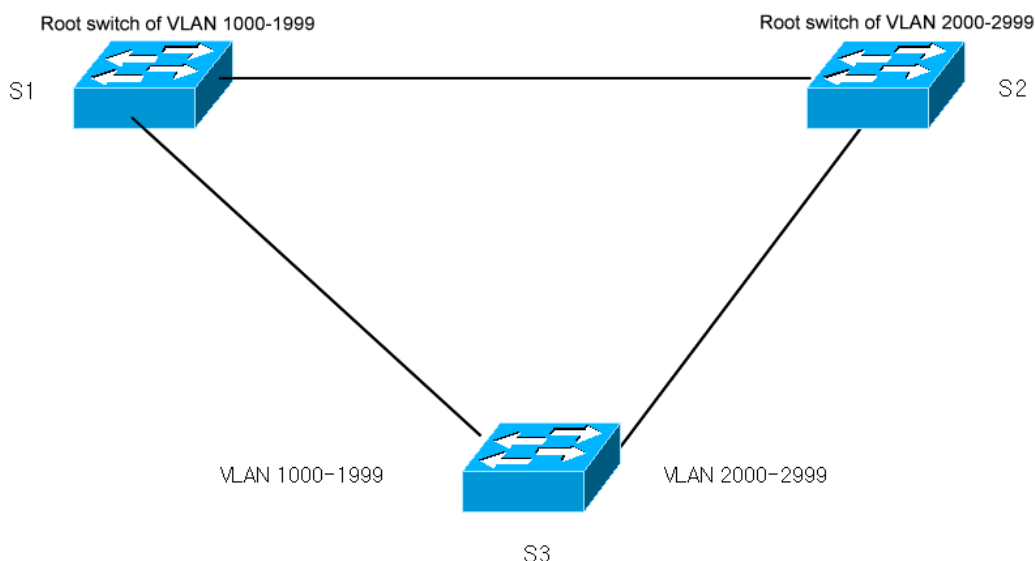


Figure 30. Load Balance

Even if the VLANs used from switch S3 is 2000 numbers from 1000 to 2999, if two spanning trees work, the system can get load balancing to S1, S2.

MST Region

The group of switchs having the same MST setting value is called one MST region. It defines the switchs that have the same MST setting values - MST name, MST revision and VLAN list value of instance as the same MST region.

IST, CST and CIST

MSTP uses two kinds of spanning tree. IST (Internal Spanning Tree) runs in one MST region. You can run 63 number spanning trees in the same MST region. You can use the number from 0 to 63 on each spanning tree instance and instance 0 is called as IST. MST sends or receives BPDU only IST. Thus, the other spanning tree information of instance is included in BPDU of IST and the BPDU of numbers that the switch covers reduce more. CIST is a group of IST and CST. In IEEE 802.1Q, even if multi VLANs exist, the spanning tree runs only one. We define this spanning tree as CST (common Spanning Tree). The following figure shows the relation of IST, CST, and CIST:

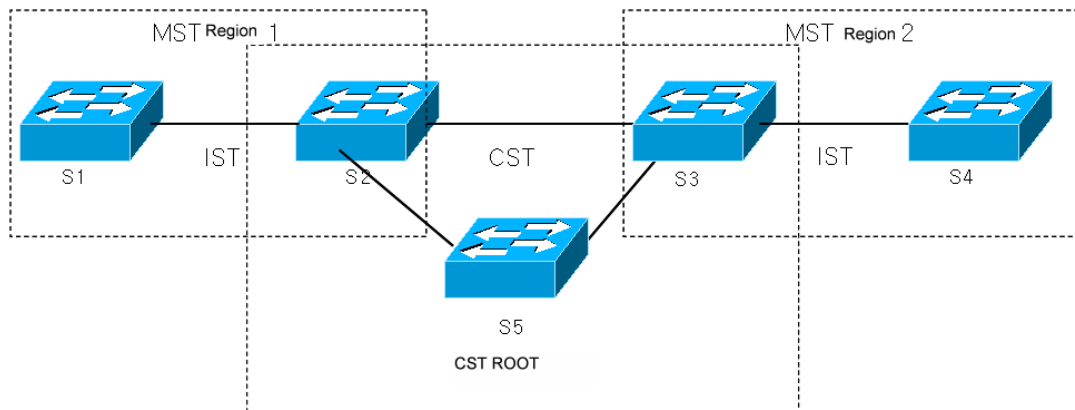


Figure 31. CST, IST, CIST

In the case that MST region differs, IST also runs separately. As MST region of S1 and S2 differs with region of S3, S4, IST running in each MST region runs separately. We define the switch having the least values about the path value to the CST root switch, bridge ID, port ID as IST master. If S5 is CST root switch, S2 and S3 run as IST master switch within each MST region. If CST root switch is outside of MST region, IST master always exist on border of CST and MST. In the case that the switch network is configured with one MST region, the same switch run as CST root and IST mater. CST run not only each different MST region but also between the switches running with 802.1D or bwtween MST and 802.1D. From view of CST, it considers a total MST region as one switch. Thus, CST knows the previous network as knowing, as in the following figure:

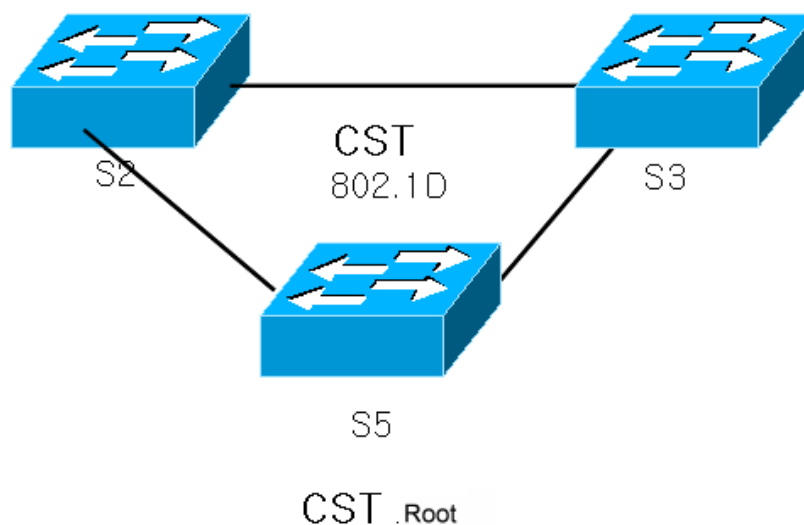


Figure 32. The network of View from CST

Configuring Spanning-Tree Features

This section describes how to configure spanning-tree features. The way of spanning-tree is different according to mode. It is set the same way in the case of RSTP and STP. In the case of MSTP, it has another way.

Default STP Configuration

The following table shows the default setting of STP.

Table 183 Default STP Configuration

Feature	Default Setting
Enable state	Disabled.
Spanning-tree mode	IEEE 802.1w 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)	10000 Mbps: 2000 1000 Mbps: 20000. 100 Mbps: 200000 10 Mbps: 2000000.
Hello time	2 sec.
Forward-delay time	15 sec.
Maximum-aging time	20 sec.

STP Configuration Guidelines

The system does not provide PVST. Thus, one spanning-tree runs in one Bridge and the VLAN included in the bridge does not affect anything. You can run spanning-tree per Bridge and create Bridge up to 256 numbers. VLAN can belong to only one Bridge. In the case of trunk VLAN, it can belong to only default Bridge. When you set spanning-tree on Trunk VLAN, you must set one spanning-tree to the total VLAN.

Enabling STP

At first, STP does not work in the system. If the possibility that the loop exists is in the network, enable STP. When you enable STP, RSTP works.

To enable STP, do the following steps on the privileged EXEC mode.

	Command	Purpose
Step1	configure terminal	Enter to Global configuration.
Step2	spanning-tree enable	Enables STP on Default Bridge.
Step3	exit	Back to Privileged EXEC mode.
Step4	show spanning-tree	Shows current configuration.
Step5	copy running-config startup-config	Saves current configuration to startup configuration.

To disable STP, execute the spanning-tree shutdown bridge-forward command on global configuration mode.

The following shows how to enable spanning tree and show the result:

```
Switch#
Switch# configure terminal
Switch(config)# spanning-tree enable
Switch(config)#
Switch(config)# exit
Switch#
Switch# show spanning-tree
Default Bridge up - Spanning Tree Enabled rstp-VLAN-bridge
  Root ID    Priority    32768
            Address      00077074ff01
This bridge is the root
Hello Time  2 sec  Max Age 20 sec  Foward Delay  15 sec
  Bridge ID  Priority    32768
            Address      00077074ff01
Hello Time  2 sec  Max Age 20 sec  Foward Delay  15 sec
Aging Time  300
Interface    Role Sts Cost      Prio.Nbr Type
-----
Giga5/3/2    Disb BLK 4      128.610 Shared
Switch#
Switch# configure terminal
Switch(config)# spanning-tree shutdown bridge-forward
Switch(config)# exit
Switch# show spanning-tree
Spanning tree instance(s) does not exist
Switch#
```


Enable STP in NO default Bridge

You can manage spanning-tree per Bridge. First, create Bridge. After you include the interface to be worked as a spanning-tree, enable the spanning-tree in the relevant Bridge.



Note

The interface included to run spanning-tree on Bridge can input on Bridge directly. After setting VLAN on the interface, you must set VLAN on the Bridge.

To enable STP in no default bridge, do the following steps on privileged EXEC mode:

	Command	Purpose
Step1	configure terminal	Enter Global configuration mode.
Step2	Bridge <1-255> protocol VLAN-bridge	Creates Bridge.
Step3	bridge <1-255> spanning-tree enable	Enables STP on Bridge.
Step4	Bridge-group <1-255>	Includes VLAN on Bridge.
Step5	copy running-config startup-config	Save the current configuration.

The following example shows how to enable STP in no default bridge:

```
Switch#
Switch# show spanning-tree
Spanning tree instance(s) does not exist
Switch# configure terminal
Switch(config) bridge 1 protocol VLAN-bridge
Switch(config) bridge 1 rapid-spanning-tree enable
Switch(config)# interface Vlan100
Switch (config-if-Vlan100)#bridge-group 1
Switch(config)# exit
Switch# show running-config
!
bridge 1 protocol VLAN-bridge
bridge 1 spanning-tree enable
!
Switch#
Switch# configure terminal
Switch(config)# bridge shutdown 1 bridge-forward
Switch(config)# no bridge 1
Switch(config)# exit
Switch# show running-config
!
Switch#
```

Configuring the Port Priority

If a loop occurs, the spanning tree decides the interface in the forwarding state with port priority.

It is possible to assign the higher priority (lower number) to the prior interface and the lower priority (higher number) to posterior interface. If all interfaces have same priority, spanning tree set interface with the lowest number in forwarding state, and block other interfaces.

To configure the port priority of interface, follow the procedures below:

Table 184 Configuring the Port Priority

	Command	Purpose
Step1	configure terminal	Enters global configuration mode
Step2	interface <i>interface-id</i>	Enters interface configuration mode, and specify an interface to configure. Available interface is physical interface and port group.
Step3	spanning-tree port-priority <i>priority</i>	Sets VLAN port priority for an interface.
Step4	exit	Changes to privileged EXEC mode
Step5	show spanning-tree	Checks Configuration
Step6	copy running-config startup-config	Saves the setting in configuration file (optional)

To return the default setting of interface, use interface configuration command `no spanning-tree VLAN VLAN-id port-priority`.

```
Switch#show spanning-tree
Default Bridge up - Spanning Tree Enabled rstp-VLAN-bridge
  Root ID    Priority    32768
    Address    00077074ff01
This bridge is the root
Hello Time  2 sec  Max Age 20 sec  Foward Delay  15 sec
  Bridge ID  Priority    32768
    Address    00077074ff01
Hello Time  2 sec  Max Age 20 sec  Foward Delay  15 sec
Aging Time  300
Interface    Role Sts Cost      Prio.Nbr Type
-----
Giga5/3      Disb BLK 4      128.138 Shared
Switch # configure terminal
Switch(config)#int GigabitEthernet 5/3
Switch(config-if-Giga5/3)#spanning-tree port-priority 0
Switch(config-if-Giga5/3)#exit
Switch # show spanning-tree
Default Bridge up - Spanning Tree Enabled rstp-VLAN-bridge
  Root ID    Priority    32768
    Address    00077074ff01
This bridge is the root
Hello Time  2 sec  Max Age 20 sec  Foward Delay  15 sec
  Bridge ID  Priority    32768
    Address    00077074ff01
Hello Time  2 sec  Max Age 20 sec  Foward Delay  15 sec
Aging Time  300
```

Interface	Role	Sts	Cost	Prio.	Nbr	Type
Giga5/3	Disb	BLK	4	0.138		Shared
Switch#configure terminal						
Switch(config)#interface GigabitEthernet 5/3						
Switch(config-if-Giga5/3)#no spanning-tree port-priority						
Switch(config-if-Giga5/3)#exit						
Switch#show spanning-tree						
Default Bridge up - Spanning Tree Enabled rstp-VLAN-bridge						
Root ID	Priority		32768			
	Address		00077074ff01			
This bridge is the root						
Hello Time	2 sec	Max Age	20 sec	Foward Delay	15 sec	
Bridge ID	Priority		32768			
	Address		00077074ff01			
Hello Time	2 sec	Max Age	20 sec	Foward Delay	15 sec	
Aging Time	300					
Interface	Role	Sts	Cost	Prio.	Nbr	Type
Giga5/3	Disb	BLK	4	128.138		Shared
Switch#						

Configuring the Path Cost

The default value of the path cost of spanning-tree is decided by the media speed of interface. If a loop occurs, the spanning tree decides the interface in forwarding state with port cost. It is possible to assign the lower cost to the prior interface and the higher cost to posterior interface. If all interfaces have the same cost, the spanning tree sets an interface with the lowest number in the forwarding state, and blocks other interface.



Note

Port group cannot decide the path cost by interface speed but each member port can have different speed. Set path cost for the port group manually.

To configure the path cost of interface, follow the procedure set out below:

Table 185 Configuring the Path Cost

Step	Command	Purpose
Step1	configure terminal	To enter global configuration mode
Step2	interface <i>interface-id</i>	To enter interface configuration mode, and specify an interface to configure. Available interface is physical interface and port group.
Step3	spanning-tree path-cost <i>cost</i>	Sets cost.
Step4	exit	To return to privileged EXEC mode
Step5	show spanning-tree	To check the setting
Step6	copy running-config startup-config	To save the setting in the configuration file (optional)

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

In the case that bridge is not a default, the system use bridge<1-255> besides of spanning-tree.

Switch#show spanning-tree

Default Bridge up - Spanning Tree Enabled rstp-VLAN-bridge

Root ID Priority 32768
 Address 00077074ff01
 This bridge is the root
 Hello Time 2 sec Max Age 20 sec Foward Delay 15 sec

Bridge ID Priority 32768
 Address 00077074ff01
 Hello Time 2 sec Max Age 20 sec Foward Delay 15 sec
 Aging Time 300

Interface	Role	Sts	Cost	Prio.Nbr	Type
Giga5/3	Disb	BLK	4	128.138	Shared

Switch#configure terminal

```
Switch(config)#interface GigabitEthernet 5/3
Switch(config-if-Giga5/3)#spanning-tree path-cost 10
Switch(config-if-Giga5/3)#exit
Switch#show spanning-tree
```

Default Bridge up - Spanning Tree Enabled rstp-VLAN-bridge

Root ID Priority 32768
 Address 00077074ff01
 This bridge is the root
 Hello Time 2 sec Max Age 20 sec Foward Delay 15 sec

Bridge ID Priority 32768
 Address 00077074ff01
 Hello Time 2 sec Max Age 20 sec Foward Delay 15 sec
 Aging Time 300

Interface	Role	Sts	Cost	Prio.Nbr	Type
Giga5/3	Disb	BLK	10	128.138	Shared

Switch#configure terminal

```
Switch(config)#interface GigabitEthernet 5/3
Switch(config-if-Giga5/3)#no spanning-tree path-cost
Switch(config-if-Giga5/3)#exit
Switch#sh spanning-tree
```

Default Bridge up - Spanning Tree Enabled rstp-VLAN-bridge

Root ID Priority 32768
 Address 00077074ff01
 This bridge is the root
 Hello Time 2 sec Max Age 20 sec Foward Delay 15 sec

Configuring the Switch Priority of a VLAN

To be a root switch, the switch priority can be changed. To return the default setting of switch, use global configuration command `no spanning-tree VLAN VLAN-id priority`. In the case that the Bridge is not a default, the system use bridge<1-255> besides a spanning-tree.

To be a root switch, the switch priority can be changed.

To configure the switch priority for VLAN, perform the following tasks:

Table 186 Configuring the Switch Priority of a VLAN

Step	Command	Purpose
Step1	<code>configure terminal</code>	To enter Global configuration mode
Step2	<code>spanning-tree priority <i>priority</i></code>	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	<code>exit</code>	To return to privileged EXEC mode.
Step4	<code>show spanning</code>	To check the setting
Step5	<code>copy running-config startup-config</code>	To Save Setting in the configuration file (optional)

To return the default setting of switch, use global configuration command `no spanning-tree VLAN VLAN-id priority`.

```
Switch#show spanning-tree
Default Bridge up - Spanning Tree Enabled rstp-VLAN-bridge
  Root ID    Priority    32768
             Address      00077074ff01
             This bridge is the root
             Hello Time 2 sec Max Age 20 sec Foward Delay 15 sec
  Bridge ID  Priority    32768
             Address      00077074ff01
             Hello Time 2 sec Max Age 20 sec Foward Delay 15 sec
             Aging Time 300
Interface   Role Sts Cost      Prio.Nbr Type
-----
Giga5/3     Disb BLK 4      128.138 Shared
Switch#
Switch#configure terminal
Switch(config)#spanning-tree priority 4096
Switch(config)#exit
Switch#show spanning-tree
Default Bridge up - Spanning Tree Enabled rstp-VLAN-bridge
  Root ID    Priority    4096
             Address      00077074ff01
             This bridge is the root
             Hello Time 2 sec Max Age 20 sec Foward Delay 15 sec
  Bridge ID  Priority    4096
             Address      00077074ff01
             Hello Time 2 sec Max Age 20 sec Foward Delay 15 sec
```

```

Aging Time 300
Interface      Role Sts Cost      Prio.Nbr Type
-----
Giga5/3       Disb BLK 4          128.138  Shared
Switch#conf t
Switch(config)#no spanning-tree priority
Switch(config)#exit
Switch#show spanning-tree
Default Bridge up - Spanning Tree Enabled rstp-VLAN-bridge
Root ID      Priority    32768
Address      00077074ff01
This bridge is the root
Hello Time 2 sec Max Age 20 sec Foward Delay 15 sec
Bridge ID Priority    32768
Address      00077074ff01
Hello Time 2 sec Max Age 20 sec Foward Delay 15 sec
Aging Time 300
Interface      Role Sts Cost      Prio.Nbr Type
-----
Giga5/3       Disb BLK 4          128.138  Shared
Switch#

```

Configuring the Hello Time

As modifying the hello time, you can change the configuration BPDU interval that root switch transmits. To configure the hello time for a VLAN, perform the following the procedures:

Table 187 Configuring the Hello Time

Step	Command	Purpose
Step1	configure terminal	To enter global configuration mode
Step2	spanning-tree hello-time <i>seconds</i>	Hello time is a period for the root switch to send a configuration message, indicating that the switch is alive. • <i>seconds</i> ranges from 1 to 10. The default setting is 2.
Step3	exit	To return to privileged EXEC mode
Step4	show spanning-tree	To check the setting
Step5	copy running-config startup-config	To save the setting in configuration file (optional)

To return the default setting of switch, use global configuration command `no spanning-tree VLAN VLAN-id hello-time`. In the case that bridge is not a default, the system use `bridge<1-255>` besides of `spanning-tree`.

```
Switch#show spanning-tree
```

```
Default Bridge up - Spanning Tree Enabled rstp-VLAN-bridge
```

```
Root ID      Priority    32768
Address      00077074ff01
This bridge is the root
Hello Time   2 sec    Max Age 20 sec    Forward Delay  15 sec
```

```
Bridge ID    Priority    32768
Address      00077074ff01
Hello Time   2 sec    Max Age 20 sec    Forward Delay  15 sec
Aging Time   300
```

```
Interface    Role Sts Cost      Prio.Nbr Type
-----
Giga5/3      Disb BLK 4      128.138 Shared
```

```
Switch#
Switch#configure terminal
```

```
Switch(config)#spanning-tree hello-time 9
Switch(config)#exit
Switch#show spanning-tree
```

```
Default Bridge up - Spanning Tree Enabled rstp-VLAN-bridge
```

```
Root ID      Priority    32768
Address      00077074ff01
This bridge is the root
Hello Time   9 sec    Max Age 20 sec    Forward Delay  15 sec
```

```
Bridge ID    Priority    32768
```

```

Address      00077074ff01
Hello Time   9  sec  Max Age 20 sec  Foward Delay  15 sec
Aging Time   300
  
```

Interface	Role	Sts	Cost	Prio.Nbr	Type
Giga5/3	Disb	BLK	4	128.138	Shared

Switch#configure terminal

Switch(config)#no spanning-tree hello-time

Switch(config)#exit

Switch#show spanning-tree

Default Bridge up - Spanning Tree Enabled rstp-VLAN-bridge

```

Root ID      Priority      32768
Address      00077074ff01
This bridge is the root
Hello Time    2  sec  Max Age 20 sec  Foward Delay  15 sec
  
```

```

Bridge ID    Priority      32768
Address      00077074ff01
Hello Time    2  sec  Max Age 20 sec  Foward Delay  15 sec
Aging Time    300
  
```

Interface	Role	Sts	Cost	Prio.Nbr	Type
Giga5/3	Disb	BLK	4	128.138	Shared

Configuring the Forwarding-Delay Time for a VLAN

To configure the forwarding-delay time for a VLAN, perform the following the procedures:

Table 188 Configuring the Forwarding-Delay Time for a VLAN

Step	Command	Purpose
Step1	configure terminal	To enter Global configuration mode
Step2	spanning-tree forward-time <i>seconds</i>	Seconds range is between 4 and 30. The default is 15.
Step3	exit	Exit the configuration mode
Step4	show spanning-tree	To check the setting
Step5	copy running-config startup-config	Saves current configuration file.

To return the default setting of switch, use global configuration command `no spanning-tree VLAN VLAN-id forward-time`.

In the case that bridge is not a default, the system use bridge<1-255> of spanning-tree.

```
Switch#show spanning-tree
```

```
Default Bridge up - Spanning Tree Enabled rstp-VLAN-bridge
```

```
Root ID    Priority    32768
           Address    00077074ff01
           This bridge is the root
           Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
```

```
Bridge ID  Priority    32768
           Address    00077074ff01
           Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
           Aging Time 300
```

```
Interface    Role Sts Cost      Prio.Nbr Type
-----
Giga5/3      Disb BLK 4      128.138 Shared
```

```
Switch#configure terminal
```

```
Switch(config)#spanning-tree forward-time 20
```

```
Switch(config)#exit
```

```
Switch#show spanning-tree
```

```
Default Bridge up - Spanning Tree Enabled rstp-VLAN-bridge
```

```
Root ID    Priority    32768
           Address    00077074ff01
           This bridge is the root
           Hello Time 2 sec Max Age 20 sec Forward Delay 20 sec
```

```
Bridge ID  Priority    32768
           Address    00077074ff01
           Hello Time 2 sec Max Age 20 sec Forward Delay 20 sec
```

Aging Time 300

Interface	Role	Sts Cost	Prio.Nbr	Type
Giga5/3	Disb	BLK 4	128.138	Shared

Switch#configure terminal

Switch(config)#no spanning-tree forward-time

Switch(config)#exit

Switch#show spanning-tree

Default Bridge up - Spanning Tree Enabled rstp-VLAN-bridge

Root ID	Priority	32768
	Address	00077074ff01
This bridge is the root		
Hello Time	2 sec	Max Age 20 sec Foward Delay 15 sec

Bridge ID	Priority	32768
	Address	00077074ff01
Hello Time	2 sec	Max Age 20 sec Foward Delay 15 sec
Aging Time	300	

Interface	Role	Sts Cost	Prio.Nbr	Type
Giga5/3	Disb	BLK 4	128.138	Shared

Configuring the Maximum-Aging Time for a VLAN

To configure the maximum-aging time, perform the follow ing the procedure:

Table 189 Configuring the Maximum-Aging Time for a VLAN

Step	Command	Purpose
Step1	configure terminal	Enters global configuration mode
Step2	spanning-tree max-age <i>seconds</i>	Sets maximum-aging time Seconds range is between 6 and 40. The default is 20.
Step3	exit	Returns to privileged EXEC mode
Step4	show spanning-tree	Checks the setting
Step5	copy running-config startup-config	Save settings in the configuration file (optional).

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

In the case that bridge is not a default, the system use bridge<1-255> of spanning-tree.

Switch#show spanning-tree

Default Bridge up - Spanning Tree Enabled rstp-VLAN-bridge

Root ID	Priority	32768
	Address	00077074ff01

This bridge is the root

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32768

Address 00077074ff01

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Aging Time 300

Interface	Role	Sts	Cost	Prio.	Nbr	Type
Giga5/3	Disb	BLK	4	128.138	Shared	

Switch#configure terminal

Switch(config)#spanning-tree max-age 15

Switch(config)#exit

Switch#show spanning-tree

Default Bridge up - Spanning Tree Enabled rstp-VLAN-bridge

Root ID Priority 32768

Address 00077074ff01

This bridge is the root

Hello Time 2 sec Max Age 15 sec Forward Delay 15 sec

Bridge ID Priority 32768

Address 00077074ff01

Hello Time 2 sec Max Age 15 sec Forward Delay 15 sec

Aging Time 300

Interface	Role	Sts	Cost	Prio.	Nbr	Type
Giga5/3	Disb	BLK	4	128.138	Shared	

Switch#configure terminal

Switch(config)#no spanning-tree max-age

Switch(config)#exit

Switch#show spanning-tree

Default Bridge up - Spanning Tree Enabled rstp-VLAN-bridge

Root ID Priority 32768

Address 00077074ff01

Changing the Max-hops for switch

MSTP mode use hop count like TTL of IP instead of using max age and forward delay.

	Command	Purpose
Step1	configure terminal	Enters to global configuration mode.
Step2	Spanning-tree max-hops count	Changes max-hop.
Step3	exit	Backs to privileged EXEC mode.
Step4	show running-config	Shows current configuration.

Step5	copy running-config startup-config	Saves current configuration to start-up configuration.
--------------	---	--

```
Switch(config)#spanning-tree max-hops 10
Switch(config)#do show spa mst
#### MST1    vlans mapped:20,70
Bridge      address 0007.70de.ad99  priority    32768    (32768    sysid 0)
Root        address 0007.709e.12fd  priority    8000     (8000     sysid 0)
Regional Root this switch
Operational hello time 2, forward delay 15, max age 20, txholdcount 6
Configured  hello time 2, forward delay 15, max age 20, max hops 10
Interface      Role    Sts Cost    Prio.Nbr Type
-----
Giga5/3        Mstr    FWD 20000    128.138 P2p
Giga5/4        Altn    BLK 20000    128.139 P2p
```

```
Switch(config)#no spanning-tree max-hops
Switch(config)#do show spa mst
#### MST1    vlans mapped:20,70
Bridge      address 0007.70de.ad99  priority    32768    (32768    sysid 0)
Root        address 0007.709e.12fd  priority    8000     (8000     sysid 0)
Regional Root this switch
Operational hello time 2, forward delay 15, max age 20, txholdcount 6
Configured  hello time 2, forward delay 15, max age 20, max hops 20
Interface      Role    Sts Cost    Prio.Nbr Type
-----
Giga5/3        Mstr    FWD 20000    128.138 P2p
Giga5/4        Altn    BLK 20000    128.139 P2p
```

Changing the Spanning-Tree mode for switch

To change the spanning-tree mode for switch, follow the procedures set out below:

Table 190 Changing the Spanning-Tree mode for switch

Step	Command	Purpose
Step1	configure terminal	To enter global configuration mode
Step2	spanning-tree mode {stp rstp mstp provider-mstp provider-rstp stp-VLAN-bridge rstp-VLAN- bridge}	To change the spanning-tree mode
Step3	exit	To return to privileged EXEC mode
Step4	show running-config	To check the setting
Step5	copy running-config startup-config	To save the settings in the configuration file (optional)

Switch#show spanning-tree

Default Bridge up - Spanning Tree Enabled rstp-VLAN-bridge

Root ID Priority 32768
Address 00077074ff01
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32768
Address 00077074ff01
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300

Interface	Role	Sts	Cost	Prio.	Nbr	Type
Giga5/3	Disb	BLK	4	128.138	Shared	

Switch#configure terminal

Switch(config)#spanning-tree mode stp-VLAN-bridge

Switch(config)#exit

Switch(config)#spanning-tree enable

Switch(config)#exit

Switch#show spanning-tree

Default Bridge up - Spanning Tree Enabled stp-VLAN-bridge

Root ID Priority 32768
Address 00077074ff01
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32768
Address 00077074ff01
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300

Interface	Role	Sts	Cost	Prio.	Nbr	Type
Giga5/3	Disb	DIS	4	128.138	Shared	

Switch#configure terminal

Switch(config)#spanning-tree mode mstp

Switch(config)#spanning-tree enable

Switch(config)#exit

Switch#show spanning-tree

Default Bridge up - Spanning Tree Enabled mstp

Root ID Priority 32768
Address 00077074ff01
This bridge is the root

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32768

Address 00077074ff01

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Aging Time 300

Configuring portfast for switch

The following example shows how to set portfast for switch:

	Command	Purpose
Step1	configure terminal	Enter the the Global configuration mode.
Step2	spanning-tree portfast {bpdu-filter bpdu-guard }	Sets the portfast to every port.
Step3	exit	Enter the privileged EXEC mode.
Step4	show running-config	Shows the current running configuration.
Step5	copy running-config startup-config	Saves the configuration to startup-configuration.

Switch(config)#do show spa inter gi5/3

Default: Bridge up - Spanning Tree Enabled

Default: Root Path Cost 4 - Root Port 138 - Bridge Priority 32768

Default: Forward Delay 15 - Hello Time 2 - Max Age 20

Default: Root Id 80000007709e12fd

Default: Bridge Id 8000000770dead99

Default: last topology change Tue Jan 13 23:32:51 1970

0: 2 topology change(s) - last topology change Tue Jan 13 23:32:51 1970

Default: portfast bpdu-filter disabled

Default: portfast bpdu-guard disabled

Default: portfast errdisable timeout disabled

Default: portfast errdisable timeout interval 300 sec

Giga5/3: Port 138 - Id 808a - Role Rootport - State Forwarding

Giga5/3: Designated Path Cost 0

Giga5/3: Configured Path Cost 4 - Add type Explicit ref count 1

Giga5/3: Designated Port Id 8001 - Priority 128 -

Giga5/3: Root 80000007709e12fd

Giga5/3: Designated Bridge 80000007709e12fd

Giga5/3: Message Age 0 - Max Age 20

Giga5/3: Hello Time 2 - Forward Delay 15

Giga5/3: Forward Timer 0 - Msg Age Timer 4 - Hello Timer 0 - topo change timer 0

Giga5/3: forward-transitions 1

Giga5/3: Version Rapid Spanning Tree Protocol - Received RSTP - Send RSTP

Giga5/3: No portfast configured - Current portfast off

Giga5/3: portfast bpdu-guard default - Current portfast bpdu-guard off

Giga5/3: portfast bpdu-filter default - Current portfast bpdu-filter off

Giga5/3: no root guard configured - Current root guard off

Giga5/3: Configured Link Type point-to-point - Current point-to-point

Switch(config)#**spanning-tree portfast bpdu-filter**

Switch(config)#do show spa inter gi5/3

Default: Bridge up - Spanning Tree Enabled

Default: Root Path Cost 4 - Root Port 138 - Bridge Priority 32768

Default: Forward Delay 15 - Hello Time 2 - Max Age 20

Default: Root Id 80000007709e12fd

Default: Bridge Id 8000000770dead99

Default: last topology change Tue Jan 13 23:32:51 1970

0: 2 topology change(s) - last topology change Tue Jan 13 23:32:51 1970

Default: portfast bpdu-filter **enabled**

Default: portfast bpdu-guard disabled

Default: portfast errdisable timeout disabled

Default: portfast errdisable timeout interval 300 sec

Giga5/3: Port 138 - Id 808a - Role Rootport - State Forwarding

Giga5/3: Designated Path Cost 0

Giga5/3: Configured Path Cost 4 - Add type Explicit ref count 1

Giga5/3: Designated Port Id 8001 - Priority 128 -

Giga5/3: Root 80000007709e12fd

Giga5/3: Designated Bridge 80000007709e12fd

Giga5/3: Message Age 0 - Max Age 20

Giga5/3: Hello Time 2 - Forward Delay 15

Giga5/3: Forward Timer 0 - Msg Age Timer 4 - Hello Timer 0 - topo change timer 0

Giga5/3: forward-transitions 1

Giga5/3: Version Rapid Spanning Tree Protocol - Received RSTP - Send RSTP

Giga5/3: No portfast configured - Current portfast off

Giga5/3: portfast bpdu-guard default - Current portfast bpdu-guard off

Giga5/3: portfast bpdu-filter default - Current portfast bpdu-filter on

Giga5/3: no root guard configured - Current root guard off

Giga5/3: Configured Link Type point-to-point - Current point-to-point



Note

Before you set bpdu-guard or bpdu-filter, you set portfast.

Changing transmit-holdcount for switch

You can limit BPDU number to transmit for the maximum transmit rate (Default: 3 sec). It is saved to transmit-holdcount. (Default: 6)

	Command	Purpose
Step1	configure terminal	Enters global configuration mode.
Step2	spanning-tree transmit-holdcount <i>holdcount</i>	Changes transmit-holdcount.
Step3	exit	Back to privileged EXEC mode.
Step4	show running-config	Shows current running configuration.
Step5	copy running-config startup-config	Saves the current running configuration to startup-configuration.

MST1 vlans mapped:70


```

Bridge      address 0007.70de.ad99  priority    32768    (32768    sysid 0)
Root        address 0007.709e.12fd  priority    8000     (8000     sysid 0)
Regional Root this switch
Operational hello time 2, forward delay 15, max age 20, txholdcount 6
Configured  hello time 2, forward delay 15, max age 20, max hops 20
Interface      Role    Sts Cost    Prio.Nbr Type
-----
Giga5/3        Mstr    FWD 20000    128.138  P2p
Giga5/4        Altn    BLK 20000    128.139  P2p

```

```

U9016B_112(config)#no spanning-tree transmit-holdcount
U9016B_112(config)#do show spa mst
#### MST1    vlans mapped:70
Bridge      address 0007.70de.ad99  priority    32768    (32768    sysid 0)
Root        address 0007.709e.12fd  priority    8000     (8000     sysid 0)
Regional Root this switch
Operational hello time 2, forward delay 15, max age 20, txholdcount 10
Configured  hello time 2, forward delay 15, max age 20, max hops 20
Interface      Role    Sts Cost    Prio.Nbr Type
-----
Giga5/3        Mstr    FWD 20000    128.138  P2p
Giga5/4        Altn    BLK 20000    128.139  P2p

```

Changing Cisco-interoperability for switch

As BPDU is defined by Cisco is different from standard BPDU, it needs to change Cisco-interoperability for the switch.

	Command	Purpose
Step1	configure terminal	Enters global configuration mode.
Step2	spanning-tree cisco-interoperability {enable disable}	Sets if it is comparable with Cisco.
Step3	exit	Back to Privileged EXEC mode.
Step4	show running-config	Shows current running configuration.
Step5	copy running-config startup-config	Saves the current running configuration to startup-configuration.

Configuring autoedge for port

You can set to check if device connected to port is edge device. When you set it with autoedge, do the following steps:

	Command	Purpose
Step1	configure terminal	Enters global configuration mode.
Step2	Interface interface-id	Enters interface configuration mode.
Step2	spanning-tree autoedge	Sets autoedge on port.
Step3	exit	Back to privileged EXEC mode.
Step4	show running-config	Shows current running configuration.
Step5	copy running-config startup-config	Saves current running configuration to startup-configuration.

Configuring the Port as Edge Port

If a port is not defined as an edge port, 2 x Forward Time will be taken for the port to transit to the forwarding state.



Note

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

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

Table 191 Configuring the Port as Edge Port

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

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

```
Switch#show spanning-tree
```

```
Default Bridge up - Spanning Tree Enabled rstp-VLAN-bridge
```

```
Root ID    Priority    32768
           Address    00077074ff01
           This bridge is the root
           Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID  Priority    32768
           Address    00077074ff01
           Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
           Aging Time 300
```

```
Interface    Role Sts Cost        Prio.Nbr Type
-----
Giga5/3      Disb BLK 4      128.138 Shared
```

```
Switch#configure terminal
Switch(config)#interface GigabitEthernet 5/3
Switch(config-if-Giga5/3)#spanning-tree edgeport
Switch(config-if-Giga5/3)#exit
Switch#show spanning-tree
```

```
Default Bridge up - Spanning Tree Enabled rstp-VLAN-bridge
```

```
Root ID    Priority    32768
```

```
Address      00077074ff01
This bridge is the root
Hello Time   2   sec   Max Age 20 sec   Foward Delay   15 sec
```

```
Bridge ID   Priority   32768
Address      00077074ff01
Hello Time   2   sec   Max Age 20 sec   Foward Delay   15 sec
Aging Time   300
```

Interface	Role	Sts	Cost	Prio.Nbr	Type
Giga5/3	Disb	BLK	4	128.138	Shared edge port

Switch#configure terminal

```
Switch(config)#interface GigabitEthernet 5/3
Switch(config-if-Giga5/3)#no spanning-tree edgeport
Switch(config-if-Giga5/3)#exit
Switch#show spanning-tree
```

```
Default Bridge up - Spanning Tree Enabled rstp-VLAN-bridge
Root ID   Priority   32768
Address      00077074ff01
This bridge is the root
Hello Time   2   sec   Max Age 20 sec   Foward Delay   15 sec
```

```
Bridge ID   Priority   32768
Address      00077074ff01
Hello Time   2   sec   Max Age 20 sec   Foward Delay   15 sec
Aging Time   300
```

Interface	Role	Sts	Cost	Prio.Nbr	Type
Giga5/3	Disb	BLK	4	128.138	Shared

Switch#Switch#

Specifying the Link Type to Ensure Rapid Transitions

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

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

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

Table 192 Specifying the Link Type to Ensure Rapid Transitions

Step	Command	Purpose
Step1	configure terminal	Enters global configuration mode.
Step2	interface <i>interface-id</i>	Enters interface configuration mode.
Step3	spanning-tree link-type point-to-point	Sets the link type of port to point-to-point.
Step4	exit	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 command **no spanning-tree link-type**.

Configuring force-version for port

To set force-version on port, do the following steps on privileged EXEC mode:

	Command	Purpose
Step1	configure terminal	Enters global configuration mode.
Step2	Interface <i>interface-id</i>	Enters interface configuration mode.
Step2	spanning-tree force-version <i>version</i>	Sets force-version on port. (0 : STP, 2 : RSTP, 3 : MSTP)
Step3	exit	Back to privileged EXEC mode.
Step4	show running-config	Shows current running configuration.
Step5	copy running-config startup-config	Saves current running configuration to startup-configuration.

Default: Bridge up - Spanning Tree Enabled

Default: Root Path Cost 4 - Root Port 138 - Bridge Priority 32768

Default: Forward Delay 15 - Hello Time 2 - Max Age 20

Default: Root Id 80000007709e12fd

Default: Bridge Id 8000000770dead99

Default: last topology change Wed Jan 14 12:07:59 1970

0: 2 topology change(s) - last topology change Wed Jan 14 12:07:59 1970

Default: portfast bpdu-filter disabled

Default: portfast bpdu-guard disabled
 Default: portfast errdisable timeout disabled
 Default: portfast errdisable timeout interval 300 sec
 Giga5/3: Port 138 - Id 808a - Role Rootport - State Forwarding
 Giga5/3: Designated Path Cost 0
 Giga5/3: Configured Path Cost 4 - Add type Explicit ref count 1
 Giga5/3: Designated Port Id 8001 - Priority 128 -
 Giga5/3: Root 80000007709e12fd
 Giga5/3: Designated Bridge 80000007709e12fd
 Giga5/3: Message Age 0 - Max Age 20
 Giga5/3: Hello Time 2 - Forward Delay 15
 Giga5/3: Forward Timer 0 - Msg Age Timer 5 - Hello Timer 0 - topo change timer 0
 Giga5/3: forward-transitions 1
 Giga5/3: Version Rapid Spanning Tree Protocol - **Received RSTP - Send RSTP**
 Giga5/3: No portfast configured - Current portfast off
 Giga5/3: portfast bpdu-guard default - Current portfast bpdu-guard off
 Giga5/3: portfast bpdu-filter default - Current portfast bpdu-filter off
 Giga5/3: no root guard configured - Current root guard off
 Giga5/3: Configured Link Type point-to-point - Current point-to-point

Switch(config)#inter gi5/3
 Switch(config-if-Giga5/3)#**spanning-tree force-version 0**
 Switch(config-if-Giga5/3)#do show spa inter gi5/3
 Default: Bridge up - Spanning Tree Enabled
 Default: Root Path Cost 4 - Root Port 139 - Bridge Priority 32768
 Default: Forward Delay 15 - Hello Time 2 - Max Age 20
 Default: Root Id 80000007709e12fd
 Default: Bridge Id 8000000770dead99
 Default: last topology change Wed Jan 14 12:09:00 1970
 0: 3 topology change(s) - last topology change Wed Jan 14 12:09:00 1970

Default: portfast bpdu-filter disabled
 Default: portfast bpdu-guard disabled
 Default: portfast errdisable timeout disabled
 Default: portfast errdisable timeout interval 300 sec
 Giga5/3: Port 138 - Id 808a - Role Designated - State Discarding
 Giga5/3: Designated Path Cost 4
 Giga5/3: Configured Path Cost 4 - Add type Explicit ref count 1
 Giga5/3: Designated Port Id 808a - Priority 128 -
 Giga5/3: Root 80000007709e12fd
 Giga5/3: Designated Bridge 8000000770dead99
 Giga5/3: Message Age 1 - Max Age 20
 Giga5/3: Hello Time 2 - Forward Delay 15
 Giga5/3: Forward Timer 14 - Msg Age Timer 0 - Hello Timer 0 - topo change timer 34
 Giga5/3: forward-transitions 1
 Giga5/3: Version Spanning Tree Protocol - **Received None - Send STP**
 Giga5/3: No portfast configured - Current portfast off
 Giga5/3: portfast bpdu-guard default - Current portfast bpdu-guard off
 Giga5/3: portfast bpdu-filter default - Current portfast bpdu-filter off
 Giga5/3: no root guard configured - Current root guard off

Giga5/3: Configured Link Type point-to-point - Current point-to-point

Configuring root guard for port

To set root guard on port, do the following steps on privileged EXEC mode:

	Command	Purpose
Step1	configure terminal	Enters global configuration mode.
Step2	Interface <i>interface-id</i>	Enters interface configuration mode.
Step2	spanning-tree guard root	Sets root guard on port.
Step3	exit	Back to privileged EXEC mode.
Step4	show running-config	Shows current running configuration.
Step5	copy running-config startup-config	Saves current running configuration to startup-configuration.

```
Giga5/3 of MST1isRootport Forwarding
Edge port: no (default) port guard : none (default)
Link type: point-to-point (auto) bpdu filter :disable (disable)
bpdu guard:disable (disable)
Bpdus send 0
Instance Role Sts Cost Prio.Nbr VLANs mapped
-----
1 Root FWD 20000 128.138
70
%
Switch#con t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#inter gi5/3
Switch(config-if-Giga5/3)#spanning-tree guard root
Switch(config-if-Giga5/3)#do show spa mst inter gi5/3
Giga5/3 of MST1isDesignated root-inconsistent
Edge port: no (default) port guard : root (root)
Link type: point-to-point (auto) bpdu filter :disable (disable)
bpdu guard:disable (disable)
Bpdus send 0
Instance Role Sts Cost Prio.Nbr VLANs mapped
-----
1 Desg RIT 20000 128.138
70
```

Configuring hello-time for port

You can set hello-time per port. This way is the same as the setting way of switch except entering interface mode.

Configuring portfast for port

You can set portfast per port. This way is the same as the setting way of switch except entering interface mode.

Configuring transmit-holdcount for port

You can set transmit-holdcount per port. This way is the same as the setting way of switch except entering interface mode.

Configuring restricted-role for port

To set restricted-role for port, do the following steps on privileged EXEC mode:

	Command	Purpose
Step1	configure terminal	Enters global configuration mode.
Step2	Interface <i>interface-id</i>	Enters interface configuration mode.
Step2	spanning-tree restricted-role	Sets restricted-role on port.
Step3	exit	Back to privileged EXEC mode.
Step4	show running-config	Shows current running configuration.
Step5	copy running-config startup-config	Saves current running configuration to startup-configuration.

```
U9016B_112(config)#inter gi5/3
U9016B_112(config-if-Giga5/3)#spanning-tree restricted-role
U9016B_112(config-if-Giga5/3)#do show spa
```

Default Bridge up - Spanning Tree Enabled rstp-VLAN-bridge

```
Root ID    Priority    32768
          Address    0007709e12fd
          Cost      4
          Port      139 (Giga5/4)
          Hello Time 2 sec  Max Age 20 sec  Foward Delay 15 sec
```

```
Bridge ID  Priority    32768
          Address    000770dead99
          Hello Time 2 sec  Max Age 20 sec  Foward Delay 15 sec
          Aging Time 300
```

```
Interface    Role Sts Cost      Prio.Nbr Type
-----
Giga5/3      Altn BLK 4      128.138 P2p
Giga5/4      Root FWD 4      128.139 P2p
```

```
U9016B_112(config-if-Giga5/3)#no spanning-tree restricted-role
U9016B_112(config-if-Giga5/3)#do show spa
```

```
Root ID    Priority    32768
          Address    0007709e12fd
          Cost      20000
          Port      138 (Giga5/3)
          Hello Time 2 sec  Max Age 20 sec  Foward Delay 15 sec
```

```
Bridge ID  Priority    32768
          Address    000770dead99
          Hello Time 2 sec  Max Age 20 sec  Foward Delay 15 sec
          Aging Time 300
```

Interface	Role	Sts Cost	Prio.Nbr	Type
Giga5/3	Root FWD	4	128.138	P2p
Giga5/4	Altn BLK	4	128.139	P2p

Configuring restricted-tcn for port

To set restricted-role for port, do the following steps on privileged EXEC mode.

	Command	Purpose
Step1	configure terminal	Enters global configuration mode.
Step2	Interface <i>interface-id</i>	Enters interface configuration mode.
Step2	spanning-tree restricted-tcn	Sets restricted-tcn on port.
Step3	exit	Back to privileged EXEC mode.
Step4	show running-config	Shows current running configuration.
Step5	copy running-config startup-config	Saves current running configuration to startup-configuration.

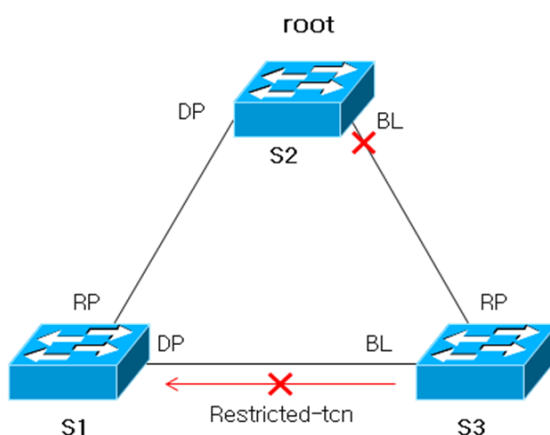


Figure 33. restricted-tcn

Configuring MSTP Features

This section describes how to set MSTP. In the MSTP. As spanning-tree is consisted of per instance, it creates instance and includes VLAN in it. Also it sets hello time and port priority like STP or RSTP.

Instance Creation and VLAN Connection

To create instance and include VLAN in it, do the following steps on privileged EXEC mode.

	Command	Purpose
Step1	configure terminal	Enters global configuration mode.
Step2	Spanning-tree mst configuration	Enters mst configuration mode to connect created instance and VLAN.
Step3	instance <i>instance-id</i> VLAN <i>VLAN-id</i>	Creates Instance ID and includes VLAN in it.

Step4	exit	Enters global configuration mode.
Step5	interface <i>interface-id</i>	Enters interface configuration mode.
Step6	Spanning-tree instance <i>instance-id</i>	Set relevant port on Instance.
Step7	exit	Back to privileged EXEC mode.
Step8	show running-config	Shows current running configuration.
Step9	copy running-config startup-config	Saves current running configuration to startup-configuration.

To delete instance, do **no instance** *instance-id* command.

```
Switch#show spanning-tree mst configuration
name      [Default]
Revision  0      Instances configured 0
%   Instance      VLAN
%   0:            2-3, 100
Switch#configure terminal
Switch(config)#spanning-tree mst configuration
Switch(config-mst)#instance 1 VLAN 2
Switch(config-mst)#exit
Switch(config)#interface GigabitEthernet 5/3
Switch(config-if-Giga5/3)#spanning-tree instance 1
Switch(config-if-Giga5/3)#exit
Switch#show spanning-tree mst configuration
name      [Default]
Revision  0      Instances configured 0
%   Instance      VLAN
%   0:            3, 100
%   1:            2
Switch# configure terminal
Switch(config)#spanning-tree mst configuration
Switch(config-mst)#no instance 1 VLAN 2
Switch(config-mst)#exit
Switch#show spanning-tree mst configuration
name      [Default]
Revision  0      Instances configured 0
%   Instance      VLAN
%   0:            2-3, 100
Switch#
```

Instance and port configuration

At MSTP, the spanning-tree runs for each instance. The priority of each instance should therefore be configured. The commands used here include each 'instance' in the commands used by STP and RSTP.

To set priority on interface, do the following steps on privileged EXEC mode:

	Command	Purpose
Step1	configure terminal	Enters Global configuration mode.
Step2	Spanning-tree mst configuration	After creating an instance, enter into the mst configuration mode to connect to the VLAN.
Step2	Spanning-tree instance instance-id priority priority	Sets priority on Instance.
Step3	exit	Back to privileged EXEC mode.
Step4	show running-config	Shows current running configuration.
Step5	copy running-config startup-config	Saves current running configuration to startup-configuration.

The following example shows how to restore to default value:

```
Switch#show spanning-tree mst
#### MST1    vlans mapped:2
Bridge      address 0007.7074.ff01  priority      32768    (32768    sysid 0)
Root        this switch for the CIST
Regional Root this switch
Operational hello time 2, forward delay 15, max age 20, txholdcount 6
Configured  hello time 2, forward delay 15, max age 20, max hops 20
Interface      Role    Sts Cost    Prio.Nbr Type
-----
Giga5/3        Disb    BLK 20000    128.138  Shared
Switch#configure terminal
Switch(config)#spanning-tree instance 1 priority 4096
Switch(config)#exit
Switch#show spanning-tree mst
#### MST1    vlans mapped:2
Bridge      address 0007.7074.ff01  priority      4096    (4096    sysid 0)
Root        this switch for the CIST
Regional Root this switch
Operational hello time 2, forward delay 15, max age 20, txholdcount 6
Configured  hello time 2, forward delay 15, max age 20, max hops 20
Interface      Role    Sts Cost    Prio.Nbr Type
-----
Giga5/3        Disb    BLK 20000    128.138  Shared
```

To set priority value on port, do the following steps on privileged EXEC mode:

	Command	Purpose
Step1	configure terminal	Enters global configuration mode.
Step2	interface interface-id	Enters interface configuration mode.
Step3	Spanning-tree instance	Sets priority on port.

	<i>instance-id</i>	priority	<i>priority</i>	
Step4	exit			Back to privileged EXEC mode.
Step5	show running-config			Shows current running configuration.
Step6	copy	running-config	startup-config	Saves current running configuration to startup-configuration.

The following example shows how to restore with default value:

```
Switch#show spanning-tree mst
#### MST1    vlans mapped:2
Bridge      address 0007.7074.ff01  priority      32768  (32768  sysid 0)
Root        this switch for the CIST
Regional Root this switch
Operational hello time 2, forward delay 15, max age 20, txholdcount 6
Configured  hello time 2, forward delay 15, max age 20, max hops 20
Interface          Role    Sts Cost      Prio.Nbr Type
-----
Giga5/3            Disb     BLK 20000      128.138  Shared
Switch#configure terminal
Switch(config)#interface GigabitEthernet 5/3
Switch(config-if-Giga5/3)#spanning-tree instance 1 priority 0
Switch(config-if-Giga5/3)#exit
Switch#show spanning-tree mst
#### MST1    vlans mapped:2
Bridge      address 0007.7074.ff01  priority      32768  (32768  sysid 0)
Root        this switch for the CIST
Regional Root this switch
Operational hello time 2, forward delay 15, max age 20, txholdcount 6
Configured  hello time 2, forward delay 15, max age 20, max hops 20
Interface          Role    Sts Cost      Prio.Nbr Type
-----
Giga5/3            Disb     BLK 20000      0.138   Shared
Switch#configure terminal
Switch(config)#interface GigabitEthernet 5/3
Switch(config-if-Giga5/3)#no spanning-tree instance 1 priority
Switch(config-if-Giga5/3)#exit
Switch#show spanning-tree mst
#### MST1    vlans mapped:2
Bridge      address 0007.7074.ff01  priority      32768  (32768  sysid 0)
Root        this switch for the CIST
Regional Root this switch
Operational hello time 2, forward delay 15, max age 20, txholdcount 6
Configured  hello time 2, forward delay 15, max age 20, max hops 20
Interface          Role    Sts Cost      Prio.Nbr Type
-----
Giga5/3            Disb     BLK 20000      128.138  Shared
```

To set the path cost value of port, do the following steps on privileged EXEC mode:

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

Step3	Spanning-tree instance <i>instance-id path-cost path-cost</i>	Sets path cost on port.
Step4	exit	Back to privileged EXEC mode.
Step5	show running-config	Shows current running configuration.
Step6	copy running-config startup-config	Saves current running configuration to startup-configuration.

To restore as default value, do **no spanning-tree instance *instance-id* path-cost** command.

```
Switch#show spanning-tree mst
#### MST1    vlans mapped:2
Bridge      address 0007.7074.ff01  priority      32768 (32768  sysid 0)
Root        this switch for the CIST
Regional Root this switch
Operational hello time 2, forward delay 15, max age 20, txholdcount 6
Configured  hello time 2, forward delay 15, max age 20, max hops 20
Interface      Role    Sts Cost      Prio.Nbr Type
-----
Giga5/3        Disb    BLK 20000     128.138  Shared
Switch#configure terminal
Switch(config)#interface GigabitEthernet 5/3
Switch(config-if-Giga5/3)#spanning-tree instance 1 path-cost 1
Switch(config-if-Giga5/3)#exit
Switch#show spanning-tree mst
#### MST1    vlans mapped:2
Bridge      address 0007.7074.ff01  priority      32768 (32768  sysid 0)
Root        this switch for the CIST
Regional Root this switch
Operational hello time 2, forward delay 15, max age 20, txholdcount 6
Configured  hello time 2, forward delay 15, max age 20, max hops 20
Interface      Role    Sts Cost      Prio.Nbr Type
-----
Giga5/3        Disb    BLK 1         128.138  Shared
Switch#configure terminal
Switch(config)#interface GigabitEthernet 5/3
Switch(config-if-Giga5/3)#no spanning-tree instance 1 path-cost
Switch(config-if-Giga5/3)#exit
Switch#show spanning-tree mst
#### MST1    vlans mapped:2
Bridge      address 0007.7074.ff01  priority      32768 (32768  sysid 0)
Root        this switch for the CIST
Regional Root this switch
Operational hello time 2, forward delay 15, max age 20, txholdcount 6
Configured  hello time 2, forward delay 15, max age 20, max hops 20
Interface      Role    Sts Cost      Prio.Nbr Type
-----
Giga5/3        Disb    BLK 20000     128.138  Shared
Switch#
```



Note

To set MSTP on the port, you must create instance before.

Setting region and revision number for MST

To set revision number and Region, do the following steps on privileged EXEC mode.

	Command	Purpose
Step1	configure terminal	Enters global configuration mode.
Step2	spanning-tree configuration mst	Enters mst configuration mode.
Step3	Region NAME	Sets region name.
Step4	Revision number	Sets revision number.
Step5	exit	Back to privileged EXEC mode.
Step6	show running-config	Shows current running configuration.
Step7	copy running-config startup-config	Saves current running configuration to startup-configuration.

```

name      [Default]
Revision  0      Instances configured 2
Instance  VLAN
-----
0          1-69, 71-4000
1          70
-----

SWITCH(config-mst)#region TEST
SWITCH(config-mst)#revision 100
SWITCH(config-mst)#do show spa mst conf
name      [TEST]
Revision  100   Instances configured 2
Instance  VLAN
-----
0          1-69, 71-4000
1          70
-----

```

Pathcost for MSTP

The pathcost value about MSTP is as follows:

speed	Path cost
10M	2000000
100M	200000
1G	20000
10G	2000

Displaying the Spanning-Tree Status

To show spanning-tree status, do the following commands on privileged EXEC mode.

Command	Purpose
show spanning-tree	Show spanning-tree information about total interface.
show spanning-tree interface <i>interface-id</i>	Shows spanning-tree information about specific interface.
show spanning-tree detail	Shows detailed spanning-tree information.

The following example shows how to show the spanning-tree information:

```
Switch#show spanning-tree
Default Bridge up - Spanning Tree Enabled rstp-VLAN-bridge
  Root ID    Priority    32768
             Address      00077074ff01
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay  15 sec
  Bridge ID  Priority    32768
             Address      00077074ff01
             Hello Time  2 sec  Max Age 20 sec  Forward Delay  15 sec
             Aging Time   300
Interface    Role Sts Cost      Prio.Nbr Type
-----
Giga5/3      Disb BLK 4      128.138 Shared
Switch#show spanning-tree interface gi5/3
% Default: Bridge up - Spanning Tree Enabled
% Default: Root Path Cost 0 - Root Port 0 - Bridge Priority 32768
% Default: Forward Delay 15 - Hello Time 2 - Max Age 20
% Default: Root Id 800000077074ff01
% Default: Bridge Id 800000077074ff01
% Default: last topology change Thu Jan 1 00:00:00 1970
% 0: 0 topology change(s) - last topology change Thu Jan 1 00:00:00 1970
% Default: portfast bpdu-filter disabled
% Default: portfast bpdu-guard disabled
% Default: portfast errdisable timeout disabled
% Default: portfast errdisable timeout interval 300 sec
% Giga5/3: Port 138 - Id 8263 - Role Disabled - State Discarding
% Giga5/3: Designated Path Cost 0
% Giga5/3: Configured Path Cost 4 - Add type Explicit ref count 1
% Giga5/3: Designated Port Id 0 - Priority 128 -
% Giga5/3: Root 000000077074ff01
% Giga5/3: Designated Bridge 000000077074ff01
% Giga5/3: Message Age 0 - Max Age 0
% Giga5/3: Hello Time 0 - Forward Delay 0
% Giga5/3: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change timer 0
% Giga5/3: forward-transitions 0
% Giga5/3: Version Rapid Spanning Tree Protocol - Received None - Sexit STP
% Giga5/3: No portfast configured - Current portfast off
% Giga5/3: portfast bpdu-guard default - Current portfast bpdu-guard off
```

```
% Giga5/3: portfast bpdu-filter default - Current portfast bpdu-filter off
% Giga5/3: no root guard configured - Current root guard off
% Giga5/3: Configured Link Type point-to-point - Current shared
%
%
Switch#show spanning-tree detail
Default is executing the rstp-VLAN-bridgecompatible Spanning Tree protocol
Bridge Identifier has priority 8000 address 00077074ff01
Configured hello time 2, max age 20, forward delay 15
We are the root of the spanning tree
Topology change flag not set, detected flagnot set
Number of topology changes 0 last change occurred Thu Jan 1 00:00:00 1970
Times: hold 6, topology change 0, notification 5
hello 2, max age 20, forward delay 15
Timers: hello 0, topology change25, notification 0, aging 300
Port 138 (Giga5/3)of Default is Discarding
Port path cost 0 Port priority 128 ,128.138.
Designated root has priority 1280, address 0007.7074.ff01
Designated bridge has priority 8000, address 0007.7074.ff01
Designated port id is 0, designated path cost 4 Hello is not pending
Number of transitions to forwarding state: 0
Link type is Shared
BPDU: sent 0
```



Note

“show spanning-tree interface IFNAME” command does not run in MSTP.

Configuring Bridge MAC Forwarding

To do MAC learning, do the following commands on config mode:

Command	Purpose
spanning-tree acquire	Sets MAC learning of Default Bridge dynamically. (It is enabled by default.)
no spanning-tree acquire	Disables it.
bridge <1-255> acquire	Sets MAC learning of Bridge except default Bridge dynamically. (It is enabled by default.)
no bridge <1-255> acquire	Disables it.
mac-address-table static MAC (forward discard) IFNAME	Forwards MAC address of relevant Bridge to interface or discards.
no mac-address-table static MAC (forward discard) IFNAME	Deletes the relevant forwarding entry of MAC address.

The following example shows how to set MAC learning statically:

```
Switch#configure terminal
Switch(config)#mac-address-table static 1111.1111.1111 forward gi5/3
Switch(config)#exit
Switch#show mac-address-table
  VLAN    mac address    type    fwd        ports
  -----
    1  1111.1111.1111    static    1 Gi5/3
Switch(config)#no mac-address-table static 1111.1111.1111 forward gi5/3
Switch(config)#exit
Switch#show mac-address-table
  VLAN    mac address    type    fwd        ports
  -----
No entries present.
Switch#
```

To delete dynamic entry and static entry from MAC address table, do the following command:

Command	Purpose
clear mac-address-table (dynamic multicast static)	Clears multicast MAC address entry in the relevant Bridge.
clear mac-address-table (static multicast dynamic) (address MACADDR interface IFNAME VLAN VID)	Clears VLAN or the physical port of muticast MAC address entry in the relevant Bridge.

The following example shows how to delete static MAC address entry:

```
Switch#show mac-address-table
      VLAN    mac address      type    fwd          ports
-----+-----+-----+-----+-----
      1  1111.1111.1111    static    1 Gi5/3

Switch#clear mac-address-table static

Switch#show mac-address-table
      VLAN    mac address      type    fwd          ports
-----+-----+-----+-----+-----

No entries present.

Switch#
```

To show MAC address entry, do the following command on EXEC mode:

Command	Purpose
show mac-address-table	Shows MAC address table information.
show mac-address-table (static dynamic multicast) VLAN <1-4094>	Shows MAC address table information as option.
show mac-address-table count (module <1-6> VLAN <1-4094>)	Shows static and dynamic multicast address number in MAC address table.

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.

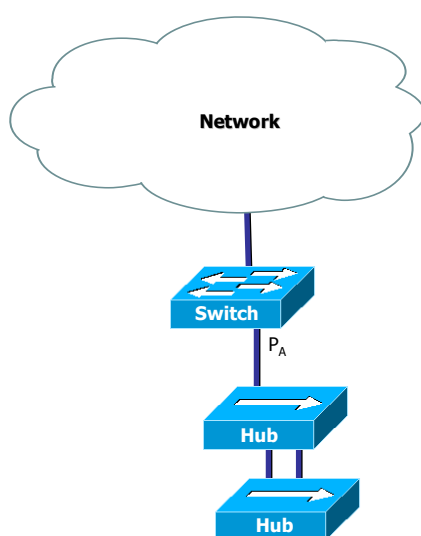


Figure 34. Environment Where a Self-loop is Formed

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:

1. Enabling Self-loop Detection
2. Changing the Service Status of Port

The following example shows how to enable self-loop detection on port gi1. as default limit time:

```

Switch# configure terminal
Switch(config)# interface vlan1
Switch(config-if-vlan1)# self-loop-detection
Switch(config-if-vlan1)# interface gi1
Switch(config-if-gi1)# self-loop-detection
Switch(config-if-gi1)# exit
Switch# show self-loop-detection
  
```

ifname	ld	link	shutdown	set_time	remain_time	count	last-occur
gi1	set	up	.	5 min	.	0	.
gi2	.	down	.	.	.	0	.
gi3	.	down	.	.	.	0	.
gi4	.	down	.	.	.	0	.
gi5	.	up	.	.	.	0	.
.....							
gi25	.	down	.	.	.	0	.
gi26	.	down	.	.	.	0	.
Switch#							

Changing the Service Status of Port

If the limit time of the port, which has been unserviceable because of the self-loop detection function, is set to 0, the port can be serviceable by manually setting it to be so.

To change the port to serviceable, execute the following procedure from the Privileged EXEC mode.

Table 193. Port enable

	Command	Purpose
Step1	Configure terminal	Enters into the global configuration mode.
Step2	interface <i>interface-name</i>	Enters into the interface configuration mode.
Step3	no shutdown	Changes the port to serviceable.
Step4	exit	Returns to the privileged EXEC mode.
Step5	show port status	Checks the status information of the port.

```
Switch# configure terminal
Switch(config)# interface vlan1
Switch(config-if-vlan1)# self-loop-detection
Switch(config-if-vlan1)# interface gi1
Switch(config-if-gi1)# no self-loop-detection
Switch(config-if-gi1)# exit
Switch# show self-loop-detection
```

ifname	ld	link	shutdown	set_time	remain_time	count	last-occur
gi1	.	up	.	.	.	0	.
gi2	.	down	.	.	.	0	.
gi3	.	down	.	.	.	0	.
gi4	.	down	.	.	.	0	.
gi5	.	up	.	.	.	0	.
.....							
gi25	.	down	.	.	.	0	.
gi26	.	down	.	.	.	0	.
Switch#							

Disabling Self-loop Detection

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

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

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

Table 194 Disabling Self-loop Detection

Step	Command	Purpose
Step1	Configure terminal	Enters global configuration mode.
Step2	interface <i>interface-name</i>	Enters Interface configuration mode.
Step3a	no self-loop-detection	Self-loop-detection shutdown caused by self-loop detection will automatically change to 'no shutdown' after 5 minutes.
Step4	interface <i>interface-name</i>	Enters interface configuration mode.
Step5a	no self-loop-detection	Self-loop-detection
Step6	exit	Changes to privileged EXEC mode.
Step7a	show running-config	Views the settings.
Step7b	show self-loop-detection	Views the self-loop settings.
Step8	copy running-config startup-config	Stores the (option) settings in the configuration file.

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

```
Switch# configure terminal
Switch(config)# interface fa1
Switch(config-if-fa1)# self-loop-detection
Switch(config-if-fa1)# end
Switch(config-if-fa1)# no self-loop-detection
Switch(config-if-fa1)# end
show self-loop-detection
```

ifname	sld	link	shutdown	set_time	remain_time	count	last-occur
gi1	.	up	.	.	.	0	.
gi2	.	down	.	.	.	0	.
gi3	.	down	.	.	.	0	.
gi4	.	down	.	.	.	0	.
gi5	.	up	.	.	.	0	.
.....							
gi25	.	down	.	.	.	0	.
gi26	.	down	.	.	.	0	.

```
Switch#
```

Displaying Self-loop Status

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

```
show self-loop-detection
```

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 example shows that the SLD of the Port gi5 is set to 5 minutes, the default time. You can see that the self-loop has been detected by the SLD on May 29 04:48:39 2006, meaning that Port gi5 has been shut down once.

Switch# **show running-config**

```
!
interface gi5
  self-loop-detection
!
interface vlan1
  self-loop-detection
  ip address 100.1.1.1/24
!
```

Switch#

Switch# **show self-loop-detection**

ifname	ld	link	shutdown	set_time	remain_time	count	last-occur
gi1	.	down	.	.	.	0	.
gi2	.	up	.	.	.	0	.
gi3	.	down	.	.	.	0	.
gi4	.	down	.	.	.	0	.
gi5	set	up	block	5 min	.	1	SEP 04:48:39 2010
gi6	.	down	.	.	.	0	.
gi7	.	down	.	.	.	0	.
gi8	.	down	.	.	.	0	.

Switch#

Chapter 13. BFD

This chapter describes BFD (Bidirectional Forwarding Detection). BFD is a protocol for rapid detecting the error of forwarding path. BFD independently runs regardless of network type and routing protocol.

This chapter consists of the following sections:

- Understanding BFD
- Restrictions BFD Configuration
- Default BFD Configuration
- Configuring BFD
- BFD Configuration Samples

Understanding BFD

BFD Operation

BFD can rapidly detect between the forwarding path error and interface, data link and forwarding layer errors. The U9016B provides a BFD asynchronous mode exchanging control message between two systems optionally. For making BFD session, you set BFD to two systems. If the BFD session is made by a routing protocol, BFD transmission period is decided by negotiating between two routers. The two routers send BFD control message periodically.

BFD can rapidly detect the error between BFD systems regardless of network type and kind of routing protocol. If BFD detects an error, it informs routing protocol. As routing protocol can rapidly reaccount routing table, it can reduce the time taken to change routing table over the total network. The following figure shows a simple network set with two routers. Each router runs OSPF and BFD. When OSPF finds out its neighbor, OSPF requests a BFD session to BFD process to make a BFD session. Then the BFD session is also made like a OSPF neighbor.

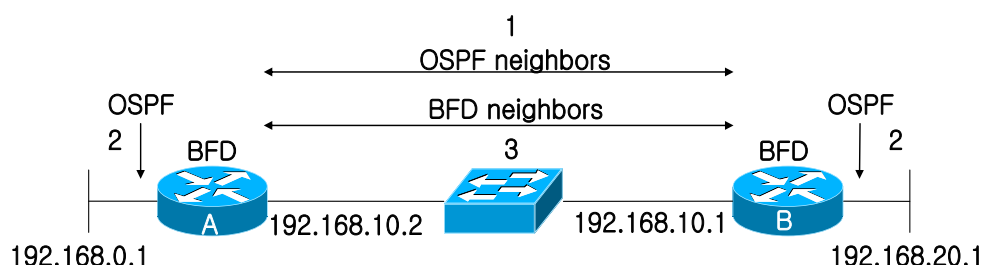


Figure 35. Establishing a BFD neighbor relationship

The following figure shows the link error to occur in the network. If OSPF neighbor and BFD session is down, the BFD informs to OSPF process that the system can not communicate with BFD peer. OSPF process disconnects the OSPF neighbor relation. If another path is available, the router recalculates the routing table immediately.

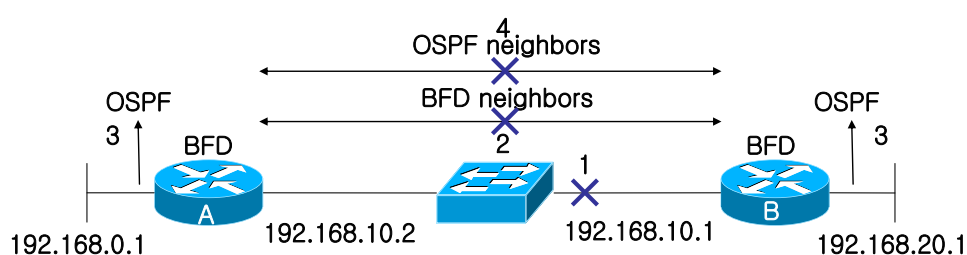


Figure 36. Tearing down an OSPF neighbor relationship

Benefits of using BFD for Failure Detection

BFD can provide failure detection in the routing protocol like OSPF. The merits of BFD are as follows:

- BFD can detect failure within one second.
- BFD can use failure detection of various routing protocols.

BFD Session Type

BFD uses BFD single hop session and BFD multi hop session according to network configuration.

BFD single hop session is used between two systems connected directly. The following figure shows BFD single hop configuration. As the two systems are directly connected via a specific interface, BFD single hop session is only made via this interface. After you set BFD session parameter on an interface of U9016B with the `bfd interval` command, BFD single hop session is made.



Figure 37. BFD single hop session

BFD multihop session is used when the connection path between two systems is optional. It differs according to routing table of network between two systems like the following figure. Therefore, BFD multihop session does not belong to specific interface. You can make BFD multihop session regardless of BFD session parameter setting on the interface. You can set BFD multihop session parameter with the `bfd multihop-peer` command.

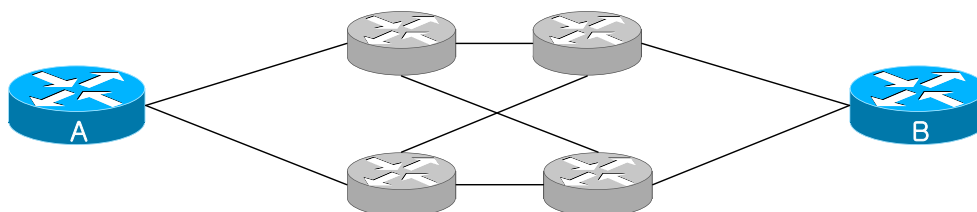


Figure 38. BFD multihop session

BFD Version Interoperability

U9016B provides not only BFD version 1 but also version 0. Even if All BFD sessions are made with version 1, it can interact with version 0.

After the system automatically detects BFD version, BFD session runs as the highest version that can use commonly with the interactive system.

For example, if one system uses version 0 and the other systems use version 0, all systems become to use version 0. You can make sure the version to use BFD session with `show bfd neighbor [details]`.

BFD Restrictions

The BFD restrictions of U9016B are as follows:

- It only supports asynchronous mode. It can start BFD session although some BFD peer.
- It supports BGP, OSPF, and static routing.
- It can make BFD session of maximum 128 numbers. When you make the session more than 128 number, the following message is displayed.

%BFD-5-SESSIONLIMIT: Attempt to exceed session limit of 128 neighbors.

- It provides all BFD functions from control plane. So if the CPU utilization increases, the error detection possibility by packet loss increases. In this case, you must adjust required minimum receive interval with proper value.

Default BFD Configuration

The following table shows the basic BFD configuration:

Table 195 Default BFD Configuration

Feature	Default Setting
BFD	Enable.
Interface passive mode	Active mode.
BFD Echo packet reception	Disable
BFD Echo mode	No use
Desired transmit interval	750 msec (Multihop session)
Required minimum receive interval	500 msec (Multihop session)
Multiplier	3 (Multihop session)
BFD Slow-timer	1000 msec

Desired transmit interval, Required minimum receive interval and Multiplier are important BFD session parameters. To make BFD single hop session, you set this parameter value directly with bfd interval command.

If bfd multihop-peer configuration for BFD multihop session does not exist, use the values defined in the table.

Configuring BFD

This section describes BFD configuration as follows:

- Configuring BFD session parameters on the interface
- Configuring BFD multi-hop session parameters
- Configuring BFD support for BGP
- Configuring BFD support for OSPF
- Configuring BFD support for static routing
- Configuring Passive Mode on the Interface
- Configuring BFD slow timer
- Configuring BFD echo mode
- Monitoring and Troubleshooting BFD

Configuring BFD session parameters on the interface

To configure BFD session parameters on the interface, do the following tasks:

Table 196 Configuring BFD session parameters on the interface

Step	Command or Action	Purpose
Step 1	configure terminal Example: Switch# configure terminal	Enters the global configuration mode.
Step 2	interface <i>interface-name</i> Example: Switch(config)# interface gi2/2/1	Enter the interface configuration mode.
Step 3	ip address <i>ip-address/prefix-length</i> Example: Switch(config-if-Giga2/2/1)# ip address 33.1.1.1/24	Sets IP address on interface.
Step 4	bfd interval <i>minlliseconds</i> min_rx <i>milliseconds</i> multiplier <i>interval-multiplier</i> Example: Switch(config-if-Giga2/2/1)# bfd interval 750 min_rx 500 multiplier 3	Sets BFD parameter on interface.
Step 5	end Example: Switch(config-if-Giga2/2/1)# end	Returns the privileged EXEC mode.



Note

You must set BFD parameter on relevant interface with **bfd interval** command to make single-hop BDF session

Configuring multi-hop BFD session parameters

You must configure multi-hop BFD session parameters per BFD peer. To configure multi-hop BFD session parameters, do the following tasks:

Table 197 Configuring multi-hop BFD session parameters

Step	Command or Action	Purpose
Step 1	configure terminal Example: Switch# configure terminal	Enters the global configuration mode.
Step 2	bfd multihop-peer A.B.C.D interval minliseconds min_rx milliseconds multiplier interval-multiplier Example: Switch(config)# bfd multihop-peer 10.1.1.1 interval 750 min_rx 500 multiplier 3	Sets multi-hop BFD session parameter
Step 3	End Example: Switch(config)# end	Returns the privileged EXEC.

Configuring BFD support for BGP

To configure BFD on BGP, do the following tasks.

Table 198 Configuring BFD support for BGP

Step	Command or Action	Purpose
Step 1	configure terminal Example: Switch# configure terminal	Enters the global configuration mode.
Step 2	router bgp as-tag Example: Switch(config)# router bgp 100	Enters the BGP router mode.
Step 3	neighbor ip-address fall-over bfd Example: Switch(config-router)# neighbor 3.3.3.2 fall-over bfd	Enables BFD for checking connection status with BGP neighbor.
Step 4	end Example: Switch(config-router)# end	Returns to the privileged EXEC.

Configuring BFD support for OSPF

You can configure BFD on OSPF with the following ways.

- You can make BFD session for all OSPF interface excepting OSPF virtual link with `bfd all-interface` command in OSPF routing configuration mode.
- You can make BFD session for specific interface of OSPF with `ip ospf bfd` command in the interface mode.

Configuring BFD support for OSPF for all interface

To configure BFD session on all OSPF interface, do the following tasks:

Table 199 Configuring BFD support for OSPF for all interface

Step	Command or Action	Purpose
Step 1	configure terminal Example: Switch# configure terminal	Enters global configuration mode.
Step 2	router ospf process-id Example: Switch(config)# router ospf 10	Enter OSPF routing configuration mode.
Step 3	bfd all-interfaces Example: Switch(config-router)# bfd all-interface	Set to make BFD session for all OSPF interface.
Step 4	exit Example: Switch(config-router)# exit	Return to global configuration mode.
Step 5	interface type number Example: Switch(config)# interface gi2/1/1	Enter interface configuration mode.
Step 6	bfd interval milliseconds min_rx milliseconds multiplier interval-multiplier Example: Switch(config-if-Giga2/2/1)# bfd interval 750 min_rx 500 min 3	Sets BFD session parameter value on OSPF interface.
Step 7	interface type number Example: Switch(config)# interface gi2/2/1	Enters interface configuration mode (Optional).
Step 8	ip ospf bfd [disable] Example: Switch(config-if-Giga2/2/1)# ip ospf bfd disable	Disable BFD session for specific OSPF interface. disable keyword command must be used only for interace enabled BFD.
Step 9	end Example: Switch(config-if-Giga2/2/1)# end	Return to privileged EXEC mode.

Configure BFD Support for OSPF for One or More Interface

To configure BFD session on the specific OSPF interface, do the following tasks:

Table 200 Configure BFD Support for OSPF for One or More Interface

Step	Command or Action	Purpose
Step 1	configure terminal Example: Switch# configure terminal	Enters global configuration mode.
Step 2	interface type number Example: Switch(config)# interface gi2/1/1	Enters interface configuration mode.
Step 3	bfd interval minlliseconds min_rx milliseconds multiplier interval-multiplier Example: Switch(config-if-Giga2/2/1)# bfd interval 750 min_rx 500 multiplier 3	Sets BFD parameter on interface.
Step 4	ip ospf bfd [disable] Example: Switch(config-if-Giga2/1/1)# ip ospf bfd	Sets to make BFD session via OSPF interface.
Step 5	end Example: Switch(config-if-Giga2/1/1)# end	Return to privileged EXEC mode.

Configuring BFD support for Static routing

To configure BFD for Static routing, do the following tasks:

Table 201 Configuring BFD support for Static routing

Step	Command or Action	Purpose
Step 1	configure terminal Example: Switch# configure terminal	Enters the global configuration mode.
Step 2	interface interface-name Example: Switch(config)# interface gi2/2/1	Enters the interface configuration mode.
Step 3	ip address ip-address/prefix-length Example: Switch(config-if-Giga2/2/1)# ip address 1.1.1.1/24	Assigns IP address on interface.
Step 4	bfd interval milliseconds min_rx milliseconds multiplier interval-multiplier Example: Switch(config-if-Giga2/2/1)# bfd interval 750 min_rx 500 min 3	Sets BFD session parameter value on interface.
Step 5	Exit Example: Switch(config-if-Giga2/2/1)# exit	Return to global configuration mode.
Step 6	ip route A.B.C.D/M gateway-addr	Sets static router.

	Example: Switch(config)# ip route 7.0.0.0/8 1.1.1.254	
Step 7	ip route static bfd <i>IFNAME gateway-addr</i> Example: Switch(config)# ip route static bfd gi2/2/1 1.1.1.254	Assign BFD neighbor of static route.
Step 8	end Example: Switch(config)# end	Return to privileged EXEC mode.

Configuring Passive Mode on the Interface

After BFD passive mode receives packet from another BFD neighbor to BFD control, start to send BFD control packet. In other words, it does not send BFD control packet at first. If BFD runs with passive mode, you set interface with the following tasks.

If you set all routers in the network with BFD passive mode, the BFD does not run. At least BFD of one system must run with active mode.

Table 202 Configuring Passive Mode on the Interface

Step	Command or Action	Purpose
Step 1	configure terminal Example: Switch# configure terminal	Enters the global configuration mode.
Step 2	interface <i>interface-name</i> Example: Switch(config)# interface gi2/2/1	Enters interface configuration mode.
Step 3	bfd passive Example: Switch(config-if-Giga2/2/1)# bfd passive	Sets interface with BFD passive mode.
Step 4	end Example: Switch(config-if-Giga2/2/1)# end	Return to privileged EXEC mode.

Configuring BFD Echo Mode

The system that receives BFD echo packet from BFD echo mode returns this packet to the sending system. In the case of using BFD Echo packet, the sending period of BFD control packet is longer. So you can reduce BFD control packet number sent or received between BFD neighbors. The default setting of BFD echo mode is enabled.

Table 203 Configuring BFD Echo Mode

Step	Command or Action	Purpose
Step 1	configure terminal Example: Switch# configure terminal	Enters the global configuration mode.
Step 2	bfd echo [accept send] Example: Switch(config)# bfd echo	Enable BFD echo mode. - accept keyword use when it receive Echo packet. - send keyword use when it sends Echo packet.

Step 3	end Example: Switch(config)# end	Returns privileged EXEC mode.
--------	---	-------------------------------

Configuring BFD slow timer

In the case that BFD session status dose not up, to configure BFD slow timer, do the following tasks:

Table 204 Configuring BFD slow timer

Step	Command or Action	Purpose
Step 1	configure terminal Example: Switch# configure terminal	Enters the global configuration mode.
Step 2	bfd slow-timer <i>milliseconds</i> Example: Switch(config)# bfd slow-timer 2000	Sets BFD slow timer.
Step 3	end Example: Switch(config)# end	Returns privileged EXEC mode.

Displaying BFD information

Table 205 Displaying BFD information

Step	Command or Action	Purpose
Step 1	show bfd neighbor [detail] Example: Switch# show bfd neighbor details	Shows BFD adjacency database (optional). - Detail keyword shows all BFD protocol parameter and timer.
Step 2	debug bfd [echo event fsm loopback neighbor nsm packet] Example: Switch# debug bfd packet	Shows debugging information about BFD (optional).

BFD Configuration Samples

The section includes the following examples:

- Sample One: Configuring BFD in an OSPF Network
- Sample Two: Configuring BFD in an BGP Network
- Sample Three: Configuring BFD for static routing

Sample One: Configuring BFD in an OSPF Network

This example describes the way of using BFD in OSPF network. Let us assume the following network configuration:

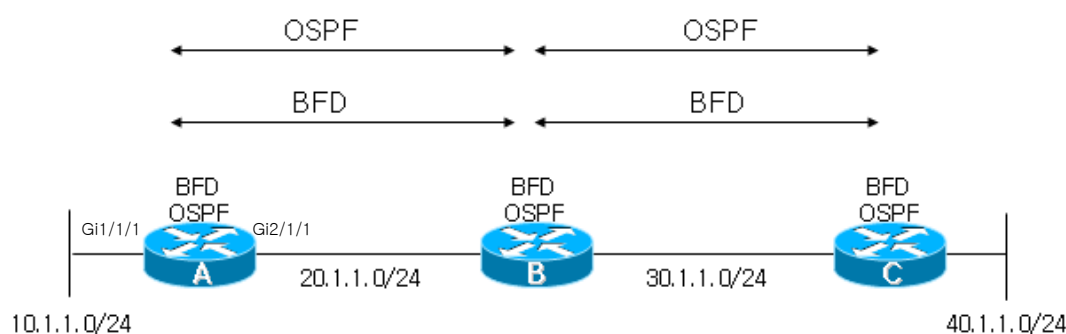


Figure 39. Configuring BFD in an OSPF Network

You must set BFD on OSPF interface. To set BFD on OSPF interface, do the following tasks:

- Set BFD on all OSPF interface.
- Set BFD on specific OSPF interface optionally.

Configuring BFD Support for OSPF for All Interfaces

To use BFD on all OSPF interface, do the following tasks:

Table 206 Configuring BFD in an OSPF Network

Step	Description
Step 1	Set OSPF. Switch_A# configure terminal Switch_A(config)# router ospf 100 Switch_A(config-router)# network 10.1.1.0/24 area0 Switch_A(config-router)# network 20.1.1.0/24 area0
Step 2	Sets BFD session parameter. Switch_A# configure terminal Switch_A(config)# interface gi2/1/1 Switch_A(config-if-Giga2/1/1)# bfd interval 300 min_rx 300 multiplier 3
Step 3	Enables BFD on all OSPF interface. Switch_A# configure terminal Switch_A(config)# router ospf Switch_A(config-router)# bfd all-interfaces

Step 4	Disables BFD session to interface not to connect with OSPF neighbor. Switch_A# configure terminal Switch_A(config)# interface gi1/1/1 Switch_A(config-if-Giga1/1/1)# ip ospf bfd disable
Step 5	Shows BFD peer information. Switch_A# show bfd neighbors



Note

If you disable BFD at the specific interface only with being set the bfd all-interface status, use ip ospf bfd disable command.

The configuration of switch is as follows:

```

!
interface Giga1/1/1
 ip address 10.1.1.1/24
 ip ospf bfd disable
!
interface Giga2/1/1
 ip address 20.1.1.1/24
 bfd interval 300 min_rx 300 multiplier 3
!
router ospf 100
 network 10.1.1.0/24 area0
 network 20.1.1.0/24 area0
 bfd all-interfaces
!

```

Configuring BFD Support for OSPF for One or More Interfaces

To use BFD on specific OSPF interface, do the following tasks:

Table 207 BFD on specific OSPF interface

Step	Description
Step 1	Sets OSPF Switch_A# configure terminal Switch_A(config)# router ospf 100 Switch_A(config-router)# network 10.1.1.0/24 area0 Switch_A(config-router)# network 20.1.1.0/24 area0
Step 2	Sets Single hop BGP session and sets bfd session parameter. Switch_A# configure terminal Switch_A(config)# interface gi2/1/1 Switch_A(config-if-Giga2/1/1)# bfd interval 300 min_rx 300 multiplier 3
Step 3	Sets BFD on the specific OSPF interface. Switch_A# configure terminal Switch_A(config)# interface gi2/1/1

	Switch_A(config-if-Giga2/1/1)# ip ospf bfd
Step 4	Shows BFD peer information.. Shows BFD peer. Switch_A# show bfd neighbors

The configuration of switch is as follows:

```
!
interface Giga2/1/1
ip address 20.1.1.1/24
ip ospf bfd
bfd interval 300 min_rx 300 multiplier 3
!
router ospf 100
network 10.1.1.0/24 area0
network 20.1.1.0/24 area0
!
```

Sample Two: Configuring BFD in an BGP Network

The example below describes the way of using BFD in BGP network.

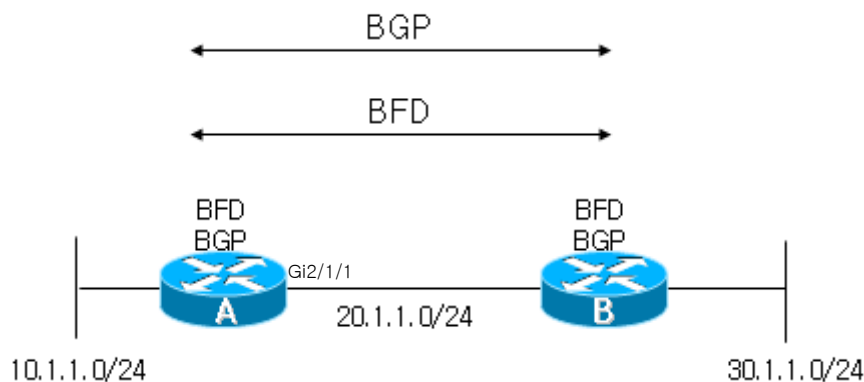


Figure 40. Configuring BFD in an BGP Network

You must configure BFD per each BGP neighbor. You set BGP to BGP neighbor and the ways setting BFD session parameter differ according to the following two cases.

- Configuring BFD Support for connected external BGP
- Configuring BFD Support for Multihop-External BGP and Internal BGP

Configuring BFD Support for connected external BGP

To use BFD about specific BGP peer on BGP, do the following tasks:

Table 208 Configuring BFD in an BGP Network

Step	Description
Step 1	Sets BGP.

	Switch_A# configure terminal Switch_A(config)# router bgp 80 Switch_A(config-router)# neighbor 20.1.1.81 remote-as 81
Step 2	Sets BFD to specific neighbor and session on BGP. Switch_A# configure terminal Switch_A(config)# router bgp 80 Switch_A(config-router)# neighbor 20.1.1.81 fall-over bfd
Step 3	Enables Single hop BGP session and sets bfd session parameter. Switch_A# configure terminal Switch_A(config)# interface gi2/1/1 Switch_A(config-if-Giga2/1/1)# bfd interval 300 min_rx 300 multiplier 3
Step 4	Shows BFD peer information. Switch_A# show bfd neighbors

The configuration of switch is as follows:

```
!
interface Giga2/1/1
 ip address 20.1.1.1/24
 bfd interval 300 min_rx 300 multiplier 3
!
router bgp 80
 neighbor 20.1.1.81 remote-as 81
 neighbor 20.1.1.81 fall-over bfd
!
```

Configuring BFD Support for Internal BGP

To use BFD on internal BGP, do the following tasks:

Table 209 BFD on internal BGP

Step	Description
Step 1	Sets Internal BGP.
	Switch_A# configure terminal Switch_A(config)# router bgp 80 Switch_A(config-router)# neighbor 20.1.1.81 remote-as 80
Step 2	Sets BGP to use BFD to session with specific neighbor.
	Switch_A# configure terminal Switch_A(config)# router bgp 80 Switch_A(config-router)# neighbor 20.1.1.81 fall-over bfd
Step 3 (Option)	Sets Multihop bfd session parameter
	Switch_A# configure terminal Switch_A(config)# bfd multihop-peer 20.1.1.81 interval 900 min_rx 500 multiplier 3
Step 4	Shows BFD peer information.
	Switch_A# show bfd neighbors

The configuration of switch is as follows:

```
!
interface Giga2/1/1
 ip address 20.1.1.1/24
!
bfd multihop-peer 20.1.1.81 interval 900 min_rx 500 multiplier 3
!
router bgp 80
 neighbor 20.1.1.81 remote-as 80
 neighbor 20.1.1.81 fall-over bfd
!
```

Sample Three: Configuring BFD for static routing

The example below describes the way of using BFD in the network using static routing:

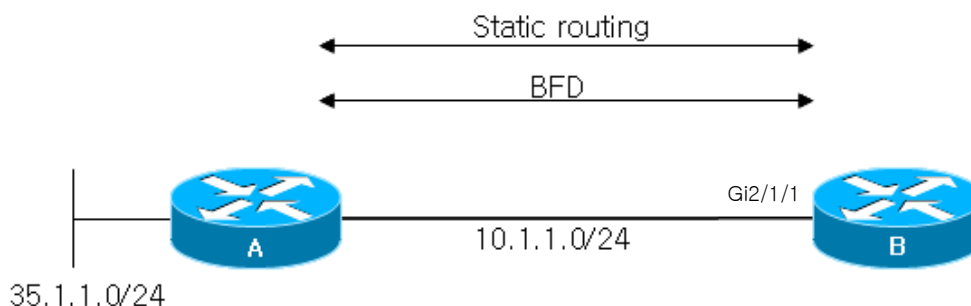


Figure 41. Configuring BFD for static routing

If you use BFD to check that next-hop to specific static router is active status actually, do the following tasks:

Table 210 Configuring BFD for static routing

Step	Description
Step 1	Sets Static route. Switch_B# configure terminal Switch_B(config)# ip route 35.1.1.0/24 10.1.1.254
Step 2	Enables Single hop BGP session and sets bfd session parameter. Switch_B# configure terminal Switch_B(config)# interface gi2/1/1 Switch_B(config-if-Giga2/1/1)# bfd interval 300 min_rx 300 multiplier 3
Step 3	Enable BFD for failure detection with next hop of Static route. Switch_B# configure terminal Switch_B(config)# ip route static bfd gi2/1/1 10.1.1.254
Step 4	Shows BFD peer information. Switch_B# show bfd neighbors



Note

To become BFD session to UP status, you must also set BFD on Switch A conneted with Switch B interface.

The configuration of Switch_B is as follows:

```
!
interface Giga2/1/1
 ip address 10.1.1.1/24
 bfd interval 300 min_rx 300 multiplier 3
 ip route 35.1.1.0/24 10.1.1.254
 ip route static bfd gi2/1/1 10.1.1.254
```


Chapter 14. LACP

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

**Note**

For the syntax and direction of commands used in this chapter, refer to command reference.

This chapter consists of the following sections:

- Understanding the Link Aggregation Control Protocol
- Configuring 802.3ad Link Aggregation Control Protocol and static link aggregation
- Displaying 802.3ad Statistics and Status

Understanding Link Aggregation Control Protocol

Link Aggregation Control Protocol (LACP) is part of an IEEE specification (802.3ad) that allows you to bundle several physical ports together to form a single logical channel. LACP allows a switch to negotiate an automatic bundle by sending LACP packets to the peer.

This chapter includes the following descriptions:

- LACP Concept
- LACP Modes
- LACP Parameters

LACP Operation Principle

LACP is configured in both connected systems. So they exchange the LACPDU to decide the interface status and the link aggregation. The interface where LACP has been configured passes through various statuses through LACPDU. When the conditions of two systems match, link aggregation occurs. When LACP is configured, a logical interface is created. Any interface which receives LACPDU recognizes that LACP is configured in the connected system. The interface then checks its LACPDU transfer interval and sends LACPDU according to the interval. It then checks whether the information received through LACPDU is identical with the information that it has. If it is identical, it connects the physical interface to the logical interface.

LACPDU Configuration

LACPDU has the information of the opponent and the information of the interface that transfers the LACPDU. By using this information, each interface saves such information and compares it to that of the next LACPDU. The following table shows the information included in the LACPDU.

Table 211. LACPDU Configuration

Field	description
Actor_System_Priority	Priority configured to the system
Actor_System	ID made by using the MAC and priority of the system
Actor_Key	logical interface ID
Actor_Port_Priority	Port priority
Actor_Port	Port index
Actor_State	The value of the port status (in the unit of bit)
Partner_System_Priority	System priority of the opponent system
Partner_System	System ID of the opponent system
Partner_Key	ID of the logical interface of the opponent system
Partner_Port_Priority	Priority of the opponent port
Partner_Port	Index of the opponent port
Partner_State	Status of the opponent port

LACP Modes

Port group configuration of U9016B 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 imitate the sending LACP packets.

The following shows the possible mode in LACP:

Table 212 LACP Modes

Mode	Description
on	This mode do not create port group by LACP. It creates static port group.
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 as 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 is assigned to each port of switch according to feature of port automatically. Administrative key feature are bandwidth, VLAN id, duplex, and mtu. In the case of the same value, the port can be a part of logical interface.

When LACP is enabled, LACP always attempts to aggregate the maximum 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 ports fails.

Configuring LACP and SLA

This section describes how to configure port group with LACP:

- Specifying the System Priority
- Specifying the Port Priority
- Specifying an Administrative Key Value
- Specifying the Timeout Value
- Configuration LACP and static port group
- Clearing LACP Statistics

Specifying the System Priority

The system priority value should be an integer between 1 and 65535. Higher the number represents lower the priority. The default priority is 32768.

To specify LACP system priority, follow the steps below from privileged EXEC mode:

Table 213 Specifying the System Priority

Step	Command	Purpose
Step1	configure terminal	Enters global configuration mode
Step2	lacp system-priority <i>priority</i>	Specifies the system priority
Step3	end	Return the privileged EXEC mode
Step4	show lacp sys-id	Checks the setting
Step5	copy running-config startup-config	Saves the setting in configuration file (optional)

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 should 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.

Table 214 Specifying the Port Priority

Step	Command	Purpose
Step1	configure terminal	To enter global configuration mode.
Step2	interface <i>interface-id</i>	To enter to interface configuration mode.
Step3	lacp port-priority <i>priority</i>	To specify the port priority
Step4	end	To return to privileged EXEC mode
Step5	show running-config	To check the setting
Step6	copy running-config startup-config	To save the setting in configuration file (optional)

To return the port priority to default setting, use interface configuration command “no lacp port-priority”

The following example shows how to set the port-priority of interface gi6/1 to 10:

```
Switch# configure terminal
Switch(config)# interface Giga6/1
Switch(config-if-Giga6/1)# lacp port-priority 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

lacp timeout command affects to LACPDU sending period of the relative switch.

To specify the timeout value, follow the steps below from the privileged EXEC Mode:

Table 215 Specifying the Timeout Value

Step	Command	Purpose
Step1	configure terminal	To enter global configuration mode
Step2	interface <i>interface-id</i>	Enter to interface configuration mode.
Step3	lacp timeout {short long}	To specify LACPDU Timeout
Step4	end	To return to privileged EXEC mode
Step5	show running-config	To check the setting
Step6	copy running-config startup-config	To save the setting in configuration file (optional)

To return the LACPDU Timeout as default, use Interface Configuration Command “no lacp timeout”.

The following example shows how to set the transmission interval of LACPDU that is connected to gi6/1 to short.

```
Switch# configure terminal
Switch(config)# interface Giga6/1
Switch(config-if-Giga6/1)# lacp timeout short
Switch(config)# end
```

Configuration LACP and static port group

You can configure the interface of LACP mode.

To change the LACP mode, follow the steps below from the privileged EXEC Mode.

Table 216 Configuration LACP and static port group

Step	Command	Purpose
Step1	configure terminal	Enters global configuration mode
Step2	interface <i>interface-id</i>	Enters the interface configuration mode.
Step3	Channel-group <i>po-id</i> mode {active on passive}	Set port group mode. active, passive: LACP mode on: static port group
Step4	end	Return the privileged EXEC mode
Step5	show running-config	Checks the setting
Step6	copy running-config startup-config	Saves the setting in configuration file (optional)

This example shows how to set the interface giga 6/1 as a port-group 1 member.

```
Switch# configure terminal
Switch(config)# interface Giga6/1
Switch(config-if- Giga6/1)# channel-group 1 mode active
Switch(config)# end
```

The following example shows how to create port-group by static mode.

```
Switch# configure terminal
Switch(config)# interface Giga6/1
Switch(config-if- Giga6/1)# channel-group 1 mode on
Switch(config)# end
```

Clearing LACP Statistics

To clear/delete LACP statistics, follow the steps below from the privilege EXEC mode.

Table 217 Clearing LACP Statistics

Step	Command	Purpose
Step1	clear lacp [aggregator-id] counters	Clears LACP statistics of the port group
Step2	show lacp counters	Checks the modification

The following is an example of deleting LACP statistics of port group 1:

```
Switch# clear lacp 1 counters
```

Displaying 802.3ad Statistics and Status

U9016B provides various commands to show the information of all ports.

Table 218 Displaying 802.3ad Statistics and Status

Command	Purpose
show etherchannel	Shows the information of port connected with port group.
show etherchannel summary	Shows the brief information of port connected with port group.
show etherchannel detail	Shows the detail information of port conneted with port group.

The following example shows how to show the information of the static port group:

```
shu#show etherchannel
```

Channel-group listing:

Group: 1

Group state = L2

Ports: 1 Max Maxports = 8

Port-channels: 1 Max Port-channels = 8

Protocol= -

```
shu#show etherchannel summary
```

Flags: D - down P - bundled in port-channel

I - stand-alone s - suspended

H - Hot-standby (LACP only)

R - Layer3

S - Layer2

U - in use

f - failed to allocate aggregator

M - not in use, minimum links not met

u - unsuitable for bundling

w - waiting to be aggregated

Number of channel-groups in use: 1

Number of aggregators: 1

Group	Port-channel	Protocol	Ports
-------	--------------	----------	-------

1	Po1(SD)	-	Gi6/1(D)
---	---------	---	----------

```
shu#show etherchannel detail
```

Channel-group listing:

Group: 1

Group state = L2

Ports: 1 Max Maxports = 8

Port-channels: 1 Max Port-channels = 8

Protocol= -

Ports in the group:

Port: Gi6/1

Port state = Down Not-in-Bndl

Channel group = 1

Port-channel = NULL

nel1

Mode = On

GC = -

Gcchange = -

Pseudo port-channel= Port-chan

Port index = 0 Load = 0x00
Protocol = -

Age of the port in the current state: 0d:16h44m24s

Port-channels in the group:

Port-channel: Port-channel1

Age of the Port-channel = 0d:0h0m18s
Number of ports = 0
GC = 0x00000000 HotStandBy port= null
Port state = Down Ag-Not-Inuse
Protocol = -
shu#

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 15. IP-OPTION

This chapter describes the IP-option of system.

IP option is the function to enable/disable the parameters related with attack prevention of the parameters under `/proc/sys/net/ipv4` provided by linux kernel.

IP OPTOIN command

The parameters that can be set by IP option are as follows.

Table 219 IP OPTION command

Command	Description	Mode
ip option icmp-drop icmp-type (any <0-255> echo-request echo-reply) length <1-65535>	Sets the icmp-type and packet size for blocking ICMP packets.	Config
no ip option icmp-drop	Disables ICMP packet blocking.	Config
ip icmp-ttl-exceed-send	Enables/Disables to send TTL Exceed ICMP errors. Default: send	Config
no ip icmp-ttl-exceed-send	Disables to send TTL Exceed ICMP errors.	Config
ip option icmp-unreachable-send	Allows / blocks to send ICMP unreachable. Default: send	Config
no ip option icmp-unreachable-send	Disable to send ICMP unreachable errors.	Config
ip option ip_default_ttl VALUE	Sets the Default TTL size. Default: 64	Config
no ip option ip_default_ttl	Changes the Default TTL size to the default value.	Config
ip option ipfrag_time VALUE	Sets the duration of IP fragment in the memory. Default: 30	Config
no ip option ipfrag_time	Changes the duration of IP fragment in the memory to the default value.	Config
ip option tcp-conn-rate-limit profile-id <1-128> (any PORT) period <1-3600> count <1-65535>	Adds a TCP connection rate-limit profile. TCP connection trials to the TCP destination port within period for more than the count value can be logging or blocked.	Config
no ip option tcp-conn-rate-limit profile-id <1-128>	Deletes the TCP connection rate-limit profile for the Profile-id.	Config
ip option tcp_fin_timeout VALUE	Sets the socket duration in FIN-WAIT-2 state. Default: 60	Config
no ip option tcp_fin_timeout	Change the socket duration in FIN-WAIT-2 state to the default value.	Config
ip option tcp_keepalive_probes VALUE	Sets the number of keepalive probe message to generate by the time the connection is determined to be disconnected. Default: 9	Config
no ip option tcp_keepalive_probes	Changes the number of Keepalive probe messages to the default value.	Config
ip option tcp_keepalive_time VALUE	Sets the keepalive message transmit time when Keepalive is activated. Default: 7200	Config
no ip option tcp_keepalive_time	Changes the Keepalive message transmit time to the default value.	Config

ip option tcp_max_syn_backlog <i>VALUE</i>	Sets the maximum value of TCP syn backlog queue. Default: 1024	Config
no ip option tcp_max_syn_backlog	Changes the maximum value of TCP syn backlog queue to the default value.	Config
ip option tcp_max_tw_buckets <i>VALUE</i>	Sets the number of Timewait sockets. Default: 18700	Config
no ip option tcp_max_tw_buckets	Changes the number of Timewait sockets to the default value.	Config
ip option tcp_retries1 <i>VALUE</i>	Sets the number of retransmits for suspected TCP session. Default: 3	Config
no ip option tcp_retries1	Changes the number of retransmits for suspected TCP session.	Config
ip option tcp_retries2 <i>VALUE</i>	Sets the number of retransmits before termination. Default: 15	Config
no ip option tcp_retries2	Changes the number of retransmits before termination to the default value.	Config
ip option tcp_syn_retries <i>VALUE</i>	Sends the initialization SYN packet after the specified time for retransmission in active TCP connection. Default: 5	Config
no ip option tcp_syn_retries	Changes the TCP syn re-transmission time to the default value.	Config
ip option tcp_syncookies (default disable enable)	Sets Syn flood attack defense. Default: enable	Config
ip option Telnet-acl access-group <1-99>	Sets to allow/block Telnet from accessing to the access-groups.	Config
no ip option Telnet-acl access-group <1-99>	Disables Telnet access limit configuration by Access-group.	Config

IPv6 OPTOIN Overview

IPv6 OPTION is the function that drops or does rate-limiting ICMPv6 packet to come in system CPU by using ip6tables.

IPv6 OPTION DROP Command

Table 220 IPv6 OPTION DROP Command

Command	Description	Mode
ipv6 option icmpv6-drop icmpv6-type <0-255> length <1-65535>	Sets icmp-type and packet size to drop ICMPv6 packet.	Config
ipv6 option icmpv6-drop icmpv6-type destination-unreachable length <1-65535>	Drops destination-unreachable packet.	Config
ipv6 option icmpv6-drop icmpv6-type packet-too-big length <1-65535>	Drops Packet-too-big packet.	Config
ipv6 option icmpv6-drop icmpv6-type time-exceeded length <1-65535>	Drops time-exceeded packet.	Config
ipv6 option icmpv6-drop icmpv6-type parameter-problem length <1-65535>	Drops parameter-problem packet.	Config
ipv6 option icmpv6-drop icmpv6-type echo-reply length <1-65535>	Drops echo-reply packet.	Config
ipv6 option icmpv6-drop icmpv6-type echo-request length <1-65535>	Drops echo-request packet.	Config
ipv6 option icmpv6-drop icmpv6-type mld-query length <1-65535>	Drops mld-query packet.	Config
ipv6 option icmpv6-drop icmpv6-type mld-report length <1-65535>	Drops mld-report packet.	Config
ipv6 option icmpv6-drop icmpv6-type mld-done length <1-65535>	Drops mld-done packet.	Config
ipv6 option icmpv6-drop icmpv6-type router-solicitation length <1-65535>	Drops router-solicitation packet.	Config
ipv6 option icmpv6-drop icmpv6-type router-advertisement length <1-65535>	Drops router-advertisement packet.	Config
ipv6 option icmpv6-drop icmpv6-type neighbor-solicitation length <1-65535>	Drops neighbor-solicitation packet.	Config
ipv6 option icmpv6-drop icmpv6-type neighbor-advertisement length <1-65535>	Drops neighbor-advertisement packet.	Config
ipv6 option icmpv6-drop icmpv6-type redirect length <1-65535>	Drops Redirect packet.	Config
ipv6 option icmpv6-drop icmpv6-type mld-reportv2 length <1-65535>	Drops mld-reportv2 packet.	Config
ipv6 option icmpv6-drop icmpv6-type ha-addr-request length <1-65535>	Drops ha-addr-request packet.	Config
ipv6 option icmpv6-drop icmpv6-type ha-addr-reply length <1-65535>	Drops ha-addr-reply packet.	Config

ipv6 option icmpv6-drop icmpv6-type ma-prefix-solicitation length <1-65535>	Drops ma-prefix-solicitation packet.	Config
ipv6 option icmpv6-drop icmpv6-type ma-prefix-advertisement length <1-65535>	Drops ma-prefix-advertisement packet.	Config
ipv6 option icmpv6-drop icmpv6-type certification-path-solicitation length <1-65535>	Drops certification-path-solicitation packet.	Config
ipv6 option icmpv6-drop icmpv6-type certification-path-advertisement length <1-65535>	Drops certification-path-advertisement packet.	Config
no ipv6 option icmpv6-drop	Disables to drop ICMPv6 packet.	Config

IPv6 OPTOIN RATE-LIMIT Command

The following table shows the parameters to be set with RATE-LIMIT command of IPv6 OPTION.

Table 221 IPv6 OPTION RATE-LIMIT Command

Command	Description	Mode
ipv6 option icmpv6-rate-limit icmpv6-type <0-255> rate <1-10000> scale (second minute hour day) (burst <1-10000>)	Sets the icmp-type and the packet size for ICMPv6 packet rate-limit.	Config
ipv6 option icmpv6-rate-limit icmpv6-type destination-unreachable rate <1-10000> scale (second minute hour day) (burst <1-10000>)	Sets the rate-limit at destination-unreachable packet.	Config
ipv6 option icmpv6-rate-limit icmpv6-type packet-too-big rate <1-10000> scale (second minute hour day) (burst <1-10000>)	Sets the rate-limit at packet-too-big packet.	Config
ipv6 option icmpv6-rate-limit icmpv6-type time-exceeded rate <1-10000> scale (second minute hour day) (burst <1-10000>)	Sets the rate-limit at time-exceeded packet.	Config
ipv6 option icmpv6-rate-limit icmpv6-type parameter-problem rate <1-10000> scale (second minute hour day) (burst <1-10000>)	Sets the rate-limit at parameter-problem packet.	Config
ipv6 option icmpv6-rate-limit icmpv6-type echo-reply rate <1-10000> scale	Sets the rate-limit at echo-reply packet.	Config

(second minute hour day) (burst <1-10000>)		
ipv6 option icmpv6-rate-limit icmpv6-type echo-request rate <1-10000> scale (second minute hour day) (burst <1-10000>)	Sets the rate-limit at echo-request packet.	Config
ipv6 option icmpv6-rate-limit icmpv6-type mld-query rate <1-10000> scale (second minute hour day) (burst <1-10000>)	Sets the rate-limit at mld-query packet.	Config
ipv6 option icmpv6-rate-limit icmpv6-type mld-report rate <1-10000> scale (second minute hour day) (burst <1-10000>)	Sets the rate-limit at mld-report packet.	Config
ipv6 option icmpv6-rate-limit icmpv6-type mld-done rate <1-10000> scale (second minute hour day) (burst <1-10000>)	Sets the rate-limit at mld-done packet.	Config
ipv6 option icmpv6-rate-limit icmpv6-type router-solicitation rate <1-10000> scale (second minute hour day) (burst <1-10000>)	Sets the rate-limit at router-solicitation packet.	Config
ipv6 option icmpv6-rate-limit icmpv6-type router-advertisement rate <1-10000> scale (second minute hour day) (burst <1-10000>)	Sets the rate-limit at router-advertisement packet.	Config
ipv6 option icmpv6-rate-limit icmpv6-type neighbor-solicitation rate <1-10000> scale (second minute hour day) (burst <1-10000>)	Sets the rate-limit at neighbor-solicitation packet.	Config
ipv6 option icmpv6-rate-limit icmpv6-type neighbor-advertisement rate <1-10000> scale (second minute hour day) (burst <1-10000>)	Sets the rate-limit at neighbor-solicitation packet.	Config
ipv6 option icmpv6-rate-limit icmpv6-type redirect rate <1-10000> scale (second minute hour day) (burst <1-10000>)	Sets the rate-limit at Redirect packet.	Config

<1-10000>)		
ipv6 option icmpv6-rate-limit icmpv6-type mld-reportv2 rate <1-10000> scale (second minute hour day) (burst <1-10000>)	Sets the rate-limit at mld-reportv2 packet.	Config
ipv6 option icmpv6-rate-limit icmpv6-type ha-addr-request rate <1-10000> scale (second minute hour day) (burst <1-10000>)	Sets the rate-limit at ha-addr-request packet.	Config
ipv6 option icmpv6-rate-limit icmpv6-type ha-addr-reply rate <1-10000> scale (second minute hour day) (burst <1-10000>)	Sets the rate-limit at ha-addr-reply packet.	Config
ipv6 option icmpv6-rate-limit icmpv6-type ma-prefix- solicitation rate <1-10000> scale (second minute hour day) (burst <1-10000>)	Sets the rate-limit at ma-prefix-solicitation packet.	Config
ipv6 option icmpv6-rate-limit icmpv6-type ma-prefix- advertisement rate <1-10000> scale (second minute hour day) (burst <1-10000>)	Sets the rate-limit at ma-prefix-advertisement packet.	Config
ipv6 option icmpv6-rate-limit icmpv6-type certification-path- solicitation rate <1-10000> scale (second minute hour day) (burst <1-10000>)	Sets the rate-limit at certification-path-solicitation packet.	Config
ipv6 option icmpv6-rate-limit icmpv6-type certification-path- advertisement rate <1-10000> scale (second minute hour day) (burst <1-10000>)	Sets the rate-limit at certification-path- advertisement packet.	Config
no ipv6 option icmpv6-rate-limit icmpv6-type	Disables the ICMPv6 rate-limit function.	Config

Chapter 16. *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 the 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 allows correlating 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 MAC address of host A within the ARP table in host B.

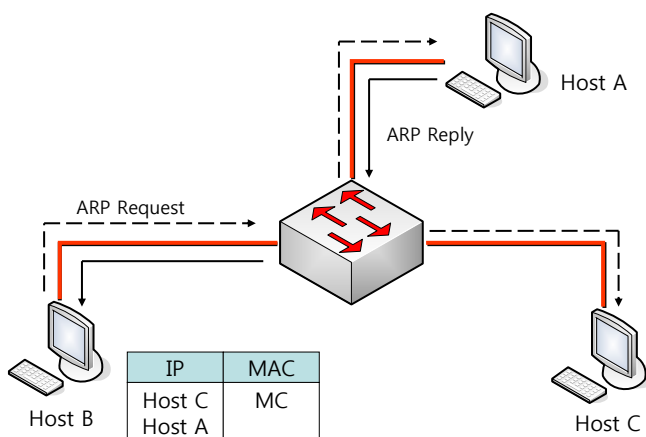


Figure 42. Understanding ARP

To find out the MAC address for host A's IP address, host B sends out broadcast message (ARP request) to all the hosts in the broadcast domain. Then all the hosts in the broadcast domain shall receive the ARP request which was sent by host B and host A will reply to this request 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. It intercepts the traffic which is intended for other networks. The following figures show examples of ARP cache poisoning.

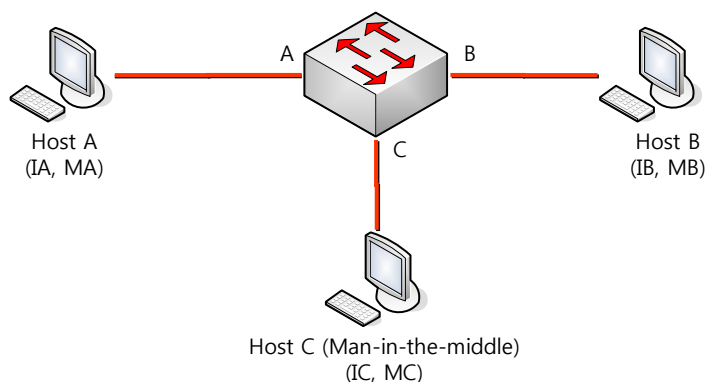


Figure 43. Understanding ARP Spoofing Attacks

Hosts 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. 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 this symptom is called as '*man-in-the middle attack*'.

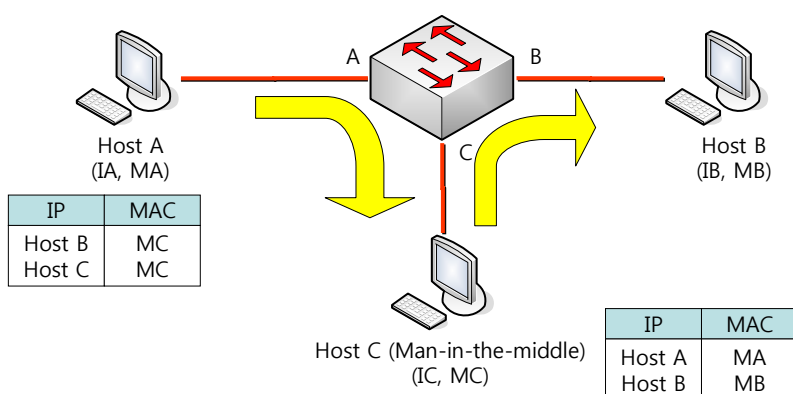


Figure 44. Understanding ARP Spoofing Attacks

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 the network from the man-in-the-middle attack.

DAI makes sure the ARP table be changed only by valid ARP request and response. The switch that is enabled for DAI function behaves as the following:

- Check out and inspect all ARP packets that come through the untrusted ports.
- Check out the received packets whether it has the valid IP-to-MAC address binding before updating its own ARP cache.
- Drop the invalid ARP packets.

When DAI checks out the validity of ARP packet, it utilizes the reliable data, which is an IP-to-MAC address binding stored 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 the following, 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 the case of the 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 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. 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 so that unicast ARP packets to be forwarded through forwarding engine can be inspected. To enable the unicast ARP packets to be inspected, refer to the section 19.4.1.

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.

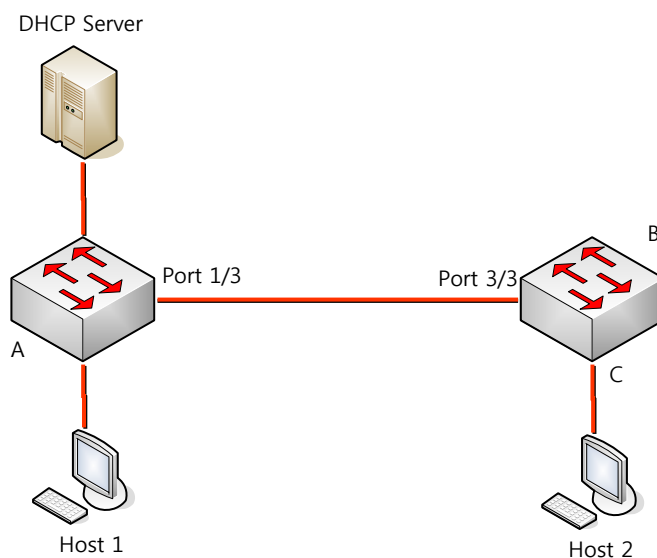


Figure 45. Interface Trust States and Network Security

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. 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

U9016B support the DAI features that inspect all ARP packets.

Rate Limiting of ARP Packets

The DAI-enabled switch will control the number of ARP packets that come into the switch CPU. As a default value, with respect to untrusted interface, 15 ARP packets per second (15 pps) are allowed meanwhile there is no limitation on the rate for trusted interface. You can configure the setting by use of the command `ip arp inspection limit`.

If the rate of ARP packets at a specified port would be over the predefined value, the switch will discard all the received ARP packets at the port. This behavior shall be maintained until user would change the configuration. By use of the command `ip arp inspection limit auto-recovery`, you can make the port get back to available status after a certain amount of time.

**Note**

The rate limit function toward ARP packets are performed at CPU in software manner, you cannot count on it for Denial-of-Service (DoS) attack.

Relative Priority of ARP ACLs and DHCP Snooping Entries

When DAI checks out the IP-to-MAC address mapping, it used DHCP snooping binding database.

ARP ACLs are used for inspection before DHCP snooping binding database. The switch will use ACL only when it is configured by `ip arp inspection filter` command. The switch will inspect ARP packets with ARP ACLs. If the ARP packet is consistent with the deny condition of ARP ACLs, the packet will be discarded even when there is valid binding that has been made by valid DHCP snooping.

Logging of Dropped Packets

The switch will keep the information about the discarded packets at log buffer and generate system message according to the ratio that has been set in advance. Once the message is generated, the corresponding information at the log buffer will be deleted. In each log there are the flow information including received VLAN id, port number, source and destination IP address, source and destination MAC address.

By use of global configuration command `ip arp inspection log-buffer` you can adjust the size of buffer and number of log per unit time so as to control the total volume of created messages. And with the global configuration command `ip arp inspection VLAN logging` you can specify the type of packets to log.

Default DAI Configuration

The following table shows the default DAI configuration.

Table 222 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 the case of trusted interfaces, there is no limitation on rate. Burst interval is 1 second. The rate limit for interfaces has a 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 packets which are denied or dropped will be logged.

DAI Configuration Guidelines and Restrictions

When DAI is configured, take care of the following points:

- DAI takes care of the ARP table only in the switch. As a better method to protect whole network, the trap function which will have ARP packet to be processed in CPU.
- DAI is intended to be used as an ingress security tool. You ought not to use it at an egress port.
- DAI is not effective for the hosts that are connected to the DAI-disabled switch. As the man-in-the-middle attack is confined to a single Layer 2 broadcast domain, you ought to separate a domain which adopts DAI from other domains which don't use DAI. This will make sure that the ARP table of the switch that are in DAI activated domain.
- DAI uses the DHCP snooping binding database in order to check the IP-to-MAC address binding of the coming ARP request and ARP response packets. To allow the ARP packets which will have dynamically assigned IP address, you ought to activate DHCP snooping.
- If DHCP snooping is inactive or DHCP is not in use, then you can utilize ARP ACL to permit or deny packets.
- Configure 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 packets that come through the VLAN as following:

- Broadcasted ARP packet
- ARP request packets that ask for MAC address of switch
- 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 the valid packets and updates the ARP table.

To enable DAI on a VLAN, execute the following commands.

Table 223 Enabling DAI on a VLAN

Command	Purpose
Switch# configure terminal	Enter Global configuration mode
Switch(config)# ip arp inspection VLAN VLAN-id	Enables DAI on a VLAN
Switch(config)# no ip arp inspection VLAN VLAN-id	Enables DAI on a VLAN
Switch# show ip arp inspection	Checks the setting



Note

When you enable DAI on a VLAN, all the ARP packets that flow through the VLAN will be inspected. In other words, the ARP cache of the switch and network are to be protected.

The following example shows how to enable DAI on VLAN 200:

```
Switch# configure terminal
Switch(config)# ip arp inspection VLAN 200
```

The following example shows how to retrieve current settings:

Switch# **show ip arp inspection**

DHCP Snoop Bootstrap : Disabled

Source MAC Validation : Disabled

Destination MAC Validation : Disabled

IP Address Validation : Disabled

ARP Field Validation : Disabled

VLAN	Config	Operation	ACL Match	Static ACL	ACL Log	DHCP Log
200	Enabled	Active+		No	Deny	Deny

200 Enabled Active+ No Deny Deny

If the system uses DAI about unicast ARP packet, you must set a trap to send ARP packet to CPU with using class-map and policy-map.

The following example shows how to set received ARP packet on VLAN 200 to CPU..

Switch(config)#class-map arp_trap_class

Switch(config-cmap)#match ethertype 0806

Switch(config-cmap)#end

Switch#show class-map

CLASS-MAP-NAME: arp_trap_class (match-all)

Match Ethertype: 0806

Switch#config terminal

Switch(config)#policy-map arp_trap_map

Switch(config-pmap)#class arp_trap_class

Switch(config-pmap-c)#trap-cpu

Switch(config-pmap-c)#exit

Switch(config-pmap)#exit

Switch(config)#int vlan200

Switch(config-if-Vlan200)#service-policy input arp_trap_map

Switch#show policy-map

POLICY-MAP-NAME: arp_trap_map

State: attached

CLASS-MAP-NAME: arp_trap _class (match-all)

Trap-cpu

Switch#show service-policy

Interface Vlan200 : input dhcp_user_map

Configuring the DAI Interface Trust State

Switch will not inspect the ARP packets that come from 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.

To configure the trust status of an interface, use the following commands:

Table 224 IP OPTION command

Command	Purpose
Switch# configure terminal	To enter global configuration mode
Switch(config)# interface ifname	To specify the interfaces that are connected to other switched and also get in the mode of configuring interface.
Switch(config-if-Giga1/1)# ip arp inspection	To configure the interface to be trusted (default:

trust Switch(config-if-Giga1/1)# no ip arp inspection trust	untrusted)
Switch(config-if-Giga1/1)# end	To get back to Enable mode
Switch# show ip arp inspection interfaces	To check the setting

The following example shows how to set Gigabit port 1/1 for trust.

```
Switch# configure terminal
Switch(config)# interface gi1/1
Switch(config-if-Giga1/1)# ip arp inspection trust
Switch(config-if-Giga1/1)# end
Switch# show ip arp inspection interfaces
```

Interface	Trust State	Rate (pps)	Burst Interval	Auto Recovery
Giga1/1	Trusted	None	1	Disabled

Applying ARP ACLs for DAI Filtering

To utilize ARP ACL feature, use the following commands.

Table 225 Applying ARP ACLs for DAI Filtering

Command	Purpose
Switch# configure terminal	Enters the global configuration mode
Switch(config)# ip arp inspection filter <i>arp_acl_name</i> VLAN <i>VLAN-id</i> [static]	Enters apply ARP ACL to a VLAN
Switch(config)# end	Return the Enable mode.
Switch# show ip arp inspection	Shows the running information.

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	Source MAC Validation	Destination MAC Validation	IP Address Validation	ARP Field Validation	VLAN	Config	Operation	ACL Match	Static ACL	ACL Log	DHCP Log
Disabled	Disabled	Disabled	Disabled	Disabled	200	Enabled	Active	example_arp_acl	No	Deny	Deny

Configuring ARP Packet Rate Limiting

Once DAI is enabled then all ARP packets are to be inspected, which will take a lot of CPU capability. Then consequently the switch will be vulnerable to the DoS attack which mainly bombarded ARP packets. Thus by putting a certain amount of limitation on the CPU it can control the amount of ARP packets to be processed rate and lessen the burden of CPU.



Note

The ARP rate limit that is provided by DAI is a software feature, so it cannot control the usage rate of CPU in direct measure. However by reducing the ARP packets which are to be handled by DAI, the CPU usage rate by DAI can be lowered.

To set the rate limit upon ARP packets for a port, do the following steps:

Table 226 Configuring ARP Packet Rate Limiting

Command	Purpose
Switch# configure terminal	Enters global configuration mode
Switch(config)# interface ifname	Specifies the interface that is connected to other switches and to enter interface configuration mode
Switch(config-if-Giga1/1)# ip arp inspection limit {rate pps [burst interval seconds] none}	Sets ARP packet rate limit (optional)
Switch(config-if-Giga1/1)# no ip arp inspection limit	To go back to default configuration
Switch(config-if-Giga1/1)# ip arp inspection limit enable	To enable the ARP rate limit of an interface
Switch(config-if-Giga1/1)# no ip arp inspection limit enable	To disable the ARP rate limit of an interface
Switch(config)# end	To go back to Enable mode
Switch# show ip arp inspection interfaces	To check the setting

When you set the ARP packet rate limit, pay attention to the following items.

- 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.
- 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 (optional).
- 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 gi1/1.

```
Switch# configure terminal
Switch(config)# interface gi1/1
Switch(config-if-Giga1/1)# ip arp inspection limit rate 20 burst interval 2
Switch(config-if-Giga1/1)# ip arp inspection limit enable
Switch(config-if-Giga1/1)# end
Switch# show ip arp inspection interfaces
```

Interface	Trust State	Rate (pps)	Burst Interval	Auto Recovery
Giga1/1	Untrusted	20	2	Disabled

Enabling DAI Error-Disabled Recovery

Use the following steps in order to restore the restricted port, which has been restricted due to the rate limit for ARP packets, to normal.

Table 227 Enabling DAI Error-Disabled Recovery

Command	Purpose
Switch# configure terminal	Enter global configuration mode
Switch(config)# interface <i>ifname</i>	Specifies the interface that is connected to other switches and to enter interface configuration mode
Switch(config-if-Giga1/1)# ip arp inspection limit auto-recovery <i>seconds</i>	Enables the automatic recovery function (optional)
Switch(config)# no ip arp inspection limit auto-recovery	To disable the automatic recovery function
Switch(config)# end	Return the enable mode
Switch# show ip arp inspection interfaces	Checks the settings

The following example shows the setting of recovering after 10 seconds automatically when ARP packet receiving on interface of gi 1/1 is disconnected by ARP rate limit.

```
Switch# configure terminal
Switch(config)# interface gi1/1
Switch(config-if-Giga1/1)# ip arp inspection limit auto-recovery 10
Switch(config-if-Giga1/1)# ip arp inspection limit enable
Switch(config-if-Giga1/1)# end
Switch# show ip arp inspection interfaces
```

Interface	Trust State	Rate (pps)	Burst Interval	Auto Recovery
gi1/1	Untrusted	20	2	10
gi1/2	Untrusted	15	1	Disabled

Enabling Additional Validation

DAI can verify the validity of ARP packet's destination MAC address, sender and target IP address, source MAC address.

Use the following steps for validity check for IP address or MAC address.

Table 228 Enabling Additional Validation

Command	Purpose
Switch# configure terminal	Enters global configuration mode
Switch(config)# ip arp inspection validate { dst-mac ip src-mac }	Enables additional validation test (optional) (default: none)
Switch(config)# no ip arp inspection validate { dst-mac ip src-mac }	Disables additional validation test
Switch(config)# end	Goes back to enable mode
Switch# show ip arp inspection	Checks the setting

To enable the validation test, pay attention to the following items.

- At least one keyword among options should 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.
- Additional validation tests according to command arguments are as below :

dst-mac – With respect to the ARP response packet, it makes comparison between the destination MAC address in Ethernet header and the target MAC address in ARP body.

ip – It checks out the invalid IP address in ARP body. Thus addresses like 0.0.0.0 or 255.255.255.255 or multicast IP address will be discarded. It also verifies the sender IP address of ARP request and the sender/target IP address of ARP response.

src-mac – With respect to all ARP packets, it makes comparison between the source MAC address in Ethernet header and the sender MAC address in ARP body.

The following example shows how to enable the additive validity inspection as to the command argument 'src-mac':

```
Switch# configure terminal
Switch(config)# ip arp inspection validate src-mac
Switch(config)# end
Switch# show ip arp inspection
DHCP Snoop Bootstrap      : Disabled
Source MAC Validation      : Enabled
Destination MAC Validation : Disabled
IP Address Validation      : Disabled
ARP Field Validation       : Disabled
VLAN  Config  Operation  ACL Match      Static ACL  ACL Log  DHCP Log
-----
200  Enabled  Active           No           Deny      Deny
```

The following example shows how to enable the additive validity inspection as to the command argument dst-mac.

```
Switch# configure terminal
Switch(config)# ip arp inspection validate dst-mac
Switch(config)# end
Switch# show ip arp inspection
DHCP Snoop Bootstrap      : Disabled
Source MAC Validation      : Disabled
Destination MAC Validation : Enabled
IP Address Validation      : Disabled
ARP Field Validation       : Disabled
VLAN  Config  Operation  ACL Match      Static ACL  ACL Log  DHCP Log
-----
200  Enabled  Active           No           Deny      Deny
```

The following example shows how to enable additional validation test as to command argument ip:

```
Switch# configure terminal
Switch(config)# ip arp inspection validate ip
Switch(config)# end
Switch# show ip arp inspection
DHCP Snoop Bootstrap      : Disabled
Source MAC Validation     : Disabled
Destination MAC Validation : Disabled
IP Address Validation     : Enabled
ARP Field Validation      : Disabled
VLAN  Config  Operation  ACL Match      Static ACL  ACL Log  DHCP Log
----  -
200   Enabled  Active           No           Deny       Deny
```

The following example shows to enable the additional validation test as to the command arguments src-mac and dst-mac:

```
Switch# configure terminal
Switch(config)# ip arp inspection validate dst-mac src-mac
Switch(config)# end
Switch# show ip arp inspection
DHCP Snoop Bootstrap      : Disabled
Source MAC Validation     : Enabled
Destination MAC Validation : Enabled
IP Address Validation     : Disabled
ARP Field Validation      : Disabled
VLAN  Config  Operation  ACL Match      Static ACL  ACL Log  DHCP Log
----  -
200   Enabled  Active           No           Deny       Deny
```


Configuring DAI Logging

This section explains on DAI logging.

- DAI Logging Overview
- Configuring the DAI Logging Buffer Size
- Configuring the DAI Logging System Messages
- Configuring DAI Log Filtering

DAI Logging Overview

Switch saves information about the discarded packets into log buffer and generates a system message according to the pre-configured generation rate. Once the message is generated, relevant information in the log buffer shall be deleted. Each log has the flow information: such as a received VLAN id, port number, source and destination IP address, source and destination MAC address.

A log buffer entry can hold information of more than one packet. For example if a VLAN receives packets with ARP parameters through the same interface, DAI will create a log buffer entry for these packets and generate one system message.

Configuring the DAI Logging Buffer Size

Use the following commands in order to adjust the size of DAI log buffer:

Table 229 Configuring the DAI Logging Buffer Size

Command	Purpose
Switch# configure terminal	Enters global configuration mode
Switch(config)# ip arp inspection log-buffer entries <i>number</i>	Sets the size of DAI log buffer (range: 0~ 1024)
Switch(config)# no ip arp inspection log-buffer entries	Returns to the default, 32
Switch(config)# end	Returns to enable mode
Switch# show ip arp inspection log	Checks the setting

The following example shows how to set the size of log buffer of DAI 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 DAL generates, use the following commands:

Table 230 Configuring the DAI Logging System Messages

Command	Purpose
Switch# configure terminal	To enter global configuration mode
Switch(config)# ip arp inspection log-buffer logs <i>number_of_messages</i> <i>interval</i> <i>length_in_seconds</i>	To configure the DAI log buffer
Switch(config)# no ip arp inspection log-buffer logs	To return to default
Switch(config)# end	To return to enable mode
Switch# show ip arp inspection log	To check the setting

You must pay attention to the following when you configure the logging system message of DAI:

- As to 'logs *number_of_messages*' (default: 5): the range is from 0 to 1024. If it is set to be 0, then log message will not be generated.
- As to 'interval *length_in_seconds*' (default: 1): the range is from 0 to 86400 (one day). If it is set to be 0, then a log message will be generated immediately. That means that the log buffer is constantly empty.
- 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 the system to generate 12 DAI log messages 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 an inspection of ARP packets you can selectively generate the system message according to the result.

Use the following commands in order to configure the log filtering of DAI:

Table 231 Configuring the DAI Log Filtering

Command	Purpose
Switch# configure terminal	To enter global configuration mode
Switch(config)# ip arp inspection VLAN <i>VLAN-id</i> { acl-match { matchlog none } dhcp-bindings { all none permit }}	To apply log filtering to each VLAN
Switch(config)# end	To return to enable mode
Switch# show running-config	To check the setting

You must pay attention to the following items setting the logging system message of DAI.

- All 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 the system not to generate log message for the packets that are consistent with ACL:

```
Switch# configure terminal
Switch(config)# ip arp inspection VLAN 200 logging acl-match none
Switch(config)# end
Switch# show ip arp inspection
DHCP Snoop Bootstrap      : Disabled
Source MAC Validation     : Disabled
Destination MAC Validation : Disabled
IP Address Validation      : Disabled
ARP Field Validation      : Disabled
VLAN  Config  Operation  ACL Match  Static ACL  ACL Log  DHCP Log
-----
200  Enabled  Active      No          None       Deny
```

Displaying DAI Information

To retrieve information, use the following commands:

Table 232 Displaying DAI Information

Command	Description
<code>show arp access-list</code>	Shows the information of ARP ACL.
<code>show ip arp inspection interfaces</code>	Shows the trust status of the interface.
<code>show ip arp inspection VLAN [VLAN-id]</code>	Shows the DAI configuration and its behavior of a VLAN.
<code>show ip arp inspection arp-rate</code>	Shows the rate of ARP packet reception in the interface.

To retrieve or initialize DAI statistics, use the following commands.

Table 233 Initialize DAI Statistics

Command	Description
<code>clear ip arp inspection statistics</code>	To initialize DAI statistics
<code>show ip arp inspection statistics [VLAN VLAN-id]</code>	To display the DAI statistics of ARP packets

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

Table 234 Initialize the DAI logging information

Command	Description
<code>clear ip arp inspection log</code>	To initialize DAI log buffer
<code>show ip arp inspection log</code>	To display the configuration and contents of DAI log buffer

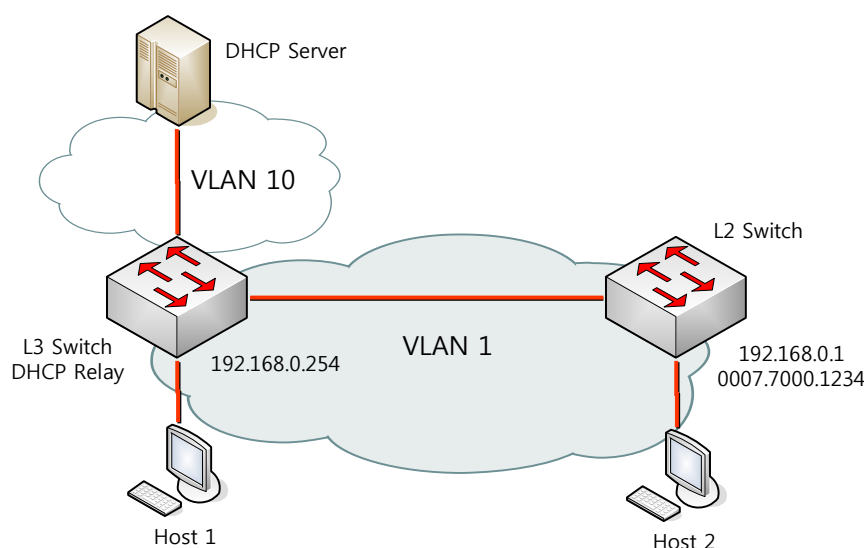
DAI Configuration Samples

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 switches 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 235 DAI Configuration

Step	Description
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	<p>To permit ARP packet of switch using static ip, set ARP ACL.</p> 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 <p>To see if the configuration has been set correctly.</p> Switch# show ip arp inspection VLAN 1
Step 4	<p>Enables DAI to VLAN1 connected with host.</p> Switch# configure terminal Switch(config)# ip arp inspection VLAN 1 Switch(config)# end <p>To see if the configuration has been set correctly.</p> 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
!

```

Chapter 17. QoS and ACL

This chapter describes the QoS configuration and the ACL of system.

QOS

Global Configuration

Use the following commands to enable QOS global.

Table 236 QOS Global Configuration Command

Command	Description	Mode
mls qos	Enables QOS global configuration	Config
no mls qos	Disables QOS global configuration	Config
show mls qos	Searches the status of QOS global configuration	Exec

All QOS-related settings of a U9016B work only under global configuration. Most QOS-related commands are not possible to set if Mls qos is not enabled.

TX Scheduling Configuration

U9016B provides SPQ (Strict Priority Queue) and WRR (Weighted Round Robin) for scheduling. These two ways can be used together.

The WRR provided by U9016B is SDWRR (Shaped Deficit Weighted Round Robin) method. DWRR operates as WRR, but has additional feature of managing quota. It controls the amount of incoming data that come regularly and those are burst in. Another feature, shaping, is added to SDWRR in order to reduce latency of data flow.

When weights are given to 2 queues at the ratio of 5:3, WRR (or DWRR) allocates queues in order of 1,1,1,1,1,0,0,0,1,1,1,1,1,0,0,0. On the other hand, SDWRR allocates queues in order of 1,0,1,0,1,0,1,1,1,0,1,0,1,0,1,1 and controls the amount of packets and reduces the latency of traffic.

Each port has 8 queues: Queue 7 has the highest priority, and Queue 0 has the lowest priority.

The following table shows an example about scheduling per queue.

Table 237 TX Scheduling Configuration

Queue	Description
Queue 7	SPQ
Queue 6	SPQ
Queue 5	WRR group 1 (50)
Queue 4	WRR group 1 (30)
Queue 3	WRR group 1 (20)
Queue 2	WRR group 2 (60)
Queue 1	WRR group 2 (40)
Queue 0	SPQ

- Q7 and Q6 are set for SPQ. Q7 will be treated as the highest priority because it is the first in order and is SPQ at the same time. Then Q6 will be treated the next.
- Q5, 4, and 3 are set for WRR group 1, and are allocated in the ratio of 50:30:20 of weight. WRR group 1 is lower in rank than SPQ, but is higher than WRR group 2. These two have different ranks as SPQ.
- Q2 and 1 are set for WRR group 2, and are allocated in the ratio of 60:40 of weight. WRR group 2 will be treated after all queues mentioned above are treated.

- Q0 is declared as SPQ, but has the lowest priority. Q0 works only after Q7 to Q1 are treated.



Notice

Do not mix 2 WRR groups (e.g. set WRR1 for Q5 and Q2, and WRR2 for Q4 and Q1): or do not use SPQ in between of WRR groups or to the lower Q. It may work different from the configuration in the scheduling.

In the scheduling setting, it first generates a mapping table then applies to a port. It can apply seven maps to each module.

In fact, it can apply eight maps in total, but queue 0 is used as the default SPQ and it cannot be changed. Therefore you can manage only seven of them.

Table 238 Tx-Scheduling Map Configuration Command

Command	Description	Mode
mls qos map tx-scheduling NAME queueing-method <0-7> (strict wrr1 wrr2)	Sets the queueing-method of nth queue of the mapping table. When no mapping table, it generates a new one.	Config
mls qos map tx-scheduling NAME queueing-method <0-7> (wrr1 wrr2) <1-100>	When setting wrr1 or wrr2, you can set WRR weights simultaneously. (Default: 1)	Config
mls qos map tx-scheduling NAME wrr-weight <0-7> <1-100>	Sets the weight for WRR of the selected queue.	Config
no mls qos map tx-scheduling NAME queueing-method <0-7>	Disables the queueing-method of the queue. Then it changes into the default, strict.	Config
no mls qos map tx-scheduling NAME wrr-weight <0-7>	Disables the weight of the queue that is set for WRR. (Default :1)	Config
no mls qos map tx-scheduling NAME	Deletes mapping table with the relevant name.	Config
show mls qos map tx-scheduling	Displays configuration of Tx-scheduling.	Exec

Set a mapping table of tx-scheduling to a designated port using the following settings:

Table 239 Tx-scheduling Configuration Command

Command	Description	Mode
mls qos tx-scheduling NAME	Sets a mapping table to a relevant port interface with the correct name	interface
no mls qos tx-scheduling NAME	Disables the mapping table with the name from the port interface.	interface

Port Trust Mode

To carry out QOS of traffic leaded into a port, it is designed to check out COS of a packet or the value of DSCP first, and then organize the priority based on the figures found. However you need to determine whether the values of COS and DSCP can be trusted.

With no configuration, it does not refer to COS or DSCP, and operates by the default COS value. The default COS is used for packets with no COS or DSCP (e.g. untagged packet) to define the basic operation.

You can set “trust mode” to COS and DSCP: you can enable both, or neither.

- When a packet has a DSCP and is in Trust DSCP (or BOTH) mode, then use this.
- When a packet has a COS and is in trust COS (or BOTH) mode, then use this.
- When a packet has no COS and is in trust COS (or BOTH), then use default COS.

- In other cases, use default COS.

When a packet has a DSCP and is in trust DSCP mode, it operates QOS based on DSCP. Otherwise, it operates QOS based on COS.

Table 240 Port Trust Configuration Command

Command	Description	Mode
mls qos trust (cos dscp both)	Sets a port interface for the trust mode.	interface
no mls qos trust	Disables the interface set for trust mode. Then it will be set as none.	interface
mls qos cos <0-7>	Sets the default COS value of a port.	interface
no mls qos cos	Disables the default COS value of a port.	interface

DSCP Conversion Map Configuration

When a packet is carried out by DSCP as a standard in Trust DSCP mode, the packet will be operated as follows.

- Queueing operation by DSCP value
- COS marking (or remarking) operation by DSCP value
- DSCP remarking operation by DSCP value

DSCP to queue Configuration

In queueing operation a packet is carried out depending on DSCP. The process works all the time without a setting of enable/disable. For this operation DSCP-queue map is maintained with the global setting.

Table 241 dscp-queue map Configuration Command

Command	Description	Mode
mls qos map dscp-queue <0-63> ... <0-63> to <0-7>	Sets Dscp-queue map	config
no mls qos map dscp-queue	Initializes Dscp-queue map	config
show mls qos map dscp-queue	Shows the current dscp-queue map configuration	Exec

Switch#show mls qos map dscp-queue

DSCP-TO-QUEUE MAP

```

d1:  d2  0   1   2   3   4   5   6   7   8   9
-----
0:    0   0   0   0   0   0   0   0   1   1
1:    1   1   1   1   1   1   2   2   2   2
2:    2   2   2   2   3   3   3   3   3   3
3:    3   3   4   4   4   4   4   4   4   4
4:    5   5   5   5   5   5   5   5   6   6
5:    6   6   6   6   6   6   7   7   7   7
6:    7   7   7   7

```

DSCP to COS Configuration

A packet can be carried out COS marking (or remarking) operation depending on DSCP values. This can be set as "enable" or "disable", and the default is "disable". For this operation DSCP to COS map is maintained with the global setting.

Switch#show mls qos map dscp-cos

DSCP-TO-COS MAP

d1 :	d2	0	1	2	3	4	5	6	7	8	9
0 :		0	0	0	0	0	0	0	0	1	1
1 :		1	1	1	1	1	1	2	2	2	2
2 :		2	2	2	2	3	3	3	3	3	3
3 :		3	3	4	4	4	4	4	4	4	4
4 :		5	5	5	5	5	5	5	5	6	6
5 :		6	6	6	6	6	6	7	7	7	7
6 :		7	7	7	7						

DSCP to DSCP Configuration

A packet can be carried out DSCP remarking operation depending on DSCP values. This is called "mutation" because it changes DSCP of itself. Each port can be set as enable/disable, and the default is "disable". For this operation DSCP to DSCP map is maintained the global setting. The default is 1:1. Change the map to apply to the port interface before use.

Table 242 Cos-Dscp map Configuration Command

Command	Description	Mode
mls qos map Cos-Dscp <0-7> <0-63>	Configures Cos-dscp map.	config
no mls qos map Cos-Dscp	Initializes Cos-Dscp map.	config
mls qos Cos-Dscp	Sets Cos-Dscp marking on the port interface.	interface
no mls qos Cos-Dscp	Disables Cos-Dscp marking on the port interface.	interface
show mls qos map Cos-Dscp	Displays current settings of Cos-Dscp map.	Exec

Switch#show mls qos map dscp-mutation

DSCP MUTATION MAP

```

d1 :  d2  0   1   2   3   4   5   6   7   8   9
-----
0 :    0   1   2   3   4   5   6   7   8   9
1 :   10  11  12  13  14  15  16  17  18  19
2 :   20  21  22  23  24  25  26  27  28  29
3 :   30  31  32  33  34  35  36  37  38  39
4 :   40  41  42  43  44  45  46  47  48  49
5 :   50  51  52  53  54  55  56  57  58  59
6 :   60  61  62  63

```

COS Conversion Map Configuration

When a packet is carried out by COS as a standard in Trust COS mode, the packet will be operated as follows.

- Queueing operation by COS value
- DSCP marking (or remarking) operation depending on COS value
- COS remarking operation depending on COS value

COS to queue Configuration

A packet is carried out queueing operation depending on COS value. It works all the time without a setting of enable/disable. For this operation COS-queue map is maintained the global setting.

Table 243 cos-queue map Configuration Command

Command	Description	Mode
mls qos map cos-queue <0-7> <0-7>	Sets Cos-queue map	config
no mls qos map cos-queue	Initializes Cos-queue map	config
show mls qos map cos-queue	Displays the current settings of cos-queue	Exec

	map	
--	-----	--

COS to DSCP Configuration

A packet can be carried out DSCP marking (or remarking) operation depending on COS value. Each port interface can be set as either “enable” or “disable”, and the default is “disable”. This operation COS to DSCP map is maintained the global setting.

Table 244 Cos-Dscp map Configuration Command

Command	Description	Mode
mls qos map Cos-Dscp <0-7> <0-63>	Configures Cos-dscp map.	config
no mls qos map Cos-Dscp	Initializes Cos-Dscp map.	config
mls qos Cos-Dscp	Sets Cos-Dscp marking on the port interface.	interface
no mls qos Cos-Dscp	Disables Cos-Dscp marking on the port interface.	interface
show mls qos map Cos-Dscp	Displays current settings of Cos-Dscp map.	Exec

```
Switch# show mls qos map Cos-Dscp
COS-TO-DSCP MAP
COS :  0   1   2   3   4   5   6   7
-----
DSCP:  0   8  16  24  32  40  48  56
```

COS to COS Configuration

A packet can be carried out COS remarking operation depending on COS values. This is called “mutation” because it changes COS of itself. Each port can be set as enable/disable, and the default is “disable”. For this operation DSCP to DSCP map is maintained the global setting. The default is 1:1. Change the map to apply to the port interface before use.

Table 245 cos-mutation Map Configuration Command

Command	Description	Mode
mls qos map cos-mutation <0-7> <0-7>	Sets Cos-mutation map.	config
no mls qos map cos-mutation	Initializes Cos-mutation map.	config
mls qos cos-mutation	Sets cos remarking on the port interface.	interface
no mls qos cos-mutation	Disables cos remarking on the port interface.	interface
show mls qos map cos-mutation	Displays the current settings of cos-mutation map.	Exec

ACL Configuration

U9016B have various options in ACL configuration including a feature sorting packets into easily acceptable ones and not easily acceptable ones.

U9016B provides three ACLs: standard IP ACL, extended IP ACL, and MAC ACL.

Standard IP ACL classifies packets by source IP only. Ranges of <1-99> and <1300-1999> are assigned for Standard IP ACL, and it can be generated with names other than numbers.

Extended IP ACL sorts packets by source IP, destination IP, and protocol type. It can sort TCP and UDP packets by L4 src and dst port, ICMP packets by icmp-type, and IGMP packets by igmp-type. The ranges of <100-199> and <2000-2699> are assigned, and it can be generated with names other than numbers.

MAC ACL sorts packets by MAC address. The command "mac-access-list" is used. The range of <1100-1199> is assigned for MAC ACL.

Standard IP ACL

Standard IP ACL classifies packets by source IP. A figure or a series of access-list can be connected, each condition can take a permit or deny.

Standard IP ACL was originally designed to set 99 ACLs of <1-99>, and 700 expanded areas of <1300-1999> were added later as additional ACLs are needed. And it is possible to add almost unlimited numbers of ACLs using names by letters.

Table 246 Standard IP ACL Configuration Command

Command	Description	Mode
access-list <1-99> (permit deny) SRC_IP_ADDRESS	Enables standard IP ACL	config
no access-list <1-99> (permit deny) SRC_IP_ADDRESS	Disables standard IP ACL	config
no access-list <1-99>	Deletes all ACL with the relevant names (numbers)	config
access-list <1-99> remark LINE	Adds the description of the relevant ACL	config
access-list <1300-1999> (permit deny) SRC_IP_ADDRESS	Sets standard IP ACL of expanded range	config
no access-list <1300-1999> (permit deny) SRC_IP_ADDRESS	Disables standard IP ACL of expanded range	config
no access-list <1300-1999>	Deletes all ACL with the relevant numbers	config
access-list <1300-1999> remark LINE	Adds the description of the relevant ACL	config
access-list standard WORD (permit deny) SRC_IP_ADDRESS	Sets named standard IP ACL	config
no access-list standard WORD (permit deny) SRC_IP_ADDRESS	Disables named standard IP ACL	config
no access-list standard WORD	Deletes all ACLs with the relevant names	config
access-list WORD remark LINE	Adds the description of the relevant ACL	config
Show access-list	Searches ACL configuration	Exed

The command, **SRC_IP_ADDRESS** can be set as follows.

Table 247 SRC_IP_ADDRESS

Command	Description
---------	-------------

A.B.C.D A.B.C.D	IP range can be set in the form of wildcard. As opposed to the general IP configuration, marking value is 0
host A.B.C.D	Add a host prefix to indicated only one IP address.
A.B.C.D	It will be treated the same as host A.B.C.D when only one IP is provided.
any	Use any when assigning all IP addresses.



Notice

10.1.1.0/24 means the same as 255.255.255.0 when indicating an IP range in general. This implies an IP range of 10.1.1.0 ~ 10.1.1.255.

However ACL configuration of wildcard needs the opposite way: you should set 10.1.1.0.0.0.255 when assigning the IP range of 10.1.1.0 ~ 10.1.1.255.

Extended IP ACL

Extended IP ACL uses both src ip and des tip addresses while standard IP ACL uses only src ip address to sort packets. It is possible to sort packets using protocol type. You can sort TCP and UDP packets using L4 src and dst port, ICMP packets using icmp-type, and IGMP packets using igmp-type.

Extended IP ACL was originally designed to set 100 ACLs of <100-199>, and 700 expanded areas of <2000-2699> were added later as additional ACLs are needed. And it is possible to add almost unlimited numbers of ACLs using names by letters.

Table 248 Extended IP ACL Configuration Command

Command	Description	Mode
access-list <100-199> (permit deny) (<0-255> icmp igmp ip ospf pim tcp udp) SRC_IP_ADDRESS DST_IP_ADDRESS	Sets extended IP ACL.	config
access-list <100-199> (permit deny) icmp SRC_IP_ADDRESS DST_IP_ADDRESS ICMP-TYPE	Sets extended IP ACL of ICMP type.	config
access-list <100-199> (permit deny) igmp SRC_IP_ADDRESS DST_IP_ADDRESS IGMP-TYPE	Sets extended IP ACL of IGMP type.	config
access-list <100-199> (permit deny) (tcp udp) SRC_IP_ADDRESS DST_IP_ADDRESS eq <0-65536>	Sets extended IP ACL of TCP / UDP type.	config
no access-list <100-199> (permit deny) (<0-255> icmp igmp ip ospf pim tcp udp) SRC_IP_ADDRESS DST_IP_ADDRESS	Disables extended IP ACL.	config
no access-list <100-199>	Deletes all ACLs with the relevant name (number).	config
access-list <100-199> remark LINE	Adds the description of the relevant ACL.	config
access-list <2000-2699> (permit deny) (<0-255> icmp igmp ip ospf pim tcp udp) SRC_IP_ADDRESS DST_IP_ADDRESS	Sets extended IP ACL of expanded range.	config
access-list <2000-2699> (permit deny) icmp SRC_IP_ADDRESS DST_IP_ADDRESS ICMP-TYPE	Sets extended IP ACL of expanded range of ICMP type.	config
access-list <2000-2699> (permit deny) igmp SRC_IP_ADDRESS DST_IP_ADDRESS IGMP-TYPE	Sets extended IP ACL of expanded range of IQMP type.	config

access-list <2000-2699> (permit deny) (tcp udp) SRC_IP_ADDRESS DST_IP_ADDRESS eq <0-65536>	Sets extended IP ACL of expanded range of TCP / UDP type.	config
no access-list <2000-2699> (permit deny) (<0-255> icmp igmp ip ospf pim tcp udp) SRC_IP_ADDRESS DST_IP_ADDRESS	Disables extended IP ACL.	config
no access-list <2000-2699>	Deletes all ACLs with the relevant name.	config
access-list <2000-2699> remark LINE	Adds the description of the relevant ACL.	config
access-list extended WORD (permit deny) (<0-255> icmp igmp ip ospf pim tcp udp) SRC_IP_ADDRESS DST_IP_ADDRESS	Sets named extended IP ACL.	config
access-list extended WORD (permit deny) icmp SRC_IP_ADDRESS DST_IP_ADDRESS ICMP-TYPE	Sets extended IP ACL of ICMP type.	config
access-list extended WORD (permit deny) igmp SRC_IP_ADDRESS DST_IP_ADDRESS IGMP-TYPE	Sets extended IP ACL of IGMP type.	config
no access-list extended WORD (permit deny) (<0-255> icmp igmp ip ospf pim tcp udp) SRC_IP_ADDRESS DST_IP_ADDRESS	Disables named extended IP ACL.	config
no access-list extended WORD	Deletes all ACLs with the relevant name.	config
access-list WORD remark LINE	Adds the description of the relevant ACL.	config
Show access-list	Searches the configuration of ACL.	Exec

The command, SRC_IP_ADDRESS and DST_IP_ADDRESS can be set as follows.

Command	Description
A.B.C.D A.B.C.D	IP range can be set in the form of wildcard. As opposed to the general IP configuration,
host A.B.C.D	Add a host prefix to indicated only one IP address.
any	Use any when assigning all IP addresses.

IPv6 Standard ACL

The standard IP ACL distinguishes packets by using the source IP. One number of a name can be connected with several access-lists and permit or deny can be executed for each condition.

In addition, the name can be made by using alphabet characters.

Table 249 IPv6 Standard ACL

Command	Command	Mode
ipv6 access-list WORD (permit deny) SRC_IPv6_ADDRESS	Sets IPv6 ACL.	Config
No ipv6 access-list WORD (permit deny) SRC_IPv6_ADDRESS	Resets IPv6 ACL.	Config

SRC_IPv6_ADDRESS is described as follows.

X:X::X:X/M	Sets the IP band with the wildcard type. Unlike general IP setting, 0 is masked.
any	Used to specify all IP addresses.

IPv6 Extended ACL

Contrary to standard IP ACL, IPv6 extended ACL uses both the source IP and the destination IP. In addition, it can distinguish packets by using protocol type. If the packet type is TCP or UDP, it can distinguish packets by using L4 src and dst ports. For ICMP, it uses icmp-type. For IGMP, it uses igmp-type.

In addition, like the standard IP ACL, the name can be made by using alphabet characters.

Table 250 IPv6 Extended ACL

Command	Command	Mode
ipv6 access-list extended WORD (permit deny) (<0-255> icmp igmp ip ospf pim tcp udp) SRC_IP_ADDRESS DST_IP_ADDRESS	Sets the named extended IPv6 ACL.	config
ipv6 access-list extended WORD (permit deny) icmp SRC_IP_ADDRESS DST_IP_ADDRESS ICMP-TYPE	Sets the extended IPv6 ACL with ICMP type.	config
ipv6 access-list extended WORD (permit deny) igmp SRC_IP_ADDRESS DST_IP_ADDRESS IGMP-TYPE	Sets the extended IPv6 ACL with IGMP type.	config
No ipv6 access-list extended WORD (permit deny) (<0-255> icmp igmp ip ospf pim tcp udp) SRC_IP_ADDRESS DST_IP_ADDRESS	Resets the named extended IPv6 ACL.	config
no ipv6 access-list extended WORD	Deletes all ACLs with the corresponding name.	config
Show access-list	Shows the ACL configuration.	Exec



Notice

A.B.C.D is not supported in extended IP ACL to prevent confusion. Host A.B.C.D is used to appoint a single IP.



Notice

An address such as 10.1.1.0/24 has the same meaning as 10.1.1.0.255.255.255.0 when indicating the IP range of 10.1.1.0 ~ 10.1.1.255.

However ACL configuration of wildcard needs the opposite way: you should set 10.1.1.0.0.0.255 when assigning the IP range of 10.1.1.0 ~ 10.1.1.255.

MAC ACL

MAC ACL uses MAC address to sort packets. MAC ACL was originally designed <1100-1199> of ACL. Unlike IP ACL, MAC ACL uses mac-access-list.

Table 251 standard IP ACL Configuration Command

Command	Description	Mode
mac-access-list <1100-1199> (permit deny) SRC_MAC_ADDRESS DST_MAC_ADDRESS <1-8>	Enables MAC ACL	config
no mac-access-list <1100-1199> (permit deny) SRC_MAC_ADDRESS DST_MAC_ADDRESS <1-8>	Disables MAC ACL	config
no mac-access-list <1100-1199>	Deletes all ACLs with the relevant names	
Show mac-access-list	Retrieves the configuration of MAC ACL	Exec

src_ip_address and dst_ip_address can be set as follows. however src_mac and dst_mac cannot be any simultaneously.

Item	Description
H.H.H H.H.H	You can set MAC address bandwidth as wildcard.
any	Use any when assigning all MAC addresses.

Application of ACL to Interface

The ACL set as above can be applied to an interface as follows. The interfaces mentioned here means VLAN interfaces, and they are applicable to port interfaces set as router ports.

Table 252 Commands for the Application of ACL to Interface

Command	Description	Mode
ip access-group { <1-199> <1300>2699> WORD } { in out }	Sets acl to the relevant interface	Interface
no ip access-group { <1-199> <1300>2699> WORD } { in out }	Disables acl of the relevant interface	Interface



Notice

Router port means a port with no switchport.



Notice

Service-policy can set up to 16000 rules in the input direction, 4000 rules in the output direction summed with ACLs.



Notice

In the input direction, you can set service and ACL simultaneously. For the output direction, you can set only either one at a time.

Service-policy Configuration

For configurations of complicated QOS you can set various forms of rules and actions using class-map and policy-map.

Class-map sorts packets using one of the choices from ACL, ehertype, cos, VLAN, protocol, dscp, ip-precedence(TOS), I4 port, tcp flag, and mlps flag, etc.

Such traffic that is sorted as a class-map carries out the basic works as permit / drop, and also other works as queueing, cos, marking / remarking, dscp marking / remarking, rate-limit etc. PBR (Policy Based Routing) is available when nexthop is linked together. It enables other operations, which is not related to QOS, such as trap-cpu, mirrot, redirect, netflow, etc.

Class-map

A class-map is produced for the purpose of sorting packets. In other words, ACL is used in sorting packets, and other means can also be used, such as ehertype, cos, VLAN, protocol, dscp, ip-precedence (TOS), I4 port, tcp flag, mlps flag to sort packets.

ACL may use both ip acl and mac-acl together, or only one of the two. Each ACL can have up to 1000 items. In order to apply more than 1000 ACLs, you need to divide ACLs into several groups and generate class-map for each.

In addition, IPv4 ACL should be set in class-map and IPv6 ACL should be set in class-map ipv6..

Sorting options including ACL basically run AND operation. For example if both ACL and DSCP are enabled, only packets that satisfy the two conditions will be sorted.

Table 253 Class-map Configuration Command

Command	Description	Mode
class-map WORD	Generates a class-map that is classified according to AND operation and moves to the node.	Config
class-map match-all WORD	Generates a class-map that is classified according to AND operation and moves to the node.	Config
class-map match-any WORD	Generates a class-map that is classified according to OR operation and moves to the node.	Config
no class-map WORD	Deletes the Class-map.	Config
class-map ipv6 WORD	Creates a class-map for IPv6 classified as AND and then moves to the node.	Config
class-map ipv6 match-all WORD	Creates a class-map for IPv6 classified as AND and then moves to the node.	Config
class-map ipv6 match-any WORD	Creates a class-map for IPv6 classified as OR and then moves to the node.	Config
no class-map ipv6 WORD	Deletes a class-map for IPv6.	Config
match access-group NAME	Sets the classification criteria using ACL.	cmap
match cos <0-7>	Sets the classification criteria using COS.	cmap
match ehertype WORD	Sets the classification criteria using Ehertype.	cmap
match ip-dscp <0-63>	Sets the classification criteria using DSCP.	cmap
match ip-precedence <0-7>	Sets the classification criteria using IP-	cmap

	Precedence.	
match layer4 {source-port destination-port} <1-65536>	Sets the classification criteria using L4 port.	cmap
match mpls exp-bit topmost <0-7>	Sets the classification criteria using MPLS flag.	cmap
match tcp-control VALUE	Sets the classification criteria using TCP-control.	cmap
match VLAN <1-4095>	Sets the classification criteria using VLAN.	cmap



Notice

Ethertype is classified as a 4-digit hexadecimal. For example, you can enter 0806 for ARP type.



Notice

TCP-control is classified as a six-digit binary number. For example, you can see the fifth digit, SYN flag by declaring 00010.

Policy-map

Such traffic that is sorted as a class-map carries out the basic works as permit / drop, and also other works as queueing, cos, marking / remarking, dscp marking / remarking, rate-limit etc. PBR (Policy Based Routing) is available when nexthop is linked together. It enables other operations, which is not related to QOS, such as trap-cpu, mirrot, redirect, netflow, etc.

Each policy-map can assign up to 100 operations. Each Class-map can have up to 1000 entries of ACL, which means a policy-map should control 100,000 entries in theory. However it is not possible to control so many entries due to the restriction of H/W.

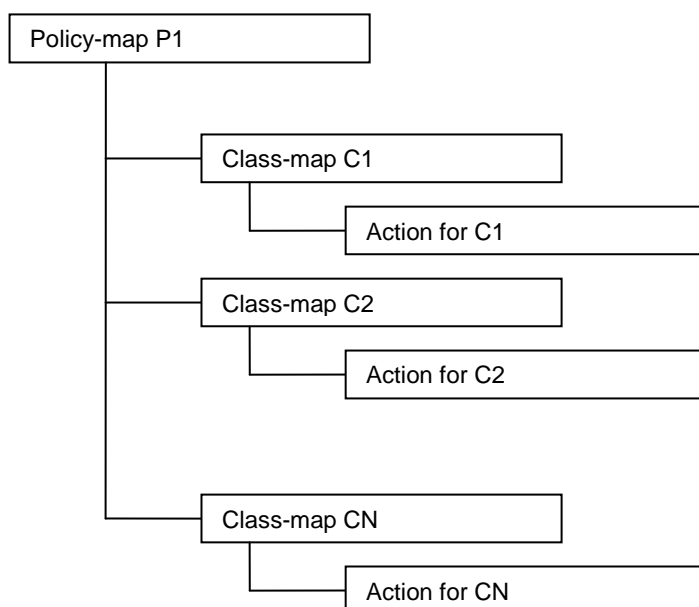


Figure 46. Hierarchy of Policy-Map

Marking and remarking are used without distinction. When there is a correspondent field to a incoming packet remarking will work, when no correspondent field marking will work. It enables other operations, which is not related to QOS, such as trap-cpu, mirrot, redirect, netflow, etc.

Table 254 Class-map Configuration Command

Command	Description	Mode
policy-map NAME	Generates a policy-map and moves to the corresponding node.	Config
no policy-map NAME	Deletes the policy-map.	Config
class NAME	Moves to the sub node which assigns the operation of Class-map.	pmap
no class NAME	Deletes the class-map setting.	pmap
drop	Drops traffic that is classified according to the class-map.	pmap-c
set cos <0-7>	Cos marking setting.	pmap-c
set drop-precedence <0-2>	Drop precedence setting.	pmap-c
set ip-dscp <0-63>	Dscp marking setting.	pmap-c
set ip-precedence <0-7>	Ip precedence (tos) setting.	pmap-c
set queueing <0-7>	Queueing setting.	pmap-c
police <1-10000000> <1-10000000> exceed-action drop	Rate-limit setting.	pmap-c
police aggregate NAME	Aggregated rate-limit setting.	pmap-c
nexthop A.B.C.D { priority <1-8> }	PBR nexthop setting and nexthop priority setting.	pmap-c
netflow	Netflow setting.	pmap-c
redirect IFNAME	Redirect setting.	pmap-c
mirror	Mirror setting.	pmap-c
trap-cpu { high-priority }	CPU trap setting.	pmap-c

Service-policy

The policy-map as above applies to VLAN interface or router port interface. It can be set as either direction of input or output. The policy-map set as above can be applied to VLAN interface or router port interface. It can be set as either direction of input or output. However, the output direction can have only one of service-policy or ACL; the input direction can have the two simultaneously.

Table 255 Service-Policy Configuration Command

Command	Description	Mode
service-policy { input output } NAME	Applies a policy-map of the relevant name to an interface.	interface
no service-policy { input output } NAME	Deletes the relevant policy-map from the interface.	interface



Notice

A router port means a port with no switchport.



Notice

Service-policy can set up to 16000 rules in the input direction, 4000 rules in the output direction summed with ACLs.



Notice

In the input direction, you can set service and ACL simultaneously. For the output direction, you can set only either one at a time.

COPP

COPP (Control Plane Policing) means the application of rate-limit and QOS policies of traffic which flow into CPU. Various controlling packets, relating to the protocol, flow into the CPU. An excessive inflow of a specific packet can cause a problem in the CPU. In this case, a packet with a higher priority of another protocol may not be carried out. Therefore, a feature that prioritizes packets and sets rate-limits is required in order to organize traffic.

Service-policy on COPP

The unit performs policing for traffic that flows into the CPU by applying service-policy in the control plane.

Table 256 Commands for Control-plane of Service-policy Configuration

Command	Description	Mode
control-plane	Enters control-plane mode.	configure
service-policy input NAME	Applies a policy-map to a control-plane.	Control-plane
no service-policy input NAME	Disables the policy-map on the control-plane.	Control-plane



Notice

When Service-policy is in use in control-plane, only police, drop, and set queueing operate.

Rate-limit on COPP

You can set a rate-limit of a specific traffic that flows into CPU.

Table 257 Commands for Control-plane of Rate-limit Configuration

Command	Description	Mode
rate-limit arp-reply <1-1000000> <0-7>	Selects the quantity of traffic (PPS) and queue of traffic that allows arp-reply among all traffic that flows into the CPU.	Control-plane
rate-limit arp-request <1-1000000> <0-7>	Selects the quantity of traffic (PPS) and queue of traffic that allows arp-request among all traffic that flows into the CPU.	Control-plane
rate-limit igmp <1-1000000> <0-7>	Selects the quantity of traffic (PPS) and queue of traffic that allows igmp among all traffic that flows into the CPU.	Control-plane
rate-limit ip-control-over-multicast <1-1000000> <0-7>	Selects the quantity of traffic (PPS) and queue of traffic that allows ip-control among all traffic that flows into the CPU.	Control-plane
rate-limit ipv6-neib-sol <1-1000000> <0-7>	Selects the quantity of traffic (PPS) and queue of traffic that allows ipv6 ns among all traffic that flows into the CPU.	Control-plane
rate-limit l4-port (both tcp udp) (both multicast unicast) <1-65535> <1-65535> <1-1000000> <0-7>	Selects the quantity of traffic (PPS) and queue of traffic that allows L4 traffic among all traffic that flows into the CPU.	Control-plane
rate-limit mld <1-1000000> <0-7>	Selects the quantity of traffic (PPS) and queue of traffic that allows mld among all traffic that flows into the CPU.	Control-plane

rate-limit multicast <1-1000000> <0-7>	Selects the quantity of traffic (PPS) and queue of traffic that allows multicast among all traffic that flows into the CPU.	Control-plane
rate-limit protocol <1-255> <1-1000000> <0-7>	Selects the quantity of traffic (PPS) and queue of traffic that allows a specific protocol among all traffic that flows into the CPU.	Control-plane
rate-limit ripv1 <1-1000000> <0-7>	Selects the quantity of traffic (PPS) and queue of traffic that allows rip(version 1) among all traffic that flows into the CPU.	Control-plane
rate-limit tcp-syn <1-1000000> <0-7>	Selects the quantity of traffic (PPS) and queue of traffic that allows tcp-syn among all traffic that flows into the CPU.	Control-plane
rate-limit udp-broadcast <1-1000000> <0-7>	Selects the quantity of traffic (PPS) and queue of traffic that allows udp broadcast among all traffic that flows into the CPU.	Control-plane

Chapter 18. GPON Configuration

This chapter describes how to make the setting in relation with GPON in the U9016B. This chapter consists of the following sections:

- GPON Overview
- OLT Management
- ONU/ONT Management
- GPON Function Setting

**Note**

Refer to the command reference for detailed description on the CLI commands used in this chapter.

GPON Overview

PON (Passive Optical Network) is an optical access network implementation method that enables a single OLT (Optical Line Termination) to multi ONUs (Optical Network Unit) or ONTs (Optical Network Terminal) access through a passive optical network on the fiber cable.

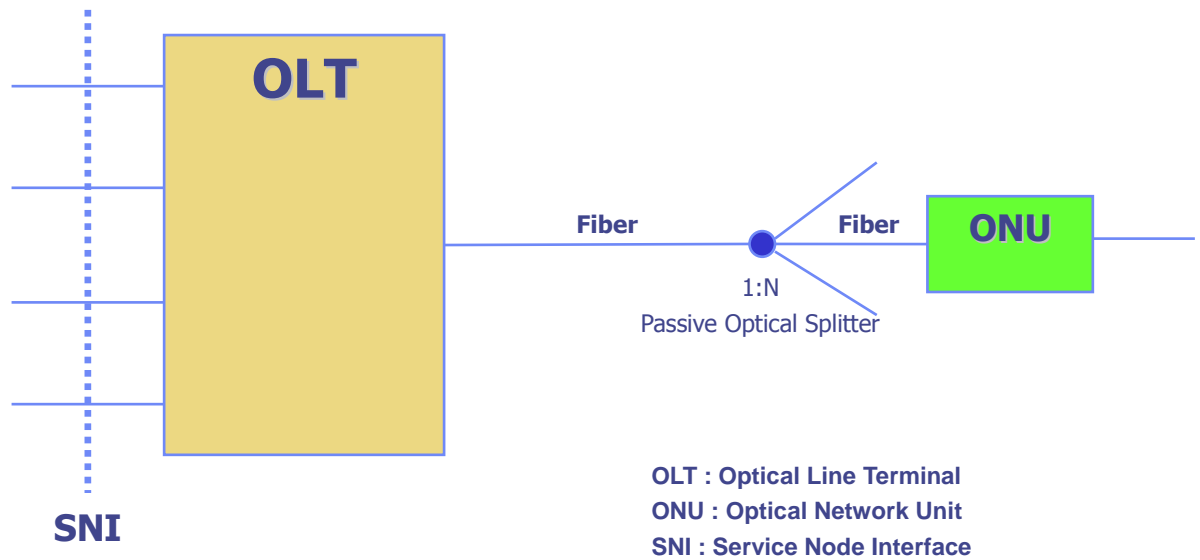


Figure 47. Basic Structure of PON

PON provides the point-to-multi point (P2MP) network so that the total bandwidth can be shared by multiple users through a passive optical splitter, saving the network implementation cost. The passive optical splitter does not require any power supply, providing convenience in field operation.

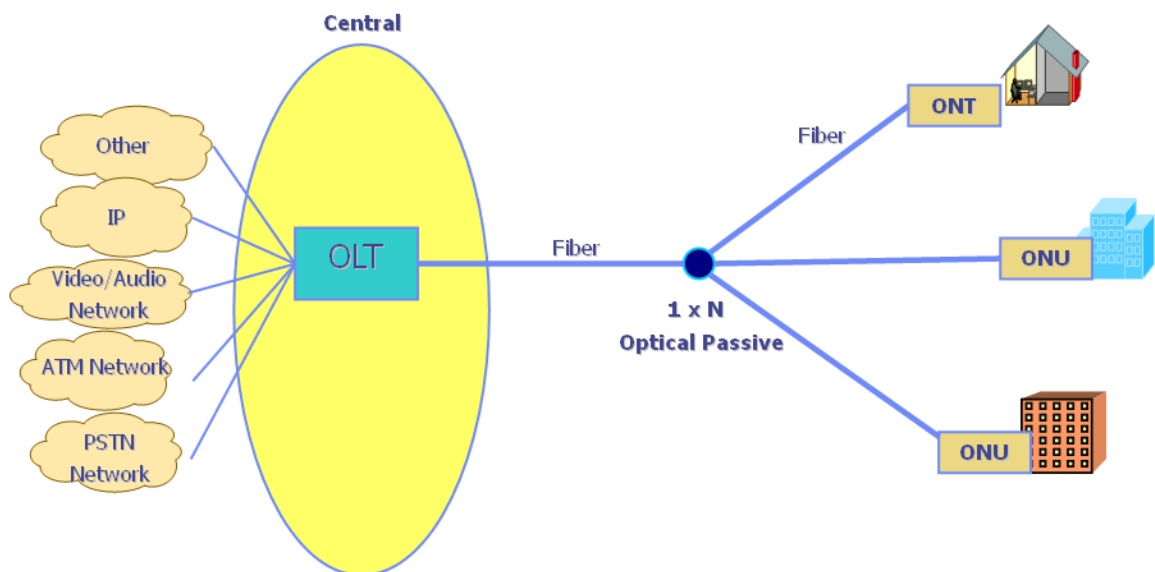


Figure 48. Architecture of GPON

GPON is a type of PON. In the FTTx network, OLT is typically installed in the central telephone office (CO) or the service provider, and is connected with numbers of ONUs or subscriber ONTs in 1:N split.

GPON adopts the broadcasting method for downstream and TDMA (Time Division Multiple Access) for upstream transmission.

On the downstream channel, each packet contains the ONU/ONT id (LLID) in the header, and the optical splitter divides and sends the packets to each ONU. Each ONU receives the packet for itself, and discards all other packets for other ONUs.

On the upstream channel, thanks to the characteristics of the optical splitter, the packet sent from an ONU/ONT is not sent to other ONU (ONT). As the packets of an ONU share a fiber, it is important to prevent collision between packets. TDMA is adopted so that ONU/ONT sends the data on the upstream channel during the time slot assigned by OLT.

OLT/ ONT Management

This section describes the guideline on OLT setting and method of OLT/ONT management.

Setting / View of PON OLT, Port status

The chapter describes the method to set administrative status on PIU interface card which plays an important role of PON. It is performed on gpon_mode, and it should be performed by entering the 'gpon' command in the config_mode. The PON port status of the system is 'enabled' in the factory default. The following table lists the commands to change and view the status.

Table 258 Setting/View of PON OLT, PORT status

Command	Description	Mode
show gpon topology olt	Shows all pon status of OLT	Enable
show gpon topology onu IF_NAME	Shows pon port status, onu status and link status	Enable
show gpon onu information IF_NAME	Shows status of ONU/ONT	Enable
show gpon onu detailed-information IF_NAME	Shows detailed status information of ONU/ONT	Enable
[no] shutdown port IF_NAME	Changes the administrative status of the PON port to [disable] enable.- IF_NAME : slot/port	Config-gpon
reset olt IF_NAME	OLT device reset	Config-gpon
show gpon stats olt-pp (downstream upstream) IF_NAME	Shows OLT PON interface performance.	Enable
show gpon olt dynamic bridging-entries IF_NAME	Shows OLT PON MAC list.	Enable
show gpon olt igmp (groups host) IF_NAME	Shows igmp group and host of OLT PON.	Enable
show gpon olt ddmi IFNAME (<1-64> idle)	Shows rx -power in OLT port	Enable

```
U9016B#show gpon topology olt
```

```
PON NETWORK OLT TOPOLOGY INFORMATION
```

```
=====
```

OLT	ADMIN	OPER	MODE	IPC STATE
1/1	ENABLE	UP	MIXED	UP
1/2	ENABLE	UP	MIXED	UP
1/3	ENABLE	UP	MIXED	UP
1/4	ENABLE	UP	MIXED	UP
1/5	ENABLE	UP	MIXED	UP
1/6	ENABLE	UP	MIXED	UP
1/7	ENABLE	UP	MIXED	UP
1/8	ENABLE	UP	MIXED	UP

```
=====
```

```
U9016B#show gpon topology onu 1/1
```

```
PON NETWORK ONU TOPOLOGY FOR OLT(1/1) INFORMATION
```

```
=====
```

IF_NAME	MAC ADDR LOCATION	ADMIN	OPER (DOWN DUR)	ONU TYPE	DISTANCE
1/1-1	5542.5153.7012.002e	ENABLE	UP	UBQS_601A	73 m
1/1-2	5542.5153.7002.101a	ENABLE	UP	UBQS_601A	73 m

```
=====
U9016B#show gpon onu information 1/1
```

OLT	ONU	STATUS	Serial No. (LOCATION)	Rx Power	Distance	Equip-id
1/1	1	Activate	5542.5153.7012.002e	-19.00	0.074km	UBQS_601A
1/1	2	Activate	5542.5153.7002.101a	-19.00	0.073km	UBQS_601A

```
=====
U9016B#show gpon onu detailed-information 1/1-1
```

```
-- GPON ONU DETAILED INFORMATION--
```

```
=====
OLT : 1/1, ONU : 1
```

```
-----
Activation Link Status      : Activate
Onu Serial Number          : 5542.5153.7012.002e
Onu Equip-id               : UBQS_601A
Onu Rx Power                : -19.00 dbm
Onu Distance                : 0.074 km
Onu Equaliztion Delay      : 266579
Onu Upstream FEC State     : Disable
Onu List of Alloc Id       : 640, 0
OMCI Port Id               : 0
Onu Encryption Key         : 00000000000000000000000000000000
Onu Host Name              :
Onu MAC Address            : 0007.7012.002e
-----
```

```
=====
U9016B#
```



Note In the case of using Shutdown port command: all links of the corresponding ports are down (disconnected).

Management/View of State of PON OLT and PORT (optical power alarm)

Table 259. Management/View of State of PON OLT and PORT (optical power alarm)

Command	Description	Mode
olt rx-optical-alarm threshold IF_NAME low LOW_THRESHOLD high HIGH_THRESHOLD	Sets the threshold of olt rx-power high/low	config-gpon
no olt rx-optical-alarm threshold IFNAME	Removes the threshold of olt rx-power high/low	config-gpon
olt rx-optical-alarm (enable disable)	Enables olt rx-power alarm	config-gpon
show gpon olt rx-optical-alarm threshold	Shows the threshold of olt rx-power high/low	enable
show gpon olt rx-optical-alarm status IF_NAME	Shows olt rx-power alarm state	enable

Management/View of State of PON OLT and PORT (performance check)

Table 260 Management/View of State of PON OLT and PORT (performance check)

Command	Description	Mode
clear gpon counters IFNAME module (all-modules xaui-all gmac-all packet-processor-downstream packet-processor-upstream)	Initializes the gpon statistics value by module of all gpon statistics values of all modules.	enable
show gpon stats olt-pp (upstream downstream) IF_NAME	Shows the OLT PON statistics value - (upstream downstream): Selects direction	enable

Management/View of State of PON OLT and PORT (others)

Table 261 Management/View of State of PON OLT and PORT (others)

Command	Description	Mode
show gpon olt igmp host IF_NAME <0-4095> A.B.C.D	Shows the OLT port igmp host	enable
show gpon olt igmp groups IF_NAME	Shows the OLT igmp group	enable
VLAN mapping IF_NAME tcont-id <1-4> s-VLAN <0-4095> c-VLAN <1-4095>	Sets QinQ service by ONT	config-gpon
no VLAN mapping IF_NAME tcont-id <1-4> (s-VLAN <0-4095> c-VLAN <1-4095>)	Clears the setting	config-gpon
show gpon VLAN mapping onu IFNAME	Shows the setting	enable
show gpon olt dynamic bridging-entries IF_NAME	Shows the dynamic mac address registered to the OLT	enable
clear olt dynamic mac-table IF_NAME	Clears the dynamic mac address registered to the OLT	config-gpon

Setting Status of ONU/ONT

The user executes the following commands to control PON port and user port which is registered in the OLT or to reset ONU/ONT status.

Table 262 Setting Status of ONU/ONT

Command	Description	Mode
[no] shutdown onu IF_NAME	Setting ONU/ONT pon admin status	Config-gpon
onu uni-status IF_NAME (enable disable)	Setting ONT uni port admin status IF_NAME : Slot/Port-Onu/Uni	Config-gpon
onu mib-upload limitation IF_NAME (enable disable)	Execute mip-upload of ONT/ONU enable : In the case of registering same ONT again, mib-upload is NOT executed again. disable : In the case of registering same ONT again, mib-upload is executed again.	Config-gpon
onu performance-monitoring IF_NAME (disable enable)	Sets ONU performance monitoring. When setting with disable, the all of performance showing value show with 0.	Config-gpon
deactivate onu IF_NAME	Executes ONT/ONU deactivation	Config-gpon
reset onu IF_NAME	Executes ONT/ONU reset	Config-gpon
show gpon stats ont-eth-count IF_NAME <1-4>	Shows performance per ONT UNI port.	Enable
show gpon stats ont-gemport-count IF_NAME	Shows performance per ONT gem-port.	Enable
show gpon onu dynamic bridging-entries IF_NAME	Shows mac list of ONT PON.	Enable
show gpon onu igmp groups IF_NAME	Shows igmp group list of OLT PON.	Enable

Management/View of State of ONU/ONT (OMCI-related)

Table 263. Management/View of State of ONU/ONT (OMCI-related)

Command	Description	Mode
VLAN-tagging-filter IF_NAME (tcont <1-4> uni <1-4> mapper <1-4>) (a_a a_e c_alf_prio_alf_prio_el_f_tci_alf_tci_el_f_vid_alf_vid_el_g_prio_alg_prio_el_g_tci_alg_tci_el_g_vid_alg_vid_el_h_prio_al_h_prio_el_h_tci_al_h_tci_el_h_vid_al_h_vid_e) filter-list <1-4095> <0-7> (<1-4095> <0-7> (<1-4095> <0-7> (<1-4095> <0-7> (<1-4095> <0-7> (<1-4095> <0-7> (<1-4095> <0-7> (<1-4095> <0-7> (<1-4095> <0-7> (<1-4095> <0-7> (<1-4095> <0-7> (<1-4095> <0-7>)))))	Sets VLAN-tagging-filter by ONT	config-onuqos
no VLAN-tagging-filter IF_NAME (tcont <1-4> uni <1-4> mapper <1-4>)	Clears VLAN-tagging-filter setting by ONT	config-onuqos

show gpon onu VLAN-tagging-filter IF_NAME	Shows VLAN-tagging-filter setting by ONT	enable
onu static-mac-binding IFNAME <1-4> H.H.H (H.H.H (H.H.H (H.H.H)))	Sets static-mac-binding	config-gpon
no onu static-mac-binding IFNAME <1-4> (H.H.H)	Clears static-mac-binding	config-gpon
show gpon onu static-mac-binding IFNAME	Shows static-mac-binding	enable
onu storm-control IF_NAME <1-4> broadcast <0-1000000> multicast <0-1000000>	Sets storm-control	config-gpon
"no onu storm-control IF_NAME <1-4>"	Clears storm-control	config-gpon
show gpon onu storm-control IF_NAME	Shows storm-control	enable
evtcd IF_NAME <1-4> <1-4> dn-mode (inverse none) filter ((untag singleTag (<0-4094> (<0-7> none) def) doubleTag ((<0-4094> (<0-7> none) <0-4094> (<0-7> none)) def)) thType (none ipoe pppoe arp)) treat (remTag0 remTag1 remTag2) outVid (noAdd ((<0-4094> cpyIn cpyOut) outPri (<0-7> cpyIn cpyOut))) inVid (noAdd ((<0-4094> cpyIn cpyOut) inPri (<0-7> cpyIn cpyOut)))	Sets Extend VLAN Tagging Operation Configuration Data	config-gpon-onuqos
no evtcd IF_NAME (uni <1-4> (rule <1-4>))	Clears Extend VLAN Tagging Operation Configuration Data	config-gpon-onuqos
onu upstream VLAN-tag <1-4095>	Sets the VLAN tag of the upstream traffic to be added in the ONT. (All ONTs in the system add the corresponding VLAN tag)	config-gpon
no onu upstream VLAN-tag	Clears the upstream tag setting	config-gpon
show gpon onu upstream VLAN-tag	Shows the upstream tag set	enable
show gpon onu evtcd IF_NAME	Shows Extend VLAN Tagging Operation Configuration Data	config-gpon-onuqos
show gpon onu omci ip-host-config-data IF_NAME	Shows omci ip-host-config-data	enable

show gpon onu dynamic bridging-entries IF_NAME	Shows the dynamic mac address registered to the ONT/ONU	enable
show gpon onu igmp groups IF_NAME	Shows the ONU igmp group	enable
show gpon hardware-version onu IF_NAME	Shows the hardware version of the ONT/ONU firmware	enable

Management/View of State of ONU/ONT (performance check)

Table 264. Management/View of State of ONU/ONT (performance check)

Command	Description	Mode
show gpon stats ont-gemport-count IF_NAME	Shows the statistics value of the ONT gem-port. - means Downstream.	enable
show gpon stats ont-eth-count IF_NAME <1-4>	Shows the statistics value of the ONT Uni. - means Upstream.	enable
onu performance-monitoring IF_NAME (enable disable)	Sets whether to show gem-port/UNI Performance monitoring history data or not	config-gpon

Management/View of State of ONU/ONT (optical power alarm)

Table 265. Management/View of State of ONU/ONT (optical power alarm)

Command	Description	Mode
show gpon onu optical-alarm threshold	Shows the threshold of ONT/ONU rx-power high/low	enable
onu optical-alarm threshold IF_NAME low PARAM1 high PARAM2	Sets the threshold of ONT/ONU rx-power high/low	config-gpon-cfmconfig
no onu optical-alarm threshold IFNAME	Removes the threshold of ONT/ONU rx-power high/low	config-gpon-cfmconfig
onu optical-alarm threshold (enable disable)	Enables ONT/ONU rx-power alarm	config-gpon-cfmconfig
show gpon onu optical-alarm status	Shows the ONT/ONU rx-power alarm state	enable

ONT Registration and Display

In order to use ONU/ONT as a resource of the system, user should register ONU/ONT with a specific index which is assigned by OLT according to the ONT/ONT activation procedure. The traffic from unregistered ONU/ONT is blocked. The following command is used to register ONU/ONT with a specific index that user want to apply when user does not use automatic registration.

It can be processed on gpon_mode.

For registration, user input interface name, serial number, location information of ONU/ONT.

Table 266 ONT Registration and Display

Command	Description	Mode
Topology onu IF_NAME serial SERIAL_NUMBER loc LINE	Register ONU/ONT as a system resource. - IF_NAME : Index(slot/port-onu) - SERIAL_NUMBER : xxxx.xxxx.xxxx.xxxx - LINE : location information strings	Config-gpon
onu-reg-mode (auto manual)	Sets ONT registration mode. When setting manual mode, The only ONU that serial-number is already registered is registered normally.	Config-gpon
show gpon onu-reg-mode	Shows ONT registration mode.	enable
show gpon onu information IF_NAME	Shows the status of registered ONU - IF_NAME : OLT Index (slot/port)	Enable
show gpon onu uni-frame-size status IF_NAME	Shows MTU size per ONU unit port.	enable
show gpon onu uni-mac-learning status IF_NAME	Shows maximum mac-learning number per ONU UNI port.	enable

U9016B#conf t

Enter configuration commands, one per line. End with CNTL/Z.

U9016B(config)#gpon

U9016B(config-gpon)#topology onu 1/1-1 serial 5542.5153.7012.002e loc GPON ONT

U9016B(config-gpon)#end

U9016B#show gpon onu information 1/1

```

-----
OLT  | ONU | STATUS |      Serial No.      | Rx Power | Distance | Equip-id
      |     |         | (LOCATION)             |           |           |
-----
1/1  |  1  | Inactive| 5542.5153.7012.002e |    0.00  | 0.000km |
      |     |         | GPON ONT             |           |           |
-----

```

U9016B#

Modification and Deletion of ONU/ONT Information

To change or delete ONU/ONT, use the following command. When user deletes ONU/ONT, the ONU/ONT is registered on unadmin-list and it is not re-registered until unadmin-list is cleared.

Table 267 Modification and Deletion of ONU/ONT Information

Command	Description	Mode
no topology onu <i>IF_NAME</i>	Deletes ONU/ONT which is registered.	Config-gpon
edit-onu loc <i>IF_NAME</i> LINE	Modifies the location information of ONU/ONT which is registered.	
show pon topolgy onu <i>IF_NAME</i>	Shows ONU registration status IF_NAME : OLT Index(slot/port)	Enable
show gpon unadmin-onu-list <i>IF_NAME</i>	Shows the deleted ONU which is registered on the unadmin-list	
onu password (enable disable)	Sets ONT password function.	Config-gpon
onu password EQUIP_ID PASSWORD	Sets password per ONU equip-id.	Config-gpon
no onu password INDEX	Deletes ONT password setting.	Config-gpon
show gpon onu password	Shows ONU password setting status.	enable
onu-auto-remove-timer <1-100>	Sets ONU auto-romove function. After ONT is down status and if the set time is ended, the relevant ONT information is deleted from topology.	Config-gpon
show gpon onu-auto-remove-timer	Shows ONU auto-remove function status.	enable

```
U9016B#conf t
U9016B(config)#gpon
U9016B(config-gpon)#edit-onu loc 1/1-1 UBIQUOSS
U9016B(config-gpon)#end
U9016B#show gpon onu information 1/1
```

OLT	ONU	STATUS	Serial No. (LOCATION)	Rx Power	Distance	Equip-id
1/1	1	Activate	5542.5153.7012.002e UBIQUOSS	-19.00	0.073km	UBQS_601A

```
U9016B#conf t
U9016B(config)#gpon
U9016B(config-gpon)#no topology onu 1/1-1
U9016B(config-gpon)#end
U9016B#show gpon onu information 1/1
```

OLT	ONU	STATUS	Serial No. (LOCATION)	Rx Power	Distance	Equip-id
-----	-----	--------	--------------------------	----------	----------	----------

```
U9016B#show gpon unadmin-onu-list 1/1
-- GPON UNADMIN ONU LIST : 1/1 --
```

IDX	SERIAL-NUMBER	REASON	EQUIP-ID
[1]	5542.5153.7012.002e	DEREGISTERED	UBQS_601A

```
U9016B#
```

Clear counters

Command	Description	Mode
clear gpon counters IF_NAME modules (all-modules xau1-all gmac-all packet-processor-downstream packet-processor-upstream)	Deletes the performance showing content of ONT PON interface.	enable

Clear unadmin-list

In the case of deleting ONU/ONT by using "no topology onu IF_NAME" command, the corresponding ONU/ONT information is registered on unadmin-list so that it cannot be re-registered in the OLT.

To register ONU/ONT again, user clears the unadmin-list that the deleted ONU/ONT is registered.

Table 268 Clear unadmin-list

Command	Description	Mode
clear gpon unadmin-onu-list IF_NAME serial SERIAL_NUMBER	Clears unadmin-list on a certain serial-number in the OLT port.	Config-gpon
clear gpon unadmin-onu-list IF_NAME all	Clears unadmin-list on all serial-number in the OLT port.	Config-gpon
clear gpon unadmin-onu-list all	Clears unadmin-list in the whole system.	Config-gpon
show gpon onu information IF_NAME	Shows ONU registration status	enable
show gpon unadmin-onu-list IF_NAME	Shows ONU unadmin-list	enable

```
U9016B#show gpon onu information 1/1
```

```
-----
OLT | ONU | STATUS | Serial No. | Rx Power | Distance | Equip-id
      (LOCATION)
-----
```

```
U9016B#
```

```
U9016B#show gpon unadmin-onu-list 1/1
```

```
-- GPON UNADMIN ONU LIST : 1/1 --
```

```
=====
IDX | SERIAL-NUMBER | REASON | EQUIP-ID
-----
[ 1] | 5542.5153.7012.002e | DEREGISTERED | UBQS_601A
=====
```

```
=====U9016B#
```

```
U9016B#clear gpon unadmin-onu-list 1/1 serial 5542.5153.7012.002e
```

```
U9016B#show gpon onu information 1/1
```

```
-----
OLT | ONU | STATUS | Serial No. | Rx Power | Distance | Equip-id
      (LOCATION)
-----
```

```
1/1 | 1 | Activate | 5542.5153.7012.002e | -19.00 | 0.073km | UBQS_601A
```

Automatic Deletion of unused ONU/ONT

The following command is to delete ONU/ONT information which is down status automatically. By using 'show gpon topology onu IF_NAME' command, user is able to check the duration time of ONU/ONT which is down status.

Table 269 Automatic Deletion of unused ONU/ONT

Command	Description	Mode
onu-auto-remove-timer <1-100>	Sets ONU/ONT unused automatically. Time duration can be set from 1 day to 100 days	Config-gpon
no onu-auto-remove-timer	Deletes onu-auto-remove-timer function	Config-gpon
show gpon onu-auto-remove-timer	Shows the status of onu-auto-remove-timer setting	Enable

```

U9016B#show gpon onu-auto-remove-timer
ONU AUTO REMOVE TIMER : disable
U9016B#
U9016B#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
U9016B(config)#gpon
U9016B(config-gpon)#onu-auto-remove-timer 100
U9016B(config-gpon)#end
U9016B#
U9016B#show gpon onu-auto-remove-timer
ONU AUTO REMOVE TIMER : 100 days
U9016B#
U9016B#
U9016B#show gpon topology onu 4/1
  PON NETWORK ONU TOPOLOGY FOR OLT(4/1) INFORMATION
=====
  IF_NAME      MAC  ADDR      ADMIN      OPER      ONU  TYPE
  DISTANCE
          LOCATION      (DOWN DUR)
-----
  4/1-1      504d.4353.d562.808f  ENABLE  CABLE DOWN  UBQS_601A      72 m
                                (2190 sec)
=====
U9016B#

```

ONU/ONT equip-id Authentication - Registration/Deletion/Display of equip-id

U9016B system supports equip-id authentication function to block the registration of unverified ONU/ONT. When ONT connects to OLT, ONU/ONT with registered equip-id can be registered to OLT. The ONU/ONT having un-registered equip-id cannot be registered on the OLT and it is registered on command. The unadmin-list User is able to register or delete the authenticated equip-id by the following command.

Table 270 ONU/ONT equip-id Authentication - Registration/Deletion/Display of equip-id

Command	Description	Mode
authenticated-equip-id add <i>EQUIP-ID DESCRIPTION</i>	Register authenticated equip-id	Config-gpon
authenticated-equip-id delete <i>EQUIP-ID</i>	Delete authenticated equip-id * Default equip-ID can not be deleted.	Config-gpon
show gpon authenticated-equip-id	Display authenticated equip-id	enable

```
U9016B#show gpon authenticated-equip-id
-- GPON AUTHENTICATED EQUIP_ID LIST--
```

```
=====
IDX |      EQUIP-ID      |      DESCRIPTION
-----
[ 1] | UBQS_ONU           | (D) ubiQuoss ONU
[ 2] | UBQS_601A          | (D) ubiQuoss 1port ONT
-----
(D) : default equip-id
```

```
=====
U9016B#conf t
U9016B(config)#gpon
U9016B(config-gpon)#authenticated-equip-id add UBQS_601B ubiQuoss ONT
U9016B(config-gpon)#end
U9016B#show gpon authenticated-equip-id
-- GPON AUTHENTICATED EQUIP_ID LIST--
```

```
=====
IDX |      EQUIP-ID      |      DESCRIPTION
-----
[ 1] | UBQS_ONU           | (D) ubiQuoss ONU
[ 2] | UBQS_601A          | (D) ubiQuoss 1port ONT
[ 3] | UBQS_601B          | ubiQuoss ONT
-----
(D) : default equip-id
```

```
=====
U9016B#
```

ONU/ONT equip-id Authentication: Function Usage

When ONU/ONT having un-authenticated equip-id attempts to connect to OLT, OLT registers the corresponding ONT's serial number into unadmin-list and change the status of the ONT as an emergency-stop status.

```
U9016B#show gpon authenticated-equip-id
-- GPON AUTHENTICATED EQUIP_ID LIST--
=====
IDX |      EQUIP-ID      |      DESCRIPTION
-----
[ 1] | UBQS_ONU           | (D) ubiQuoss ONU
[ 2] | UBQS_601A          | (D) ubiQuoss 1port ONT
-----
(D) : default equip-id
=====
U9016B#show gpon unadmin-onu-list 1/1
-- GPON UNADMIN ONU LIST : 1/1 --
=====
IDX | SERIAL-NUMBER | REASON | EQUIP-ID
-----
[ 1] | 4451.9245.5e27.3128 | UNAUTHENTICATED | U014PL-102
=====
U9016B#
```

To register the ONU/ONT which is blocked by equip-ip authentication function, the equip-id of blocked ONT/ONT is registered as an authenticated equip-id in the OLT and then execute 'clear gpon unadmin-list' command.

```
U9016B#conf t
U9016B(config)#gpon
U9016B(config-gpon)#authenticated-equip-id add U014PL-102
U9016B(config-gpon)#end
U9016B#
U9016B#clear gpon unadmin-onu-list 1/1 serial 4451.9245.5e27.3128
U9016B#
U9016B#show gpon onu information 1/1
=====
OLT | ONU | STATUS |      Serial No.      | Rx Power | Distance |      Equip-id
      (LOCATION)
-----
1/1 | 3 | Activate | 4451.9245.5e27.3128 | 19.00 | 0.071km | U014PL-102
-----
U9016B#
```

ONU/ONT Password: Setting the password function

The U9016B system provides a function to limit registration of unauthorized ONT by using the ONT password function.

When the password function for the ONT is configured in the U9016B system, the OLT extracts the password from the ONT when the ONT is initially registered to the OLT and determines whether to allow registration or not.

Table 271 ONU/ONT password function: Setting the password function

Command	Description	Mode
onu password (enable disable)	Sets ONT/ONU password authentication function	config-gpon
onu password IF_NAME PASSWORD	Sets the ONT/ONU password	config-gpon
no onu password IF_NAME	Removes the ONT/ONU password setting	config-gpon
show gpon onu password (IF_NAME)	Shows the password setting	enable

U9264_129#

U9016B_129#show gpon onu password

=====

ONU PASSWORD AUTHENTICATION INFO

=====

state : DISABLED

=====

U9016B_129#

U9016B_129#conf t

Enter configuration commands, one per line. End with CNTL/Z.

U9016B_129(config)#gpon

U9016B_129(config-gpon)#onu password 1/1-1 ONT_PASSWD

U9016B_129(config-gpon)#end

U9016B_129#show gpon onu password 1/1

=====

ONU PASSWORD AUTHENTICATION INFO

=====

state : ENABLED

=====

=====

IF_NAME | PASSWORD

1/1-1 | ONT_PASSWD

=====

U9016B_129#

ONU/ONT password function: How to perform the function

When an ONT of which password is not identical tries to register to the OLT, the OLT registers the serial-number of the ONT to the unadmin-list and limits registration.

```
U9016B_129#show gpon unadmin-onu-list 4/1
```

```
-- GPON UNADMIN ONU LIST : 4/1 --
```

```
=====
  IDX |   SERIAL-NUMBER   |   REASON   |   EQUIP-ID
-----
[  1] | 5542.5153.70cd.fe95 | ONU-PASSWORD | S674G
=====
U9016B_129#
```

To register the ONT to the OLT successfully while the password function has been enabled, the ONT should be configured with the password in advance.

VLAN Mapping Table Creation (QinQ Function)

To support QinQ function between OLT and ONT, VLAN mapping table is configured as follows:

Table 272 VLAN Mapping Table Creation (QinQ Function)

Command	Description	Mode
(no) VLAN mapping IF_NAME <1-4> s-VLAN <1-4095> c-VLAN <1-4095>	Create VLAN mapping table In the case of using QinQ, s-VLAN and c-VLAN are configured by referring to the corresponding mapping table	Config-gpon
show gpon VLAN mapping onu	Display VLAN mapping table	enable

VoIP Config Mode

Command	Description	Mode
(no) service voip IFNAME	Sets VoIP service per ONT.	Config-gpon
sip IF_NAME auth pots1 USERNAME PASSWORD pots2 USERNAME PASSWORD	Set SIP user name and password of SIP protocol.	Config-gpon-voipconfig
sip IF_NAME phone-number pots1 NUMBER pots2 NUMBER	Sets phone-number of SIP protocol.	Config-gpon-voipconfig
no sip IF_NAME (phone-number auth) (pots1 pots2)	Deletes phone-number or auth setting.	Config-gpon-voipconfig
(no) sip proxy-server A.B.C.D	Sets proxy-server address of SIP protocol.	Config-gpon-voipconfig
(no) sip register-server A.B.C.D	Sets register-server address of SIP protocol.	Config-gpon-voipconfig
(no) sip reg-exp-time <0-4294967294>	Sets registration expire time of SIP protocol.	Config-gpon-voipconfig
show gpon onu voip-config	Shows VoIP setting.	enable

PON Environment Setting

This section shows the commands and examples of PON OLT and ONU environment setting.

To set PON, user should write the service profile, and apply the profile to the interface. OLT / ONU Service Profile and the commands for OLT and ONU are available in OLT_QOS_MODE and ONU_QOS_MODE, respectively, which are sub-modes of GPON_MODE.

PON OLT Environment Setting

The OLT service profile consists of Policy-map, Bridge-map, and Igmp-map.

The Policy-map is configured by various items of alarm-setting and the Bridge-map is composed of the bridging configuration setting. Igmp-map is to set the IGMP functions.

The initial system setting is made on the service profile called 'oltProfile', and it contains 'oltPmap' as the Policy-map, 'oltBmap' as the Bridge-map, and 'oltlmap' as the Igmp-map.

Table 273 PON OLT Environment Setting

Command	Description	Mode
olt-qos	Changes a mode to write OLT Service Profile	Config-gpon

Configuring and Applying OLT Service Profile

To write the OLT service profile, user should write Policy-map and Bridge-map and Igmp-map first. The following tables show the commands how to write/delete service profiles and apply it to the OLT port interface:

Table 274 Writing and Applying OLT Service Profile

Command	Description	Mode
service-map PROFILE_NAME policy-map POLICY_NAME bridge-map BRIDGE_NAME igmp-map IGMP_NAME	Writes OLT Service Profile - PROFILE_NAME : Service Profile Name - POLICY_NAME : Policy-map Name - BRIDGE_NAME : Bridge-map Name - IGMP_NAME : Igmp-map Name	Config-gpon-oltqos
no service-map PROFILE_NAME	Deletes OLT Service Profile - Default Profile (oltProfile) and the profile applied to the current interface are not deleted.	Config-gpon-oltqos

Table 275 Deleting and displaying Policy map

Command	Description	Mode
no policy-map MAP_NAME	Deletes OLT Policy-map - The map in service is not deleted.	Config-gpon-oltqos
no bridge-map MAP_NAME	Deletes OLT Bridge-map - The map in service is not deleted.	Config-gpon-oltqos
service-policy IF_NAME service-map PROFILE_NAME	IF_NAME : Name of the OLT port interface PROFILE_NAME : OLT service profile name	Config-gpon-oltqos
show gpon service-map olt (SERVICE_MAP)	Shows the OLT Service profile list or the details of a specific service profile	Enable
show gpon service-policy olt	Shows the service profile applied to the OLT port	Enable

(SERVICE_NAME I)	interface.	
------------------	------------	--

Configuring an OLT Policy-map

OLT Policy-map consists of alarm setting of OLT port.

By using the 'policy-map' command, user changes the OLT_QOS_MODE to OLT_PMAP_MODE.

Table 276 Writing an OLT Policy-map

Command	Description	Mode
olt-qos	Enters the OLT Service Profile write mode	Config-gpon
(no) policy-map MAP_NAME	Enters the Policy-map write mode.	Config-gpon-oltqos
alarm (dowi rdii loami lcdgi) (enable disable)	dowi : ONU transmission is received at an expected place within the virtual frame rdii : RDI fields asserted loami : Three consecutive PLOAM message is lost lcdgi : GEM fragment delineation is lost	Config-gpon-oltqos-pmap
alarm (loai pee loki tiwi tia) (enable disable)	loai : OLT does not receive any acknowledgement pee : OLT receives the PEE from the ONU loki : Key transmission message is failed tiwi : Drift of ONU transmission exceed the threshold tia : ONU turns on its laser at a time assigned to another ONU	Config-gpon-oltqos-pmap
alarm sdi (enable <4-9> disable)	sdi : Upstream BER is $\geq 10^{-x}$ - Range of x is 4 to 9	Config-gpon-oltqos-pmap
alarm sfi (enable <3-8> disable)	sfi : Upstream BER is $\geq 10^{-y}$ - Range of y is 3 to 8	Config-gpon-oltqos-pmap
Map-end	Finishes writing the Policy-map and moves to the upper mode. (if user doesn't enter this command, no map is created. Therefore, user should always write this command to move to the upper mode.)	Config-gpon-oltqos-pmap
show gpon policy-map olt (POLICY_MAP I)	Shows the OLT Policy-map list or the details of a specific Policy-map.	enable

Configuring OLT Bridge-map

OLT Bridge-map includes the OLT port Bridge setting. Change the mode from OLT_QOS_MODE to OLT_BMAP_MODE with the 'bridge-map' command in order to write OLT bridge-map.

Table 277 Configuring OLT Bridge-map

Command	Description	Mode
olt-qos	Enters the OLT Service Profile write mode.	Config-gpon
bridge-map MAP_NAME	Switches to the Bridge-map write mode.	Config-gpon-oltqos
base-map MAP_NAME	Selects existing OLT bridge-map to use with base-map. When executing, it copys relevant bridge-map and use it.	Config-gpon-oltqos
address-table s-VLAN (none <1-4095>) (forwarding-mode (1:1 N:1)) (use-s-VLAN (on off)) (use-c-VLAN (on off)) (use-priority (on off)) (discard-unknown (on off))	s-VLAN : Set service VLAN id forwarding-mode : Set OLT forwarding-mode 1:1 is operated based on VLAN, N:1 is on mac. use-c-VLAN : Set client VLAN enable or disable use-priority : Set use-priority enable or disable discard-unknown : Set to enable/disable to discard unknown traffic	Config-gpon-oltqos-bmap
bridgeconfig (remove-when-aged (on off)) (discard-unlearned-sa (on off)) (learned-entry-age-limit <5-17280>)	remove-when-aged : set entry deletion discard-unlearned-sa : set to enable/disable unlearned source address discard learned-entry-age-limit : set aging time	Config-gpon-oltqos-bmap
bridgeconfig VLAN priority-mapping (upstream downstream) <0-7> <0-7> <0-7> <0-7> <0-7> <0-7> <0-7> <0-7>	Sets the priority-mapping value of upstream/downstream	Config-gpon-oltqos-bmap
bridgeconfig VLAN 1:1 <0-4094>	Sets VLAN 1:1 mode	Config-gpon-oltqos-bmap
show gpon bridgeconfig olt IF_NAME	Shows OLT bridgeconfig setting.	enable
VLAN downlink s-VLAN (none <1-4095>) (double-tag-handling (on off)) (VLAN-priority-handling (on off))	VLAN downlink setting double-tag-handling : double tagging setting VLAN-priority-handling : priority handling setting	Config-gpon-oltqos-bmap
dot1q-encapsulation enable	Enables QinQ function from OLT PON side.	Config-gpon-oltqos-bmap
dot1q-encapsulation disable	Disables QinQ function from OLT PON side.	Config-gpon-oltqos-bmap
dot1q-encapsulation vlan ethertype (uplink downlink) SVID_ETHER_TYPE CVID_ETHER_TYPE	When QinQ function is enabled from OLT PON side, it designates s-vid ethertype and c-vid ethertype per uplink and downlink. Default value is 0x8100(s-vid and c-vid)	Config-gpon-oltqos-bmap
dhcp option82 (enable (rate-limit <0-512>) disable)	Sets the dhcp option82 function of the OLT PON	config-gpon-oltqos-bmap

pppoe vendor-tag (enable (rate-limit <0-512>) disable)	Sets the PPPoE vendor-tag add function of the OLT PON	config-gpon-oltqos-bmap
igmp translate-vid ((enable VLAN_TAG) (rate-limit <0-512>) disable)	Sets the igmp VID change function of the OLT PON	config-gpon-oltqos-bmap
address-table migration (enable disable)	Sets whether to allow/limit the MAC move of the OLT PON	config-gpon-oltqos-bmap
Map-end	Finishes writing the Bridge-map and moves to the upper mode. (If you don't enter this command, no map is created. Therefore, you should always write this command to move to the upper mode.)	Config-pon-oltqos-bmap
show gpon bridge-map olt (BRIDGE_MAP)	Shows the OLT Bridge-map list or the details of a specific Bridge-map.	Enable

OLT Igmp-map

OLT Igmp-map includes the setting of IGMP protocol in OLT port. Change the mode from OLT_QOS_MODE to OLT_IMAP_MODE with the 'igmp-map' command to write OLT Igmp-map.

Table 278 IP OLT Igmp-map

Command	Description	Mode
olt-qos	Enters the OLT Service Profile write mode	Config-gpon
(no) igmp-map MAP_NAME	Enters the Igmp-map write mode.	Config-gpon-oltqos
(no) ip igmp discard-untagged	Sets discard of untagged frame.	Config-gpon-oltqos-imap
(no) ip igmp ignore-VLAN	Sets discard of VLAN tag.	Config-gpon-oltqos-imap
ip igmp last-member-query-count <1-8> no ip igmp last-member-query-count	Sets last-member-query-count.	Config-gpon-oltqos-imap
ip igmp last-member-query-interval <1-255> no ip igmp last-member-query-interval	Sets last-member-query-interval.	Config-gpon-oltqos-imap
ip igmp query-interval <1-18000> no ip igmp query-interval	Sets query-interval.	Config-gpon-oltqos-imap
ip igmp ra-option no ip igmp ra-option	Sets IGMP Strict RA option validation.	Config-gpon-oltqos-imap
ip igmp robustness-variable <1-8> no ip igmp robustness-variable	Sets the robustness counter.	Config-gpon-oltqos-imap
ip igmp snooping fast-leave no ip igmp snooping fast-leave	Sets igmp snooping fast-leave.	Config-gpon-oltqos-imap
ip igmp version <1-3> no ip igmp version	Sets igmp version.	Config-gpon-oltqos-imap
ip igmp mode (disable snoop proxy)	Sets igmp mode.	Config-gpon-oltqos-imap
ip igmp VLAN-select (inner outer)	In receiving double tag frame, set to choose inner or outer tag.	Config-gpon-oltqos-imap
Map-end	Finishes writing the Igmp-map and moves to the upper mode. (If you don't enter this command, no map is created. Therefore, you should always write this command to move to the upper mode.)	Config-gpon-oltqos-imap
show gpon igmp-map olt (IGMP_MAP I)	Displays the OLT Igmp-map list or the details of a specific Igmp-map.	Enable

PON ONU Environment Setting

The ONT service profile consists of Sla-map, Bridge-map, and Multicast-map.

Sla-map configures SLA setting of the Link. Bridge-map is to set bridging configuration. Multicast-map is to set parameters related to Multicast service.

Sla-map, Bridge-Map, and Multicast-map configure service-policy which is a service profile applied to the ONT currently registered.

In the system, default service policy with equip-id is set to the ONT automatically when ONT is registered.

In addition, Sla-map, Bridge-map, and Multicast-map can be set to the ONT respectively. The service-policy which is set by user is applied prior to default service-policy.

The default service-policy by equip-id is shown as below table. Default service-policy can be added via CLI.

Table 279 PON ONU Environment

equip-id	sla-map	bridge-map	multicast-map
UBQS_ONU	ubqs1000	hybridBmap	mcastMap-noSnoop
UBQS_601A	ubqs1000	ont1PortBmap	mcastMap-snoop
H645A	ubqs1000	ont1PortBmap	mcastMap-snoop

User can write the ONU service profile in ONU-QOS_MODE, which is the sub-mode of GPON_MODE.

Table 280 PON ONU Environment Setting

Command	Description	Mode
onu-qos	Switches to the ONU Service Profile write mode.	Config-gpon-onuqos

Creating and Deleting ONU Sla-map

The ONU Sla-map configures the SLA setting of the ONU link. As below table, to write Sla-map, user should switch the mode from 'ONU_QOS_MODE' to 'ONU_SMAP_MODE' with the 'sla-map' command in the GPON_MODE.

Table 281 Creating and Deleting ONU Sla-map

Command	Description	Mode
onu-qos	Enters the ONU Service Profile write mode.	Config-gpon
sla-map MAP_NAME	Enters the sla-map write mode.	Config-gpon-onuqos
upstream sla <1-4> (data voip) (nsr type0 type1) <1-1244> <0-15> <1-1244> <0-15>	Sets the UpstreamSLA of ONU Links - tcont <1-4> : Select tcont ID to set SLA - (data voip) : Select service type - (nsr type0 type1) : Select status-report type - Guaranteed bandwidth : <1-1244> - Fine Guaranteed bandwidth : <0-15> - Best Effort bandwidth : <1-1244> - Fine Best Effort bandwidth : <1-1244>	Config-pgon-onuqos-smap

downstream policing <1-4> <1-2500> <1-2500>	Sets the downstream policing of ONU Links - tcont <1-4> : Select tcont ID to set policing - Committed Bandwidth in Mbps : <1-2500> Excess Bandwidth in Mbps : <1-2500>	Config-pon-onuqos-smap
show gpon sla-map onu (MAP_NAME)	Shows the ONU Sla-map list or the details of a specific Sla-map.	enable

Creating and Deleting ONU policy-map

ONU Policy-map includes the settings about User port, Bridge of Link, OMCI ME, encryption, and fec.

Table 282 Creating and Deleting ONU policy-map

Command	Description	Mode
onu-qos	Enters onu-qos mode.	Config-gpon
policy-map MAP_NAME base-map MAP_NAME	Creates ONT policy-map. When creating policy-map, specify existing default policy-map with base-map.	Config-gpon-onuqos
mapper <1-4>	Sets 802.1p mapper service profile - To set up the 802.1p mapper service profile, mapper mode is accessed. - Up to 4 mapper can be created.	Config-gpon-onuqos-bmap
gemport count (1 2 4)	Sets gem-port number to use per ONT.	Config-gpon-onuqos-pmap-mapper
gem-port-mapping <1-4> tcont <1-4>	Appoint tcon ID per gem-port	Config-gpon-onuqos-bmap-mapper
default-pbit-marking (enable disable)	Set the function whether pbit of all frames is changed to the default value or not.	Config-gpon-onuqos-bmap-mapper
default-cos <0-7>	Sets the value of default pbit in case that default-pbit-marking function is activated.	Config-gpon-onuqos-bmap-mapper
unmarked-frame-option (0 1)	Sets the unmarked-frame-option - 0 : Convert from DSCP to 802.1p - 1 : Tag frame to a certain value	Config-gpon-onuqos-bmap-mapper
bridge <1-4>	Sets MAC bridge service profile - access to the bridge mode to configure MAC bridge service profile..	Config-gpon-onuqos-bmap
mac-learning	Sets MAC-Learning function - Configure it to activate or deactivate the function of bridge learning .	Config-gpon-onuqos-bmap - bridge
uni <1-4>	Access to uni mode to configure UNI which is connected to the MAC bridge service profile.	Config-gpon-onuqos-bmap - bridge
uni-mtu-size <64-2032>	Sets the size of mtu that UNI is capable of.	Config-gpon-onuqos-bmap - bridge-uni

351

	used or not.	onuqos-bmap - bridge
fec upstream (enable disable)	Configures whether fec is used or not.	Config-gpon-onuqos-bmap - bridge
Show gpon bridge-map onu (MAP_NAME)	Shows the ONU bridge-map list or the details of a specific Bridge-map	Enable
"voip-config"	Changes the mode to the voip-config configuration mode	config-gpon-onuqos-pmap
"no voip-config"	Removes the voip-config configuration	config-gpon-onuqos-pmap
"fax-mode (t-38 pass-thru)"	Sets the fax-mode of the voip-config	config-gpon-onuqos-pmap-voipconfig
"no fax-mode"	Removes the fax-mode configuration	config-gpon-onuqos-pmap-voipconfig
"codec (1 2 3 4) (pcmu pcma g722 g723 g728 g729 gsm) packet-period <10-30> silence-suppression (on off)"	Sets the codec	config-gpon-onuqos-pmap-voipconfig
"no codec (1 2 3 4)"	Removes the codec configuration	config-gpon-onuqos-pmap-voipconfig

Creating and Deleting ONU Bridge-map

The ONU Bridge-map configures Bridge Setting for user port, link, OMCI ME. It also includes encryption and fec settings.

To write the map, user should switch the mode from `onu_qos_mode` to `onu_bmap_mode` with the 'bridge-map' command.

Table 283 Writing and Deleting ONU Bridge-map

Command	Description	Mode
onu-qos	Enters the ONU Service Profile write mode.	Config-gpon
bridge-map MAP_NAME	Creates ONU bridge-map	Config-gpon-onuqos
max-host<0-255>	Sets MAC learning depth - usually used to limit no. of MAC (mac-limit) address per user port.	Config-gpon-onuqos-bmap – bridge
Show gpon bridge-map onu (MAP_NAME)	Shows the ONU bridge-map list or the details of a specific Bridge-map	Enable

Writing and Deleting ONU Multicast-map

ONU Multicast-map includes the configurations related to the multicast service of ONU. To write the map, user should switch the mode from `onu_qos_mode` to `onu_mcastmap_mode` with the 'igmp-map' command.

Table 284 Writing and Deleting ONU Multicast-map

Command	Description	Mode
onu-qos	Enters the ONU service profile write mode	Config-gpon
multicast-map MAP_NAME	Enters the multicast-map write mode.	Config-gpon-onuqos
group-range start A.B.C.D end A.B.C.D (no) group-range	Sets the range of multicast group	Config-gpon-onuqos
igmp snoop version <1-3> no igmp snoop version	Sets the version of igmp snoop In the case of using 'no igmp snoop version' command, IGMP version 2 is configured as a default value.	Config-gpon-onuqos-mcastmap
(no) igmp snoop fast-leave	Activates or deactivates igmp snoop fast-leave	Config-gpon-onuqos-mcastmap
igmp snoop max-groups eth <1-4> <0-1000> no igmp snoop max-groups eth <1-4>	Sets the max number of groups per user port. In using 'no' command, the number of group can be appointed at the maximum number. (release the limit.)	Config-gpon-onuqos-mcastmap
(no) igmp snoop	Activates or deactivates igmp snooping	Config-gpon-onuqos-mcastmap
Map-end	Finishes writing the multicast-map and moves to	Config-pn-

	the upper mode. (if you don't enter this command, no map is created. Therefore, user should always write this command to move to the upper mode.)	oltqos-imap
igmp upstream-tag-control VLAN_ID COS tag-control (none add_vid replace_vid replace_vid_cos)"	Sets VLAN tag processing for the igmp control packet	config-gpon- onuqos- mcastmap
no igmp upstream-tag-control	Removes the setting	config-gpon- onuqos- mcastmap
downstream tag-control mode (transparent strip_tag replace_only_vid vid <1-4095> (add_tag replace_tag) vid <1- 4095> cos <0-7>)	Sets VLAN tag processing for the multicast downstream traffic	config-gpon- onuqos- mcastmap
no downstream tag-control	Removes the setting	config-gpon- onuqos- mcastmap
igmp upstream rate-limit <0-100>	Sets the rate-limit for the igmp control packet	config-gpon- onuqos- mcastmap
no igmp upstream rate-limit	Removes the setting	config-gpon- onuqos- mcastmap
service eth <1-4>	Enables/disables the multicast service by UNI	config-gpon- onuqos- mcastmap
no service eth <1-4>	Removes the setting	config-gpon- onuqos- mcastmap
Show gpon multicast-map onu (MAP_NAME)	Shows ONU Multicast-map List or the details of a specific Multicast-map	Enable

Configuration and Display of ONU default service-policy

User configures the ONU default service policy so that the ONT can be configured based on the default service policy matching the equip-id of the ONT automatically when ONT is registered.

Table 285 Configuration and Display of ONU default service-policy

Command	Description	Mode
default service-policy EQUIP_ID bridge-map MAP_NAME sla-map MAP_NAME (multicast-map MAP_NAME) no default service-policy POLICY_INDEX	Sets ONU Default service-policy. - SLA_NAME : Sla-map Name - BRIDGE_NAME : Bridge-map Name - IGMP_NAME : Igmp-map Name	Config-gpon- onuqos
show gpon default service-policy onu	Shows ONU default Service-policy.	Enable
"no default service-policy POLICY_INDEX"	Removes the ONU default service-policy setting	config-gpon- onuqos
"default policy-map EQUIP_ID MAP_NAME"	Sets the ONT/ONU default policy-map - MAP_NAME : Policy-map name	config-gpon- onuqos

Configuration, Display and Deletion of ONU service-policy

Table 286 Configuration, Display and Deletion of ONU service-policy

Command	Description	Mode
service-policy IFNAME BRIDGE_MAP SLA_MAP (mcast- map MAP_NAME) (vlan-tag <0- 4095> <0-4095> <0-4095> <0-4095>)	Sets ONU service-policy - IFNAME : Interface Name - BRIDGE_MAP : Bridge-map Name - SLA_MAP : Sla-map Name - MCAST_MAP : multicast-map Name - VLAN-tag : VLAN-tag is the configuration of upstream tag which is applied to VLAN-tagging- operation-config on the ONT bridge-map. In the case of existing the VLAN-tag configurations in the bridge-map and service policy map, bridge-map configuration is applied preferentially. - Setting the multicast map and the VLAN tag is optional. (if not input mcast-map configuration, igmp snoop is not activated.	Config-gpon- onuqos
no service-policy IFNAME	Deletes the service-policy which is applied to ONU. - The service-profile using in the working ONU applied can not be deleted.	Config-gpon- onuqos
show pon service-policy onu (IF_NAME)	Shows the service-policy applied to ONU	enable

Defective Optic Module ONT Management

Auto Shutdown of ONU/ONT with fiber optic module fault

This function detects ONT which occur a fault of optic module, and then automatically shuts down the ONT to prevent network service failure.

Table 287 Auto shutdown of ONU/ONT with fiber optic module fault

Command	Description	Mode
ldshutdown (enable disable)	Activate/Deactivate LD shutdown function	Config-gpon
show gpon ldshutdown	Shows the status of LD shutdown function	Enable

Limiting the tx-power of ONT fiber optic module

Users can limit the tx-power of ONT fiber optic module for the time period set.

Table 288 limiting the tx-power of ONT fiber optic module

Command	Description	Mode
ldshutdown onu IF_NAME <0-65535>	IF_NAME : slot/port-onuld <0-65535> : Set time(sec.) to limit tx-power (0 : permanently, Unit: second)	Config-gpon

Firmware upgrade

OLT firmware upgrade

User upgrades OLT firmware through tftp as below commands.

Table 289 OLT firmware upgrade

Command	Description	Mode
software download olt (address IF_NAME) FILENAME (A.B.C.D)	<p>Upgrades the firmware of the OLT system</p> <p>address : Input the address at slot/port. The name of port must be '1' or '5' because OLT is using 2 PON Chips per one slot. For example, port no. 1 covers port 1,2,3,4 and port no. 5 covers port 5,6,7,8. User can input multiple addresses to upgrade numbers of address at the same time. e) 1/1, 1/5, 2/1, 1/1~2/1, 1/1, 1/5, 2, 1 If user does not input the address, all PON ports and slots is upgraded.</p> <p>FILENAME : input the firmware file name to be upgraded. (A.B.C.D) : input tftp server address If not input the address, OLT attempts to find the firmware file in the flash memory of the OLT and then upgrade the firmware. (if there is no firmware file in the flash memory, OLT terminates the upgrade function.)</p> <p>Checking the upgrade progress. : To check the status of upgrade, user input the 'terminal monitor' command in the enable mode before doing upgrade. When upgrade is completed, the log message 'completed' is displayed and upgraded pon chip is reloaded.</p>	Config-gpon
show gpon software olt	Shows the version of OLT firmware.	enable

--> The below example is shown how to download and upgrade the firmware at Second pon chip of 4th slot.

U9016B#show gpon software olt

DEV_NAME	F/W VER	H/W VER
4/1	2.1.5.2	5211 2
4/2	2.1.4.4	5211 2

Host Version : 1.2.50

U9016B#

U9016B#configure terminal

U9016B(config)#gpon

U9016B(config-gpon)#software download olt address 4/5 PAS5211_v2_1_build_5_2.bin 192.168.0.9

U9016B(config-gpon)#Jan 1 02:15:53 [5] OLT IMAGE UPGRADE STATUS: transfered Slot 4 Port 0 with pmc/PAS5211_v2_1_build_5_2.bin image

U9016B(config-gpon)#Jan 1 02:16:10 [5] OLT IMAGE UPGRADE STATUS: completed Slot 4 Port 0 with pmc/PAS5211_v2_1_build_5_2.bin image

U9016B(config-gpon)#

U9016B(config-gpon)#end

U9016B#show gpon software olt

DEV_NAME	F/W VER	H/W VER
4/1	2.1.5.2	5211 2
4/2	2.1.5.2	5211 2

Host Version : 1.2.50

U9016B#

ONT/ONU firmware upgrade (manual-upgrade)

TO upgrade the ONT/ONU pon chip firmware, you must enter the ONT information and firmware information in advance.

This function avoids a non-compatible firmware being downloaded to the ONT.

Table 290. ONT/ONU firmware upgrade (manual-upgrade)

Command	Description	Mode
software download support-info EQUIP_ID DELIMITER (pmc broadlight broadcom (delimiter-position POSITION))	Sets the information on firmware upgradable for ONT/ONU - Set the vendor or the starting position of the delimiter. - (pmc broadlight broadcom) : Select one of chip vendors. - (delimiter-position POSITION): Sets the starting position of the delimiter.	config-gpon
no software download support-info INDEX_NUMBER	Removes the firmware information set in the software download support-info. - INDEX_NUMBER: The number which saves the firmware information	config-gpon
show gpon software download support-info	Shows the information on the firmware set for upgrading ONT/ONU firmware	enable

User upgrades ONT/ONU firmware through tftp as below commands.

Table 291 ONT/ONU firmware upgrades (TFTP)

Command	Description	Mode
software download onu (address IF_NAME) (image-id <0-1>) FILENAME (A.B.C.D)	<p>Upgrades the firmware of ONT/ONU address : The type of address is input as 'slot/port-onu' . User can input a number of addresses or range interfaces to upgrade multiple ports of ONUs. ex) ONT 1/1-1, 1/1-2, 1/1-3 : 1/1-1~1/1-3 or 1/1-1,1/1-2,1/1-3 If user does not input the address, all ONT is upgraded.</p> <p>image-id <0-1> : GPON ONT/ONU supports dual images. User input the image number which is applied to ONT/ONU for upgrade.</p> <p>FILENAME : Input file name of firmware to be upgraded.</p> <p>(A.B.C.D) : Input tftp server address. If not input the address, the system attempts to find the firmware file in the flash memory and then upgrade the firmware. (if there is no firmware file in the flash memory, the system terminates the upgrade function.)</p> <p>Checking the upgrade progress. : To check the status of upgrade, user input the 'terminal monitor' command in the enable mode before doing upgrade. When upgrade is completed, the log message 'completed' is displayed. To apply upgraded firmware, the ONT should be reloaded. (uses 'software activate' command for s/w reload.)</p>	Config-gpon
software commit onu IF_NAME <0-1>	Commit ONU/ONT to use the image-id for next booting. However, if ONT power is on/off, ONT is not applied to the committed firmware image-id. Only executing the command 'software activate', committed image-id is applied to the ONT.	Config-gpon
software activate onu IF_NAME <0-1>	Reload ONT software and do booting with selected image-id.	Config-gpon
show gpon software onu IF_NAME	Shows the version of firmware ONT/ONU is using.	enable
software download support-info EQUIP_ID DELIMITER (broadcom broadlight pmc (delimiter-position <1-1000>))	Inserts equip-id information applied f/w download. Equip-id that the support information does not exist is not supported f/w download.	Config-gpon
show gpon software support-info	Shows download support information.	Enable

show gpon software manual-download status	Shows the firmware download progresss state	enable
--	---	--------

ONT/ONU firmware Upgrade (Auto-Upgrade)

U9016B GPON OLT supports auto-upgrade function for ONT/ONU firmware.

Auto-upgrade function does not perform the firmware download by interfaces which is the method of manual-upgrade. When user uploads the firmwares of each ONTs into the flash memory and then executes auto-download function, the system upgrades the firmware of all ONTs registered in the OLT.

Table 292 ONT/ONU firmware upgrades (auto-upgrade)

Command	Description	Mode
software add onu FILENAME A.B.C.D	Uploads the firmware file into flash memory from tftp server. Up to 10 firmware files can be uploaded.	Config- gpon
software remove onu FILENAME software remove onu all	Deletes the firmware file for auto-upgrade in the flash memory.	Config- gpon
software auto-download onu start (autoReset (time <0-23>) manualReset)	Activate the auto-download function autoReset : reload the ONT completing upgrade by force. time (0-23) : configure the time to process autoReset (0 o'clock ~ 23 o'clock. Fixed time) manualReset : AutoReset is not executed for the ONT completing upgrade. To apply firmware upgraded, user execute the reload via CLI.	Config- gpon
software auto-download onu stop	Deactivates the auto-download function	Config- gpon
show gpon software auto- download status SLOT	Shows the status of auto-download progress and firmware lists.	enable

Chapter 19. IPv6 Configuration

This chapter describes how to configure the IPv6 address.

Overview

First, prior to configuring IPv6, you should assign the IPv6 address to the network interface. By assigning the IPv6 address to the interface, the interface is enabled as a Layer3 interface.

The U9016B OLT can assign the IP to the following interfaces:

- VLAN interface
- Loopback interface
- Management interface

Assigning IPv6 Address

The IPv6 address is a 128-bit identifier for one interface or a set of multiple interfaces. The IPv6 address is classified into the following three types:

- **Unicast:** An identifier for one interface. Packets with the Unicast address are sent to the interface identified with that address.
- **Anycast:** An identifier for a set of interfaces which belongs to another node. Packets with the Anycast address are sent to the nearest interface among all interfaces identified with that address, and this decision is based on calculating the routing protocol distance.
- **Multicast:** An identifier for a set of interfaces which belong to another node. Packets with the Multicast address are sent to all interfaces identified with that address.



Notice

For the official technical description for IPv6 address, refer to RFC2460, IPv6 Specification or RFC3513, IPv6 Addressing Architecture.



Notice

U9016B OLT does not support IPv6 anycast address due to security issues.

The IPv6 has no broadcast address; the broadcast function is replaced with the multicast address. The anycast address shares the unicast address space, so it is not particularly distinguished from the unicast address space. The IPv6 address types are listed as follows.

Address type	Binary prefix	IPv6 notation
Unspecified	00...0 (128 bits)	::/128
Loopback	00...1 (128 bits)	::1/128
Multicast	11111111	FF00::/8
Link-local unicast	1111111010	FE80::/10
Site-local unicast	1111111011	FEC0::/10
Global unicast	(everything else)	

To assign an IPv6 address, execute the following commands in interface configuration mode.

Table 293. Assigning IPv6 Address

Command	Description
ipv6 enable	Enables IPv6 to the corresponding interface. Automatically creates a link-local address by using the MAC address-based modified EUI-64 interface ID.
no ipv6 enable	Disables IPv6 on the corresponding interface. Resets the link-local address which has been automatically created.
ipv6 address ipv6-address link-local	Assigns a link-local address to the corresponding interface to enable IPv6.
no ipv6 address ipv6-address	Resets the link-local address on the corresponding interface to

link-local	disable IPv6.
ipv6 address ipv6-prefix/prefix-length	Assigns a global address to the corresponding interface to enable IPv6. Automatically creates a link-local address by using the MAC address-based modified EUI-64 interface ID.
no ipv6 address ipv6-prefix/prefix-length	Resets a global address on the corresponding interface to disable IPv6. Resets the link-local address which has been automatically created.

The following example shows how to enable IPv6 by assigning a global address to an interface:

```

Router# configure terminal
Router (config)# interface vlan100
Router (config-if-Vlan100)# ipv6 address 3ffe:506::1/48
Router (config-if-Vlan100)# end
Router# show ipv6 interface
Vlan100 is up, line protocol is up
IPv6 is enabled, link-local address is fe80::207:70ff:fe92:6589
Global unicast address (es):
3ffe:506::1
Joined group address (es):
ff02::2
ff02::1:ff00:1
ff02::1:ff92:6589
ff02::1
MTU is 1500 bytes
ND DAD is enabled, number of DAD attempts: 1
ND advertised retransmit interval is 0 milliseconds
ND router advertisements are sent every 600 seconds
ND router advertisements live for 1800 seconds
Hosts use stateless autoconfig for addresses.
Router#

```

The following example shows how to create a link-local address automatically and enable IPv6 when the interface needs a link-local address only:

```

Router# configure terminal
Router (config)# interface vlan100
Router (config-if-Vlan100)# ipv6 enable
Router (config-if-Vlan100)# end
Router# show interface VLAN 100

Vlan100 is up, line protocol is up
Hardware is VLAN Current HW addr: 0007.7092.6589
Physical: (not set) Logical: (not set)
index 2100 (snmp index 2100) metric 1 mtu 1500 arp ageing timeout 600
<UP,BROADCAST,RUNNING,MULTICAST>
ARP proxy is disabled VRF Binding: Not bound

```

Bandwidth 1g

inet 100.1.1.100/24 broadcast 100.1.1.255

VRRP Master of : VRRP is not configured on this interface.

inet6 fe80::207:70ff:fe92:6589/64

ND router advertisements are sent every 600 seconds

ND next router advertisement due in 11 seconds.

ND router advertisements live for 1800 seconds

Hosts use stateless autoconfig for addresses.

0 packets input, 0 bytes

0 packets output, 0 bytes

Router#



Notice

For the official technical description for IPv6 address, refer to RFC2460, IPv6 Specification or RFC3513, IPv6 Addressing Architecture.

ND (Neighbor Discovery)

Neighbor Advertisement (ND) Overview

IPv6 Neighbor Advertisement (ND) uses ICMPv6 messages. To get the link-local addresses of other nodes on the same network, it uses the multicast address. A node with IPv6 enabled sends a query by using the neighbor solicitation message (ICMPv6 Type 135) over the local network. Other nodes which have received the neighbor solicitation message respond to the message with the neighbor advertisement message (ICMPv6 Type 136).

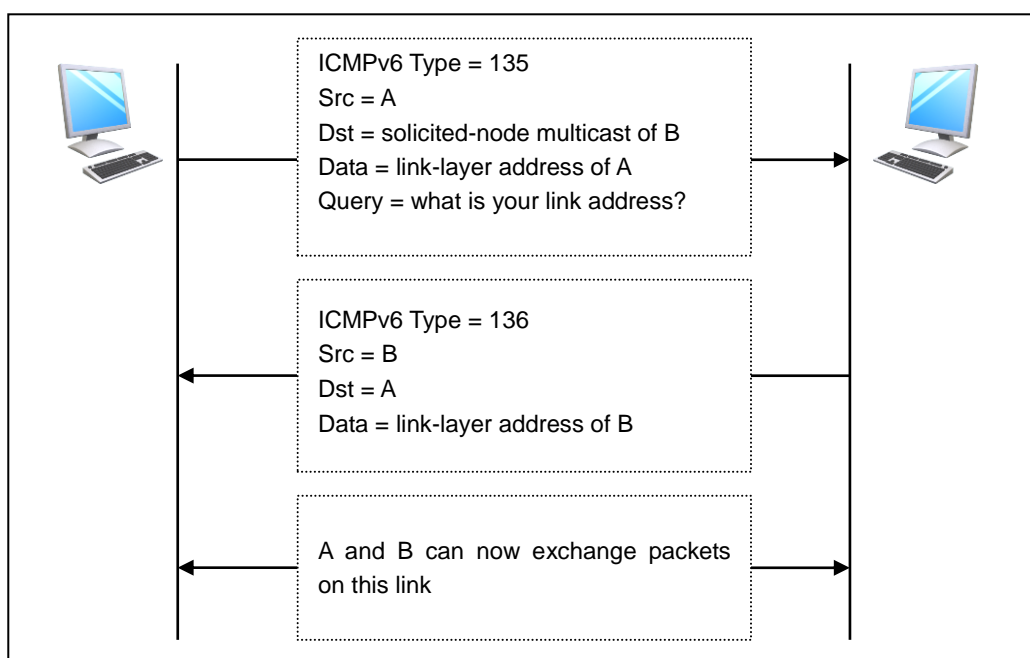


Figure 49 IPv6 Neighbor Solicitation-Neighbor Advertisement Message

Configure Neighbor Advertisement Functionality

Neighbor Solicitation Interval

To set the IPv6 neighbor solicitation interval, execute the following commands in interface configuration mode.

Table 294. Neighbor Solicitation Interval

Command	Description
ipv6 nd ns-interval <1000-3600000>	Sets the IPv6 neighbor solicitation interval to the corresponding interface.
no ipv6 nd ns-interval	Resets the IPv6 neighbor solicitation interval on the corresponding interface.

```
Router# configure terminal
Router (config)# interface vlan100
Router (config-if-Vlan100)# ipv6 nd ns-interval 10000
Router (config-if-Vlan100)# end
```

```
Router# show ipv6 interface
Vlan100 is up, line protocol is up
IPv6 is enabled, link-local address is fe80::207:70ff:fe92:6589
No global unicast address is configured
Joined group address (es):
    ff02::2
    ff02::1
    ff02::1:ff92:6589
MTU is 1500 bytes
ND DAD is enabled, number of DAD attempts: 1
ND advertised retransmit interval is 10000 milliseconds
ND router advertisements are sent every 600 seconds
ND router advertisements live for 1800 seconds
Hosts use stateless autoconfig for addresses.Router#
Router#
```

Neighbor Reachable Time

Neighbor reachable time detects unserviceable neighbors. When the setting value is smaller, the detection is made more quickly, however, it uses more IPv6 network bandwidth and IPv6 network device resources.

To set the IPv6 neighbor reachable time, execute the following commands in interface configuration mode:

Table 295. Neighbor Reachable Time

Command	Description
ipv6 nd reachable-time <0-3600000>	Sets the IPv6 neighbor reachable time to the interface.
no ipv6 nd reachable-time	Resets the IPv6 neighbor reachable time on the interface.

DAD

Duplicate Address Detection (DAD) detects any duplicate addresses to ensure the uniqueness of the IPv6 address created while processing autoconfiguration. Before assigning an IPv6 address created through autoconfiguration, DAD creates the multicast destination address by using the IPv6 address and then multicasts it across the local network. The interfaces receive the packet and compare the bit of the multicast destination address and the IPv6 address assigned to them. If the address is already being used, they respond to the sender through Neighbor Advertisement.

To set DAD, execute the following commands in interface configuration mode:

Table 296. DAD

Command	Description
ipv6 nd dad attempts <0-600>	Sets DAD to the corresponding interface..
no ipv6 nd dad attempts	Resets DAD on the corresponding interface.

```
Router# configure terminal
Router (config)# interface vlan100
Router (config-if-Vlan100)# ipv6 nd dad attempts 0
Router (config-if-Vlan100)# end
Router# show ipv6 interface
Vlan100 is up, line protocol is up
```

IPv6 is enabled, link-local address is fe80::207:70ff:fe92:6589
No global unicast address is configured
Joined group address (es):
 ff02::2
 ff02::1
 ff02::1:ff92:6589
MTU is 1500 bytes
ND DAD is disabled
ND advertised retransmit interval is 10000 milliseconds
ND router advertisements are sent every 600 seconds
ND router advertisements live for 1800 seconds
Hosts use stateless autoconfig for addresses.
Router#

Router Advertisement Overview

Each interface with enabled IPv6 periodically sends the router advertisement message (ICMPv6 Type 134). The destination of the router advertisement message is set as all-nodes multicast address (FF02::1). It consists of the following data: IPv6 prefix and flag required for host autoconfiguration, the lifetime for the IPv6 prefix, default router, hop limit, MTU, neighbor solicitation interval, and neighbor reachable time to be used by the host.

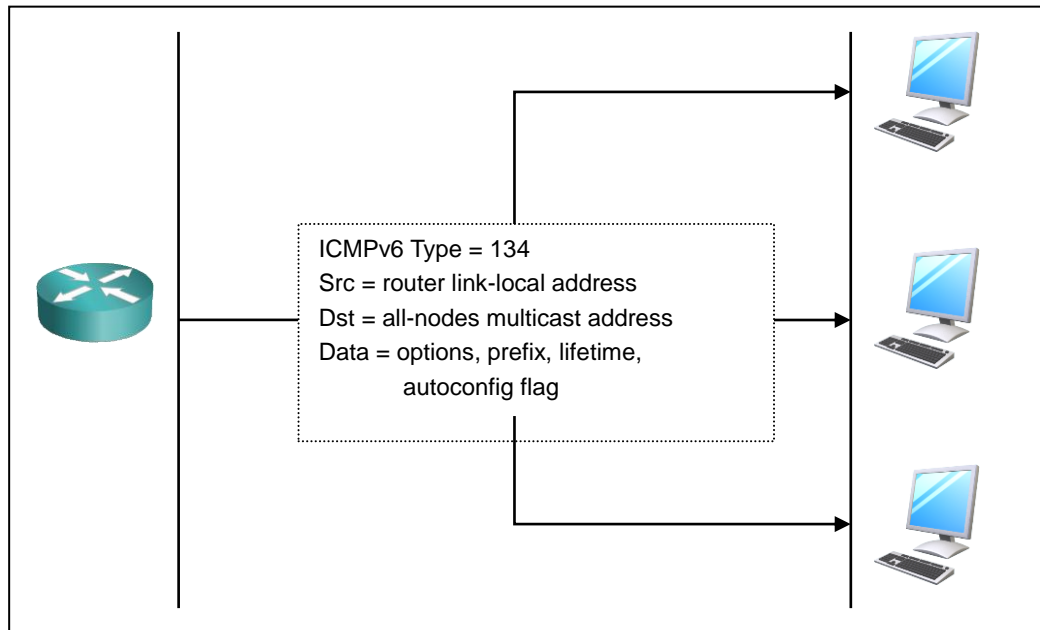


Figure 50 IPv6 Router Advertisement Message (Periodic)

The router advertisement message is sent to the host as a response to the router solicitation message (ICMPv6 Type 133). In short, the host sends the router solicitation message for immediate autoconfiguration, without waiting for the next scheduled router advertisement message. The source address of the router advertisement message is set to an unspecified IPv6 address (0:0:0:0:0:0:0) and the destination address is set to the all-routers multicast address (FF02::2).

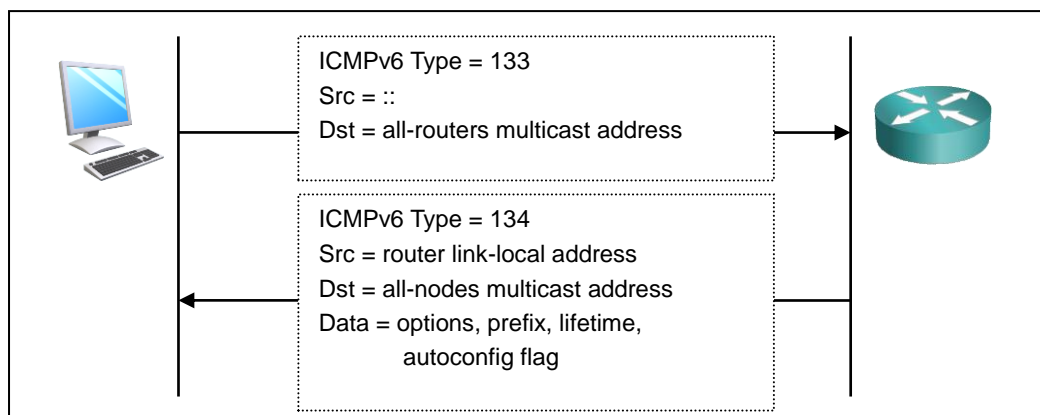


Figure 51 IPv6 Router Solicitation-Router Advertisement Message

Configure Router Advertisement Functionality

Router Advertisement Interval

To set the router advertisement interval, execute the following commands in interface configuration mode:

Table 297. Router Advertisement Interval

Command	Description
ipv6 nd ra-interval <3-1800>	Sets the router advertisement interval to the interface.
no ipv6 nd ra-interval	Resets the router advertisement interval on the interface.

```

Router# configure terminal
Router (config)# interface vlan100
Router (config-if-Vlan100)# ipv6 nd ra-interval 60
Router (config-if-Vlan100)# end
Router# show ipv6 interface
Vlan100 is up, line protocol is up
  IPv6 is enabled, link-local address is fe80::207:70ff:fe92:6589
  No global unicast address is configured
  Joined group address (es):
    ff02::2
    ff02::1
    ff02::1:ff92:6589
  MTU is 1500 bytes
  ND DAD is enabled, number of DAD attempts: 1
  ND advertised retransmit interval is 10000 milliseconds
ND router advertisements are sent every 60 seconds
  ND router advertisements live for 1800 seconds
  Hosts use stateless autoconfig for addresses.
Router#

```

Suppress Router Advertisement

To suppress the interface not to send the router advertisement message, execute the following commands in interface configuration mode:

Table 298. Suppress Router Advertisement

Command	Description
ipv6 nd suppress-ra	Suppresses the interface not to send router advertisement message.
no ipv6 nd suppress-ra	Resets suppress-ra on the corresponding interface.

```

Router# configure terminal
Router (config)# interface vlan100
Router (config-if-Vlan100)# ipv6 nd suppress-ra
Router (config-if-Vlan100)# end
Router#

```

Router Advertisement Lifetime

You can set the aging-time of the default router to be used by the host on the router lifetime field of the router advertisement message that the host will receive. To set the retransmission time, execute the following commands in interface configuration mode:

Table 299. Router Advertisement Lifetime

Command	Description
ipv6 nd ra-lifetime <0-9000>	Sets the router advertisement lifetime to the interface.
no ipv6 nd ra-interval	Resets the router advertisement lifetime on the interface.

```
Router# configure terminal
Router (config)# interface vlan100
Router (config-if-Vlan100)# ipv6 nd ra-lifetime 3000
Router (config-if-Vlan100)# end
Router# show ipv6 interface
Vlan100 is up, line protocol is up
  IPv6 is enabled, link-local address is fe80::207:70ff:fe92:6589
  No global unicast address is configured
  Joined group address (es):
    ff02::2
    ff02::1
    ff02::1:ff92:6589
  MTU is 1500 bytes
  ND DAD is enabled, number of DAD attempts: 1
  ND advertised retransmit interval is 10000 milliseconds
  ND router advertisements are sent every 600 seconds
  ND router advertisements live for 3000 seconds
  Hosts use stateless autoconfig for addresses.
Router#
```

Router Advertisement Prefix

You can set the IPv6 prefix of the global unicast, which the host will create through autoconfiguration, on the Prefix Information (NDP Options) field of the router advertisement message. To set the retransmission time, execute the following commands in interface configuration mode:

Table 300. Router Advertisement Prefix

Command	Description
ipv6 nd prefix ipv6-prefix/prefix-length	Sets the router advertisement prefix to the interface.
no ipv6 nd prefix ipv6-prefix/prefix-length	Resets the router advertisement prefix on the interface.

```
Router# configure terminal
Router (config)# interface vlan100
Router (config-if-Vlan100)# ipv6 nd prefix 3ffe::/64
Router (config-if-Vlan100)# end
Router#
```

Router Advertisement Current Hoplimit

You can set the hop limit, which the host will use, on the current hop limit field of the router advertisement message that the host will receive. To set the retransmission time, execute the following commands in interface configuration mode:

Table 301. Router Advertisement Current Hoplimit

Command	Description
ipv6 nd current-hoplimit <0-255>	Sets the router advertisement current-hoplimit to the interface.
no ipv6 nd current-hoplimit	Resets the router advertisement current-hoplimit on the interface.

```
Router# configure terminal
Router (config)# interface vlan100
Router (config-if-Vlan100)# ipv6 nd current-hoplimit 10
Router (config-if-Vlan100)# end
Router#
```

Router Advertisement Reachable Time

You can set the reachable time, which the host will use, on the reachable time field of the router advertisement message that the host will receive. To set the retransmission time, execute the following commands in interface configuration mode:

Table 302. Router Advertisement Reachable Time

Command	Description
ipv6 nd reachable-time <0-3600000>	Sets the router advertisement reachable time to the interface.
no ipv6 nd reachable-time	Resets the router advertisement reachable time on the interface.

```
Router# configure terminal
Router (config)# interface vlan100
Router (config-if-Vlan100)# ipv6 nd reachable-time 3000
Router (config-if-Vlan100)# end
Router#
```

Router Advertisement Retransmission Time

You can set the retransmission time, which the host will use, on the retransmission timer field of the router advertisement message that the host will receive. To set the retransmission time, execute the following commands in interface configuration mode:

Table 303. Router Advertisement Retransmission Time

Command	Description
ipv6 nd retransmission-time <0-3600000>	Sets the router advertisement retransmission time to the interface.
no ipv6 nd retransmission -time	Resets the router advertisement retransmission time on the interface.

```
Router# configure terminal
Router (config)# interface vlan100
Router (config-if-Vlan100)# ipv6 nd retransmission-time 1000
Router (config-if-Vlan100)# end
Router#
```


IPv6 Tools

Telnet

A system administrator can access U9016B OLT through the terminal which provides TCP/IP and Telnet access function. To use Telnet, the administrator should set the ID and password and the switch should have at least one IPv6 address.

When a Telnet connection is successfully made, a prompt asking for the user password appears. When the user enters the #Ttelnet user password, the mode is changed to *User Mode*.

The following example shows how to make a Telnet connection to U9016B OLT with the global unicast address (2001::1/64) set on the vlan100 interface via the terminal:

```
Switch# telnet 2001::1
Trying 2001::1...
Connected to 2001::1.
Escape character is '^J'.
```

Router login:



Notice

For the security to access the system or server, the some specific system can only use the SSH2 with the accessing way.
If the telnet does not work to connect the system, try SSH2 connection way.

Ping

The following example shows how to test for ping on the IPv6-enabled system on the local network under U9016B OLT *User*

```
Router#
Router# ping ipv6 fe80::207:70ff:feaa:172
Output Interface: vlan100
PING fe80::207:70ff:feaa:172 (fe80::207:70ff:feaa:172) from fe80::207:70ff:fe92:6589 vlan100: 56
data bytes
64 bytes from fe80::207:70ff:feaa:172: icmp_seq=1 ttl=64 time=63.2 ms
64 bytes from fe80::207:70ff:feaa:172: icmp_seq=2 ttl=64 time=64.2 ms
64 bytes from fe80::207:70ff:feaa:172: icmp_seq=3 ttl=64 time=65.1 ms
64 bytes from fe80::207:70ff:feaa:172: icmp_seq=4 ttl=64 time=66.1 ms
64 bytes from fe80::207:70ff:feaa:172: icmp_seq=5 ttl=64 time=67.0 ms

--- fe80::207:70ff:feaa:172 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3996ms
rtt min/avg/max/mdev = 63.263/65.166/67.091/1.381 ms

Router#
```

Chapter 20. MLD_Snooping

This chapter describes how to configure MLD snooping.

MLD Snooping Overview

Multicast traffic is processed as an unknown MAC address or broadcast frame, flooded to all ports included in the VLAN.

MLD snooping does not transmit IPv6 multicast traffic to all ports included in the VLAN; instead, it dynamically adds/deletes interfaces which will receive the multicast traffic, allowing efficient usage of the network bandwidth.

MLD snooping snoops MLD messages transmitted between an MLD host and a multicast router to collect the information on the multicast group and VLAN ports.

The MLD snooping is summarized as follows. When an MLD Join message for a specific multicast group is received, the switch adds the VLAN ports where the corresponding MLD host is connected to the multicast forwarding table entry. When the MLD host sends the MLD Done message to the switch, in reverse, the switch removes the VLAN ports where the corresponding MLD host is connected from the multicast forwarding table entry. In addition, the switch forwards the MLD queries received from the multicaster router to all ports of the VLAN and then removes multicast forwarding table entries which have not been updated by the MLD Join message.

Configuring MLD Snooping

Enable MLD Snooping on a VLAN

MLD snooping can be set for each VLAN. To set MLD snooping, execute the following commands in interface configuration mode:

Table 304 Enable MLD Snooping on a VLAN

Command	Description
ipv6 mld snooping	Enables MLD snooping on the VLAN.
no ipv6 mld snooping	Disables MLD snooping on the VLAN.

```

Router# configure terminal
Router (config)# interface vlan22
Router (config-if-Vlan22)# ipv6 enable
Router (config-if-Vlan22)# ipv6 mld snooping
Router (config-if-Vlan22)# end
Router# show ipv6 mld interface
Interface Vlan22 (Index 2022)
  MLD Enabled, Active, Non-Querier, Version 2 (default)
  Internet address is fe80::207:70ff:fe92:6589
  MLD interface has 0 group-record states
  MLD activity: 0 joins, 0 leaves
  MLD querying router is ::
  MLD query interval is 125 seconds
  MLD querier timeout is 262 seconds
  MLD max query response time is 25 seconds
  Last member query response interval is 1000 milliseconds
  Group Membership interval is 275 seconds
  MLD Snooping is enabled on this interface
  MLD Snooping fast-leave is not enabled
  MLD Snooping querier is not enabled
  MLD Snooping report suppression is enabled
.....
Router#

```

Configure MLD Snooping Functionality

To set various MLD snooping functions, perform the tasks listed below.

MLD Report-Suppression

When MLD snooping is enabled on a specific VLAN interface, MLD Report-suppression is enabled by default. Just on MLD Report is forwarded to the multicast router per MLD membership. When MLD Report-suppression is disabled, all received MLD Reports are forwarded to the multicast router.

To enable MLD Report-suppression, execute the following commands in interface configuration mode:

Table 305. MLD Report-Suppression

Command	Description
ipv6 mld snooping report-suppression	Enables MLD report-suppression on the VLAN interface.
no ipv6 mld snooping report-suppression	Disables MLD report-suppression on the VLAN interface.

```

Router# configure terminal
Router (config)# interface vlan22
Router (config-if-Vlan22)# no ipv6 mld snooping report-suppression
Router (config-if-Vlan22)# end
Router# show ipv6 mld snooping interface
Interface Vlan22 (Index 2022)
  MLD Enabled, Active, Non-Querier, Version 2 (default)
  Internet address is fe80::207:70ff:fe92:6589
  MLD interface has 0 group-record states
  MLD activity: 0 joins, 0 leaves
  MLD querying router is ::
  MLD query interval is 125 seconds
  MLD querier timeout is 262 seconds
  MLD max query response time is 25 seconds
  Last member query response interval is 1000 milliseconds
  Group Membership interval is 275 seconds
  MLD Snooping is enabled on this interface
  MLD Snooping fast-leave is not enabled
  MLD Snooping querier is not enabled
  MLD Snooping report suppression is disabled
.....
Router#

```

MLD Fast-Leave

When MLD fast-leave is enabled, the switch immediately removes the membership interface of the corresponding VLAN from the multicast forwarding table as soon as receiving the MLDv1 Done message from the host.

MLD fast-leave should be used only when each port of the VLAN interface has only one host. If this function is enabled for a port which has several hosts, hosts which have not sent the MLDv1 Done message may not receive traffic from a multicast group for extended periods of time.

Table 306. MLD Fast-Leave

Command	Description
ipv6 mld snooping fast-leave	Enables fast-leave on the VLAN.
no ipv6 mld snooping fast-leave	Disables fast-leave on the VLAN.

```

Router# configure terminal
Router (config)# interface vlan22
Router (config-if-Vlan22)# ipv6 mld snooping fast-leave
Router (config-if-Vlan22)# end
Router# show ipv6 mld snooping interface
Interface Vlan22 (Index 2022)
  MLD Enabled, Active, Non-Querier, Version 2 (default)
  Internet address is fe80::207:70ff:fe92:6589
  MLD interface has 0 group-record states
  MLD activity: 0 joins, 0 leaves
  MLD querying router is ::
  MLD query interval is 125 seconds
  MLD querier timeout is 262 seconds
  MLD max query response time is 25 seconds
  Last member query response interval is 1000 milliseconds
  Group Membership interval is 275 seconds
  MLD Snooping is enabled on this interface
MLD Snooping fast-leave is enabled
  MLD Snooping querier is not enabled
  MLD Snooping report suppression is enabled
.....
Router#

```

MLD Mrouter-Port

Multicast traffic and MLD messages received from all member ports, excluding the Mrouter port in the VLAN interface, must be forwarded to the multicast router. Therefore, the Mrouter port of the VLAN interface connected to the multicaster router is added to all multicast forwarding table entries as a traffic forwarding port.

In other words, MLD snooping detects an MLD message and the Mrouter port connected to the multicast router.

Whenever a new multicast forwarding table entry is created, the Mrouter port is always added as the traffic forwarding port, and the MLD messages sent from the MLD host are forwarded, as well as multicast traffic.

To configure a multicast router port statically, execute the following commands in interface configuration mode:

Table 307. MLD Mrouter-Port

Command	Description
ipv6 mld snooping mrouter interface IFNAME	Manually sets the Mrouter port on the VLAN. At this time, IFNAME should be a member port in the VLAN.
no ipv6 mld snooping mrouter interface IFNAME	Disables the Mrouter port on the VLAN.

```

Router# configure terminal
Router (config)# interface vlan22
Router (config-if-Vlan22)# ipv6 mld snooping mrouter interface Giga6/1
Router (config-if-Vlan22)# end
Router# show ipv6 mld snooping mrouter
VLAN      Interface
22        Giga6/1
Router#

```

MLD Access-Group

MLD snooping allows you to restrict a specific group of MLD hosts received on a specific interface.

To restrict a multicast group of MLD hosts, execute the following commands in interface configuration mode:

Table 308. MLD Access-Group

Command	Description
ipv6 mld snooping access-group <access-list>	Restricts a specific multicast group of MLD hosts received on the port.
no ipv6 mld snooping access-group <access-list>	Permits a specific group of MLD hosts received on the port.

```
Router# configure terminal
Router (config)# ipv6 access-list test permit ff05::e100:1
Router (config)# access-list 10 deny any
Router (config)# interface gi6/1
Router (config-if-Giga6/1)# ipv6 mld snooping access-group test
Router (config-if-Giga6/1)# end
Router#
```

To restrict a multicast group of MLD hosts on a specific VLAN interface when the interface is a member of several VLAN interfaces, execute the following commands in interface configuration mode:

Table 309. Ipv6 mld snooping access-group

Command	Description
ipv6 mld snooping access-group <access-list> VLAN <VLAN-id>	Restricts a specific multicast group of MLD hosts received on the port to a specific VLAN.
no ipv6 mld snooping access-group <access-list> VLAN <VLAN-id>	Permits a specific multicast group of MLD hosts received on the port to a specific VLAN.

```
Router# configure terminal
Router (config)# interface gi6/1
Router (config-if-Giga6/1)# ipv6 mld snooping limit 10 VLAN 22
Router (config-if-Giga6/1)# end
Router#
```

MLD Group-Limit

MLD snooping allows you to limit the number of multicast group by interface.

To limit the number of multicast group, execute the following commands in interface configuration mode:

Table 310. MLD Group-Limit

Command	Description
ipv6 mld snooping limit <count>	Limits the number of multicast groups received on the port.
ipv6 mld snooping limit <count> except <access-list>	Limits the number of multicast groups received on the port. Specifies the groups not to limit in access-list.
no ipv6 mld snooping limit <count>	Clears limit of the number of multicast groups received on the port.

```
Router# configure terminal
Router (config)# interface gi6/1
Router (config-if-Giga6/1)# ipv6 mld snooping limit 10
Router (config-if-Giga6/1)# end
Router#
```

To limit the number of multicast groups on a specific VLAN interface when the interface is a member of several VLAN interfaces, execute the following commands in interface configuration mode:

Table 311. ipv6 mld snooping limit

Command	Description
ipv6 mld snooping limit <count> VLAN <VLAN-id>	Limits the number of multicast groups received on the port to a specific VLAN.
ipv6 mld snooping limit <count> VLAN <VLAN-id> except <access-list>	Limits the number of multicast groups received on the port to a specific VLAN. Specifies the groups not to limit in access-list.
no ipv6 mld snooping limit <count> VLAN <VLAN-id>	Clears limit of the number of multicast groups received on the port to a specific VLAN.

```
Router# configure terminal
Router (config)# interface gi6/1
Router (config-if-Giga6/1)# ipv6 mld snooping limit 10 VLAN 22
Router (config-if-Giga6/1)# end
Router#
```

A limit to the number of multicast groups can be specified by VLAN interface. To specify the limit, execute the following commands in interface configuration mode:

Table 312. ipv6 mld limit

Command	Description
ipv6 mld limit <count>	Limits the number of multicast groups received on the VLAN.
ipv6 mld limit <count> except <access-list>	Limits the number of multicast groups received on the VLAN. Specifies the groups not to limit in access-list.
no ipv6 mld limit	Clears limit of the number of multicast groups received on the VLAN.


```
Router# configure terminal
Router (config)# interface vlan22
Router (config-if-Vlan22)# ipv6 mld limit 10
Router (config-if-Vlan22)# end
Router#
```

A limit of the number of multicast groups can be specified for all VLAN interfaces. To specify the limit, execute the following commands in configuration mode:

Table 313. Limit the number of all multicast groups

Command	Description
ipv6 mld limit <count>	Limits the number of all multicast groups.
ipv6 mld limit <count> except <access-list>	Limits the number of all multicast groups. Specifies the groups not to limit in access-list.
no ipv6 mld limit	Clears limit of the number of all multicast groups.

```
Router# configure terminal
Router (config)# ipv6 mld limit 10
Router (config)# end
Router#
```

MLD snooping forced-source-ip

MLD snooping allows you to specify the source address for MLD message sent to the Mrouter port while MLD snooping. This function can be used to specify the source address of a message to be sent to the Mrouter port when you have set a static group on a VLAN which has no given IP address.

Table 314. MLD snooping forced-source-ip

Command	Description
ipv6 mld snooping forced-source-ip <ip-address>	Specifies the source address of the leave message and the report of the VLAN.
no ipv6 mld snooping forced-source-ip	Clears the specified source address of the leave message and the report of the VLAN.

```
Router# configure terminal
Router (config)# interface vlan22
Router (config-if-Vlan22)#ipv6 mld snooping forced-source-ip ff05::e100:1
Router# end
```

MLD version

MLD snooping allows you to set the MLD version for each VLAN interface. When the mode is set to MLDv2, the system is compatible with the MLDv1 messages. However, when it is set to MLDv1, it drops the MLDv2 messages.

To set the MLD version, execute the following commands in interface configuration mode:

Table 315. MLD snooping version

Command	Description
ipv6 mld version <version>	Sets the MLD version on the VLAN interface.
no ipv6 mld version	Resets the MLD version on the VLAN interface to the default

	(MLDv2) value.
--	----------------

```
Router# configure terminal
Router (config)# interface vlan22
Router (config-if-Vlan22)#ipv6 mld version 1
Router# end
```

Configure MLD Static Group Functionality

MLD Static Group

For a specific multicast network, multicast traffic should be received even when there is no multicast membership.

In this case, set the VLAN interfaces of the network which should receive the multicast traffic as a static group to receive the multicast traffic from the specified VLAN. In addition, define the member-port of the VLAN while setting the static group to receive the multicast traffic on the specified port regardless of MLD Join.

The MLD static-group commands are executed under interface configuration mode. The following table describes the commands:

Table 316. MLD snooping version

Command	Description
ipv6 mld static-group <group-address>	Sets a static group in <group-address>.
ipv6 mld static-group <group-address> interface IFNAME	Sets a static group. The multicast traffic is forwarded to the specified interface.
no ipv6 mld static-group <group-address>	Resets the static group specified in <group-address>.
no ipv6 mld static-group <group-address> interface IFNAME	Resets the static group and the interface.

```
Router#configure terminal
Router (config)#interface vlan22
Router (config-if-Vlan22)#ipv6 mld static-group ff05::e100:1 interface Giga6/2
Router (config-if-Vlan22)#end
Router#show ipv6 mld groups
MLD Connected Group Membership
Group Address    Interface    Uptime    Expires    Last Reporter
ff05::e100:1     Giga6/2     00:00:03  static    ::
Router#
```

Display System and Network Statistics

The following table shows MLD snooping-related monitoring commands:

Table 317. MLD Snooping-related Monitoring Command

Command	Description
show ipv6 mld groups	Shows the MLD Join information.
show ipv6 mld interface	Shows the MLD snooping configuration.
show ipv6 mld interface summary	Shows the MLD snooping configuration by summarizing per VLAN.
show ipv6 mld snooping statistics	Shows the MLD snooping statistics.
show ipv6 mld snooping mrouter <IFNAME>	Shows the Mrouter port on the VLAN.
show ipv6 mld snooping table	Shows the list of hosts with MLD Join.

Chapter 21. RIP

This chapter introduces how to set up RIP (Routing Information Protocol). RIP has been used for many years and is still used for IGP (Interior Gateway Protocol) of small network.

Information about RIP

RIP is an interior gateway protocol that has been used for many years and is still used for small network environment. RIP is one of routing protocols that is a classical distance-vector.

RIP broadcasts User Datagram Protocol (UDP) data packets to exchange routing information. By default routing information is advertised every 30 seconds. If a switch cannot receive an update from another switch for more than 180 seconds, it will say that the router information is from an irrelevant switch. If the switch does not receive any update until 240 seconds, it will remove the whole entries.

The metric using in RIP is hop count. Hop count is number of router going through to router.

A connected network has metric value of 0 and Unreachable router has metric value of 16. Because it uses small metric scope like this, it does not suit with routing protocol for big network. The switch can receive or make default network via update from another system.

In this case, default network become advertisement via RIP and another RIP neighbor.

How to Configure RIP

The following commands should be completed for RIP configuration.

- Enabling RIP
- Allowing Unicast Updates for RIP
- Passive interface
- Applying Offsets to Routing Metrics
- Adjusting Timers
- Specifying a RIP version
- Applying Distnace
- Enabling Split Horizon

Enabling RIP

To enable RIP, do the following steps.

Table 318 Enabling RIP

Step	Command or Action	Purpose
Step 1	Configure terminal Example: Switch# configure terminal	Enters the Global configuration mode
Step 2	router rip Example: Switch(config)# router rip	Enter the RIP routing configuration mode
Step 3	network ip-address/prefix-len Example: Switch(config-router)# network 33.1.1.0/24	Assigns network for advertising to another router via RIP.
Step 4	End Example: Switch(config-router)# end	Enters the privileged EXEC mode

Allowing Unicast updates for RIP

To allow unicast updates for RIP, use the following command in the router configuration mode.

Table 319 Allowing Unicast updates for RIP

Command or Action	Purpose
neighbor ip-address Example: Switch(config-router)# neighbor 3.3.3.2	Defines switch for neighboring to exchange routing information.

Passive interface

To set passive interface, use the mmand in router configuration mode.

Table 320 Passive interface

Command or Action	Purpose
passive-interface IFNAME Example: Switch(config-router)# passive-interface gi2/1	Sets Passive interface

Applying Offsets to Routing metrics

Offset list is a mechanism to increase both incoming and outgoing metrics of RIP: it can be done by Access list and offset list. To increase the routing metric, use the following command in router configuration mode.

Table 321 Applying Offsets to Routing metrics

Command or Action	Purpose
offset-list <i>access-list-name {in out} metric IFNAME</i>	To apply offset on routing metric
Example: Switch (router-config)# offset-list aa in 5 gi2/1	

Adjusting Timers

Routing protocol uses various timers. Network administrator can manage the timer that changes the routing protocol performance to match for the network. You can make adjustments as follows:

- Routing table update timer (default 30 seconds)
- Routing information timeout timer (180seconds)
- Garbage collection timer (120 seconds)

To adjust time value, use the following command in router configuration mode

Table 322 Adjusting Timers

Command or Action	Purpose
timer basic <i>update invalid holddown</i>	Adjusts routing protocol timer
Example: Switch(config-router)# timer basic 30 120 120	

Specifying a RIP Version

To set to change a RIP version, use the following command in router configuration mode

Table 323 Specifying a RIP Version

Command or Action	Purpose
version {1 2}	Sets to change RIP version.
Example: Switch(config-router)# version 2	

To manage RIP version sent by a specific interface, use the following command in configuration mode of interface.

Table 324 Specifying a RIP Version

Command or Action	Purpose
-------------------	---------

ip rip send version VERSION Example: Switch(config-if-Giga2/1)# ip rip send version 1 Switch(config-if-Giga2/1)# ip rip send version 2 Switch(config-if-Giga2/1/1)# ip rip send version 1 2	Sets interface to receive only RIP packets that are relevant Note Both versions of 1 and 2 are supported when they are selected.
--	--

To control packet version by interface, use the following command in interface configuration mode.

Table 325 Specifying a RIP Version

Command or Action	Purpose
ip rip receive version VERSION Example: Switch(config-if-Giga2/1)# ip rip receive version 1 Switch(config-if-Giga2/1)# ip rip receive version 2 Switch(config-if-Giga2/1)# ip rip receive version 1 2	Sets interface to receive only RIP packets that are relevant Note. Both versions of 1 and 2 are supported when they are selected.

Applying Distance

Administrative distance represents the reliability of routing information source. In general, a large number means less reliability. The default of RIP is 120.

To adjust administrative distance value, use the following commands in router configuration mode.

Table 326 Applying Distance

Command or Action	Purpose
distance VALUE A.B.C.D/M Example: Switch(config-router)# distance 90 10.1.1.1/24	Changes the Administrative distance value.

Enabling Split Horizon

Distance-vector routing uses split horizon mechanism to lower the risk of routing loop.

Use the following commands to enable Split horizon in interface configuration mode.

Table 327 Enabling Split Horizon

Command or Action	Purpose
ip rip split-horizon [poisoned] Example: Switch(config-if-Giga2/1)# ip rip split-horizon poisoned	To enable Split horizon poisoned

Configuration Examples for RIP

RIP Construction

Let us investigate an example of RIP construction by looking at the Network Configuration in the following figure.

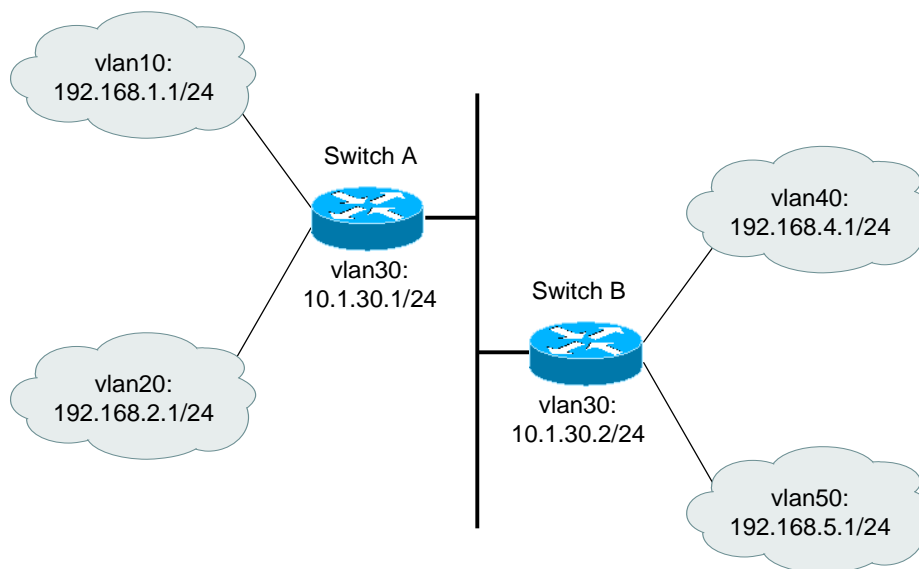


Figure 52. RIP Network Configuration Example and Diagram

Switch A	Switch B
vlan10 192.168.1.1/24 vlan20 192.168.2.1/24 vlan30 10.1.30.1/24	vlan30 10.1.30.2/24 vlan40 192.168.4.1/24 vlan50 192.168.5.1/24

To enable RIP protocol of each interface, use the following commands in the router configuration mode.

Switch A Configuration

```
Switch A(config)# router rip
Switch A(config-router)# network 192.168.1.1/24
Switch A(config-router)# network 192.168.2.1/24
Switch A(config-router)# network 10.1.30.1/24
Switch A(config-router)# end
Switch A# show ip route database
```

Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
 O - OSPF, IA - OSPF inter area
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
 E1 - OSPF external type 1, E2 - OSPF external type 2
 i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
 > - selected route, * - FIB route, p - stale info

```
C>* 10.1.30.0/24 is directly connected, vlan30
C>* 192.168.1.0/24 is directly connected, vlan10
C>* 192.168.2.0/24 is directly connected, vlan20
R> 192.168.4.0/24 [120/1] via 10.1.30.2, vlan30, 00:01:42
```

```
R>* 192.168.5.0/24 [120/1] via 10.1.30.2, vlan30, 00:01:42
Switch A#
```

Switch B Configuration

```
Switch B(config)# router rip
```

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

```
Switch B(config-router)# network 192.168.5.1/24
```

```
Switch B(config-router)# network 10.1.30.2/24
```

```
Switch B(config-router)# end
```

```
Switch B# show ip route database
```

```
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
```

```
O - OSPF, IA - OSPF inter area
```

```
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
```

```
E1 - OSPF external type 1, E2 - OSPF external type 2
```

```
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
```

```
> - selected route, * - FIB route, p - stale info
```

```
C>* 10.1.30.0/24 is directly connected, vlan30
```

```
R>* 192.168.1.0/24 [120/1] via 10.1.30.1, vlan30, 00:02:13
```

```
R>* 192.168.2.0/24 [120/1] via 10.1.30.1, vlan30, 00:02:13
```

```
C>* 192.168.4.0/24 is directly connected, vlan40
```

```
C>* 192.168.5.0/24 is directly connected, vlan50
```

```
Switch B#
```

Offset-list Setting

The following example shows how to increase the metric value of all incoming RIP route to Router A by 2 using the offset-list.

```
Switch A(config)# router rip
Switch A(config-router)# offset-list 4 in 2
Switch A(config-router)# exit
Switch A(config)# access-list 4 permit any
Switch A(config)# end
Switch A# show ip route database
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
        > - selected route, * - FIB route, p - stale info
C>* 10.1.30.0/24 is directly connected, vlan30
C>* 192.168.1.0/24 is directly connected, valn10
C>* 192.168.2.0/24 is directly connected, vlan20
R> 192.168.4.0/24 [120/3] via 10.1.30.2, vlan30, 00:06:26
R>* 192.168.5.0/24 [120/3] via 10.1.30.2, vlan30, 00:29:04
Switch A#
```

As shown above, the metric values of 192.168.4.0 and 192.168.5.0 have increased to 3. You can also set up outgoing setting as 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.

```
Switch A(config)# router rip
Switch A(config-router)# passive-interface vlan30
Switch A(config-router)# end
Switch A# show ip route database
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
        > - selected route, * - FIB route, p - stale info
C>* 10.1.30.0/24 is directly connected, vlan30
C>* 192.168.1.0/24 is directly connected, vlan10
C>* 192.168.2.0/24 is directly connected, vlan20
R> 192.168.4.0/24 [130/1] via 10.1.30.2, vlan30, 00:14:28
R>* 192.168.5.0/24 [120/1] via 10.1.30.2, vlan30, 00:37:06
Switch A#
Switch B# show ip route database
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
        > - selected route, * - FIB route, p - stale info
C>* 10.1.30.0/24 is directly connected, vlan30
C>* 192.168.4.0/24 is directly connected, vlan40
C>* 192.168.5.0/24 is directly connected, vlan50
Switch B#
```

Chapter 22. OSPF

This chapter introduces OSPF routing protocol used in U9016B. OSPF routing protocol is described in RFC 2328.

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 cost 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 328 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 type of router into the three categories as follows:

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 exchanges 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 not 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.

OSPF Configuration

To use OSPF Routing Protocol, you must enable OSPF. The following explains the procedure.

- Enter from config mode to ospf mode.
router ospf [process id]
- Specify the network to enable OSPF protocol and the area where OSPF protocol to be located.
network (ip address/M | ip address wildcard mask) area (area id | area address)

After enabling OSPF, use the following commands to manage protocol according to the requirements and needs.

OSPF interface parameters

You must set some OSPF parameters with the same value about all router in a network. These parameters can be set with **ip ospf hello-interval**, **ip ospf dead-interval**, **ip ospf authentication-key** command. When you change OSPF parameters, you must change all interface parameters of all router in a network.

To change interface parameters, use the following commands in interface configuration mode.

Table 329 OSPF interface parameter CLI

Command	Description
Router (config-if) # ip ospf cost cost	Sets the cost of packet sent by OSPF interface
Router (config-if) # ip ospf retransmit-interval seconds	Sets LSA retransmit-interval of OSPF interface
Router (config-if) # ip ospf transmit-delay seconds	Sets expected time of transmission sent by OSPF interface.
Router (config-if) # ip ospf priority number-value	Sets the priority used when selecting a OSPF designated router
Router (config-if) # ip ospf hello-interval seconds	Sets a interval of hello packet sent by OSPF interface
Router (config-if) # ip ospf dead-interval seconds	Sets OSPF dead-interval time.
Router (config-if) # ip ospf authentication-key key	Sets a password that will be used in network segment which uses OSPF simple password authentication
Router (config-if) # ip ospf message-digest-key key-id md5 key	Sets a key-id and key value that are used in OSPF MD5 authentication
Router (config-if) # ip ospf authentication {message-digest null}	Sets the Authentication type

Different Physical Networks

There are three default network types depending on different medium of OSPF.

- Broadcast networks (Ethernet, Token Ring, FDDI)
- Nonbroadcast multi-access(NBMA) networks (Switched Multimegabit Data Service(SMDS), Frame Relay, X.25)
- Point-to-Point networks (High-Level Data Link Control(HDLC), PPP)

OSPF Network type

You can set OSPF network with broadcast or NBMA regardless of Default media type. For example, you can set broadcast network like NBMA network or NBMA network with broadcast Network.

OSPF point-to-multipoint interface is defined with numbered point-to-point having more than one neighbor. OSPF point-to-multipoint network has the merit as follows:

- Point-to-multipoint does not need neighbor setting, be easy because it does not select DR.
- Reduce cost because it does not need Full meshed topology.
- More reliable because it maintains connection on VC (virtual circuit) failure.

To set OSPF network type, use the following commands in interface configuration mode.

Table 330 OSPF network type CLI

Command	Description
Router (config-if) # ip ospf network {broadcast non-bradcast {point-to-multipoint [non-broadcast] point-to-point}}	Sets OSPF network type of OSPF interface.

Point-to-Multipoint, Broadcast Networks

You need not to set neighbor setting on broadcast network. However, if you change cost as relevant neighbor, you can set with using **neighbor** command. OSPF Hello, LS Update, LS acknowledgment message is sent to multicast. Even if Cost sets with `ip ospf cost` command, you can each different cost with using neighbor command in case that the broadband differs per neighbor actually.

To configure point-to-multipoint and broadcast network, do the following steps.

Table 331 P-to-Multipoint Network, Broadcast Network Configuration

Step	Command	Description
Step 1	Router (config-if) # ip ospf network point-to-multipoint	Sets Interface as Point-to-multipoint broadcast network type.
Step 2	Router (config-if) # exit	Changes with Global configuration mode.
Step 3	Router (config) # router ospf process-id	Changes with Router configuration mode.
Step 4	Router (config-router) # neighbor ip-address cost number	Sets cost of specific neighbor.

Nonbroadcast Networks

You must select DR (designated router) because many routers in OSPF network may exist. If you do not set broadcast capability, need to set specific parameter for selecting DR.

You need to set this parameter only to have nonzero priority to become DR/BDR (backup DR) by itself.

To set router setting of Nonbroadcast networks, use the following command in the router configuration mode.

Table 332 Nonbroadcast network CLI

Command	Description
Router (config-router) # neighbor ip-address [priority number] [poll-interval seconds]	Connets router of Nonbroadcast network.

To indentfy neighbors form point-to-multipoint nonbroadcast network, use neighbor command in rotuer configuration mode.

To set the interface with point-to-multipoint to the system not applied broadcast, use the following commands with order.

Table 333 Nonbroadcast network Configuration

Step	Command	Description
Step 1	Router (config-if) # ip ospf network point-to-multipoint non-boradcast	Sets interface as Point-to-multipoint nonbroadcast network type.
Step 2	Router (config-if) # exit	Changes with Global configuration mode.
Step 3	Router (config) # router ospf process-id	Change with Router configuration mode.
Step 4	Router (config-router) # neighbor ip-address [cost number]	Sets cost of neighbor and neighbor.

OSPF Area parameters

OSPF has the possible setting area parameters. These are stub area setting, authentication setting, and the cost setting about default summary route. The authentication setting cuts area access of non-

authentication with setting password. Even if Stub area setting cuts access of external router, it sends default external route that ABR router creates to area. If you use **no-summary** keyword, cut summary route and reduce router number accessing to area.

To set OSPF area parameter, use the following command in the router configuration mode.

Table 334 OSPF area parameter CLI

Command	Description
Router (config-router) # area area-id authentication	Sets authentication to OSPF area.
Router (config-router) # area area-id authentication message-digest	Sets MD5 authentication to OSPF area.
Router (config-router) # area area-id stub	Sets Stub area.
Router (config-router) # area area-id default-cost cost	Set cost of default summary route for Stub area.

OSPF NSSA

NSSA extends OSPF function with setting between corporate router and remote router with stub area. The following figure shows OSPF Area 1 set with stub area. Because route redistribution is not allowed in Stub area, ISIS route can not be sent to OSPF routing domain.

Like the OSPF stub area, the NSSA area cannot allow flooding of the Type 5 LSAs. Route redistribution to the NSSA area is allowed for a special type of LSAs (Type 7 LSAs) only. The Type 7 LSAs should exist on the NSSA area only. NSSA autonomous system boundary router (ASBR) creates the Type 7 LSAs for route redistribution and NSSA area border router (ABR) converts the Type 7 LSAs to the Type 5 LSAs and floods them to all OSPF routing domains.

In the following figure, the OSPF Area 1 is set to the stub area. As the stub area does not allow route redistribution, the ISIS route cannot be sent to the OSPF routing domain.

But if you set OSPF Area 1 with NSSA, NSSA ASBR can flood ISIS route to OSPF NSSA after making Type 7 LSAs.

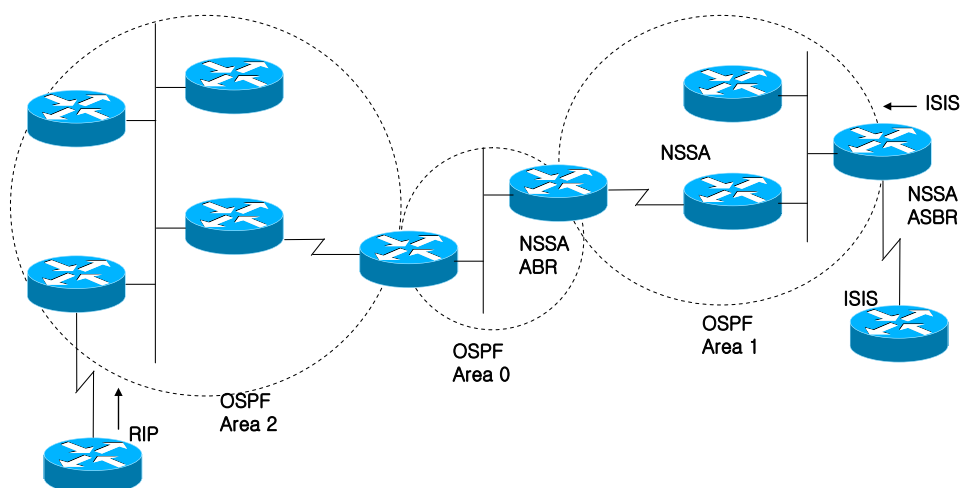


Figure 53. OSPF Network

Because NSSA is extension of stub area, Route redistributed from RIP does not income to OSPF Area 1. So It still maintains tendency of Stub area not incoming Type 5 LSAs.

To set OSPF NSSA, use the following command in router configuration mode.

Table 335 OSPF NSSA CLI

Command	Description
Router (config-router) # area area-id nssa [no-redistribution] [default-information-originate]	Sets NSSA.

OSPF Area Route Summarization

Route summarization is a function that summarizes the advertised routes. When this function is enabled, the ABR router advertises only one summarized route to the other area. In the OSPF, the ABR forwards the network in one area to another area. If one area has many networks, you can set the ABR router to advertise the summarized route (a route within a certain range) which includes each route in order to reduce the number of routes flooded.

To set summary address range, use the following command on router configuration mode.

Table 336 OSPF area router summarization CLI

Command	Description
Router (config-router) # area area-id range <i>ip-address mask</i> [advertise not-advertise] [cost cost]	Sets an address range for Summary route advertisement

Route Summarization of Redistributed Routes

When routes are redistributed from other routing protocol, each route is distributed to the Type 5 AS-External LSA. However, the routes can be summarized to one route that includes all routes redistributed by the summary-address command.

To summarize all redistributed routes with one route, use the following command in router configuration mode.

Table 337 External Router summarization CLI

Command	Description
Router (config-router) # summary-address { <i>ip-address/prefix</i> } [not-advertise] [tag tag]	Sets an address including redistributed routes sent to one route.

Virtual Links

In the OSPF, all areas should be linked to the backbone area. If the link to the backbone area is disconnected, you can set a virtual link. The two end terminals of the virtual link are the ABR routers and the virtual link should be set for both routers. In addition, the two routers should be in the same area (transit area) and no virtual link can be set in the stub area.

To set Virtual Link, use the following command in router configuration mode.

Table 338 OSPF virtual link CLI

Command	Description
Router (config-router) # area area-id virtual-link <i>router-id</i> [authentication [message-digest null]] [hello-interval seconds] [retransmit-interval seconds] [transmit-delay seconds] [dead-interval seconds] [[authentication-key key] [message-digest-key key-id md5 key]]	Sets Virtual link.

Generating a Default Router

The ASBR router can generate a default router with the OSPF routing domain. You can set the router as an ASBR router through router redistribution; however, essentially, the ASBR router does not generate a default router.

To generate a default router with ASBR, use the following command on router configuration mode.

Table 339 OSPF default route CLI

Command	Description
Router (config-router) # default-information originate [always] [metric <i>metric-value</i>] [metric-type <i>type-value</i>] [route-map <i>map-name</i>]	ASBR makes default route to OSPF routing domain

Router ID Choice with a Loopback Interface

The OSPF uses the largest value among the IP addresses configured to the interface as its router ID. If IP addresses are configured to the loopback interface, the IP address with the largest value among the loopback interfaces is used as the router ID even when an IP address with the largest value is configured in another interface.

To assign IP address in Loopback interface, use the following commands in the order.

Table 340 Loopback Interface Configuration

	Command	Description
Step 1	Router (config-if) # interface Loopback 0	Creates a Loopback interface
Step 2	Router (config-if) # ip address ip-address/prefix	Assigns a IP address to Interface

Default metric

The OSPF differentially calculates the OSPF metric according to the bandwidth of the interface. In the OSPF, the value calculated by dividing the reference-bandwidth by the interface bandwidth is used as the OSPF metric. The interface bandwidth can be changed by using the bandwidth command at the interface configuration mode.

To change reference-bandwidth, use the following command in router configuration mode.

Table 341 Reference bandwidth CLI

Command	Description
Router (config-router) # auto-cost reference-bandwidth ref-bw	Changes reference-bandwidth

OSPF administrative Distance

The administrative distance refers to the reliability of the routing information source, ranging from 0 to 255. Generally, a large value indicates a low reliability. If the administrative distance value is 255, it means that the routing information source is not reliable and the corresponding route is ignored.

The OSPF uses three administrative distances (intra-area, inter-area, and external) and the default value of each one is 110.

To change OSPF distance, use the following commands in router configuration mode.

Table 342 OSPF distance CLI

Command	Description
Router (config-router) # distance ospf {[intea-area <i>dist1</i>] [inter-area <i>dist2</i>] [external <i>dist3</i>]}	Changes OSPF distance

Passive interface

The passive-interface command limits sending the hello message to a specific interface, but allows the receipt of a message by the interface.

To set passive interface, use the following command in router configuration mode.

Table 343 OSPF passive interface CLI

Command	Description
Router (config-router) # passive-interface <i>interface-name</i>	Restricts hello packets that transmitting through interface.

Route Calculation Timers

The OSPF calculates the shortest path first (SPF) whenever the network configuration is changed. To prevent frequent SPF calculation, you can set the delay time between the time that the configuration change starts and the time that the SPF calculation starts.

To set SPF delay time, use the following command in router configuration mode.

Table 344 OSPF SPF timer CLI

Command	Description
Router (config-router) # timers throttle spf <i>spf-start spf-hold spf-max-wait</i>	Changes the calculation time of SPF

Logging Neighbors Going Up/Down

The OSPF generates a system message for a neighbor up/down event. If you want to generate a detailed system message for the changed neighbor status, use the detail keyword.

To make system message about neighbor Up/Down, use the following command.

Table 345 OSPF adjacency LOG CLI

Command	Description
Router (config-router) # log-adjacency-changes [detail]	Makes system message about OSPF neighbor UP/Down

Blocking LSA Flooding

When OSPF receives new LSA, OSPF floods LSA to interface excepting the received interface. But this running may make bandwidth waste and CPU overload. If you use database-filter command, you can block LSA flooding to specific interface.

To block OSPF LSA flooding from Broadcast, non-broadcast, and point-to-point, use the following command.

Table 346 Block LSA CLI

Command	Description
Router (config-router) # ip ospf database-filter all out	Restricts LSA flooding of interface

Ignoring MOSPF LSA Packets

Because the system does not support LSA Type 6 Multicast OSPF (MOSPF), the system makes system message when receiving LSA. If receive many MOSPF LSA, the system makes many system message. If the system does not make system message, use this function.

To ignore MOSPF LSA Packets, use the following command.

Table 347 Ignore MOSPF LSA CLI

Command	Description
Router (config-router) # ignore lsa mospf	When the system receives MOSPF LSA packet, ignores it.

Monitoring and Maintaining OSPF

You can show the information about OSPF routing table, database, and connection status of neighbour router. This information can be used about solving the network trouble or resource management of switch.

To search information on OSPF, use the following commands in EXEC mode.

Table 348 Monitoring OSPF CLI

Command	Description
Router # show ip ospf [process-id]	Shows OSPF routing process information
Router # show ip ospf border-routers	Shows all routing tables of ABR/ASBR
Router # show ip ospf [process-id] database	Shows OSPF database
Router # show ip ospf [process-id] database [database-summary]	
Router # show ip ospf [process-id] database [router] [self-originate]	
Router # show ip ospf [process-id] database [router] [adv-router [ip-address]]	
Router # show ip ospf [process-id] database [router] [link-state-id]	
Router # show ip ospf [process-id] database [network] [link-state-id]	
Router # show ip ospf [process-id] database [summary] [link-state-id]	
Router # show ip ospf [process-id] database [asbr-summary] [link-state-id]	
Router # show ip ospf [process-id] database [external] [link-state-id]	
Router # show ip ospf [process-id] database [nssa-external] [link-state-id]	
Router # show ip ospf [process-id] database [opaque-link] [link-state-id]	
Router # show ip ospf [process-id] database [opaque-area] [link-state-id]	
Router # show ip ospf [process-id]	

database [opaque-as] [link-state-id]	
Router # show ip ospf flood-list [interface-name]	Shows all LSAs that will be Flooding
Router # show ip ospf interface [interface-name]	Shows OSPF interface information
Router # show ip ospf neighbor [neighbor-id] [detail]	Shows OSPF neighbor information
Router # show ip ospf [process-id] summary-address	Shows all summary address information on Redistribution
show ip ospf [process-id] traffic	Shows OSPF traffic statistics
show ip ospf [process-id] virtual-links	Shows OSPF virtual link information

Use the following command in EXEC mode to restart OSPF process.

Table 349 Maintaining OSPF CLI

Command	Description
Router # clear ip ospf [process-id] {process redistribution counters traffic}	Restarts OSPF process/counters/redistribution/traffic

Chapter 23. BGP

This chapter introduces BGP among available IP Unicast routing protocols of U9016B.

BGP Overview

BGP is a protocol that receives/sends routing information among Management Domains (Autonomous System: AS), and manages routing between domains unlike RIP and OSPF. U9016B support BGP-4.

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. Enter BGP router configuration mode.
router bgp <14294967295>

The last number in the AS number, which 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
3. Designate network informed via BGP.

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 such 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. Other functions

BGP Filtering

BGP update sending/receiving can be managed by filtering functions such as route filtering, path filtering, and community filtering. Even though the functions have the 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}
--

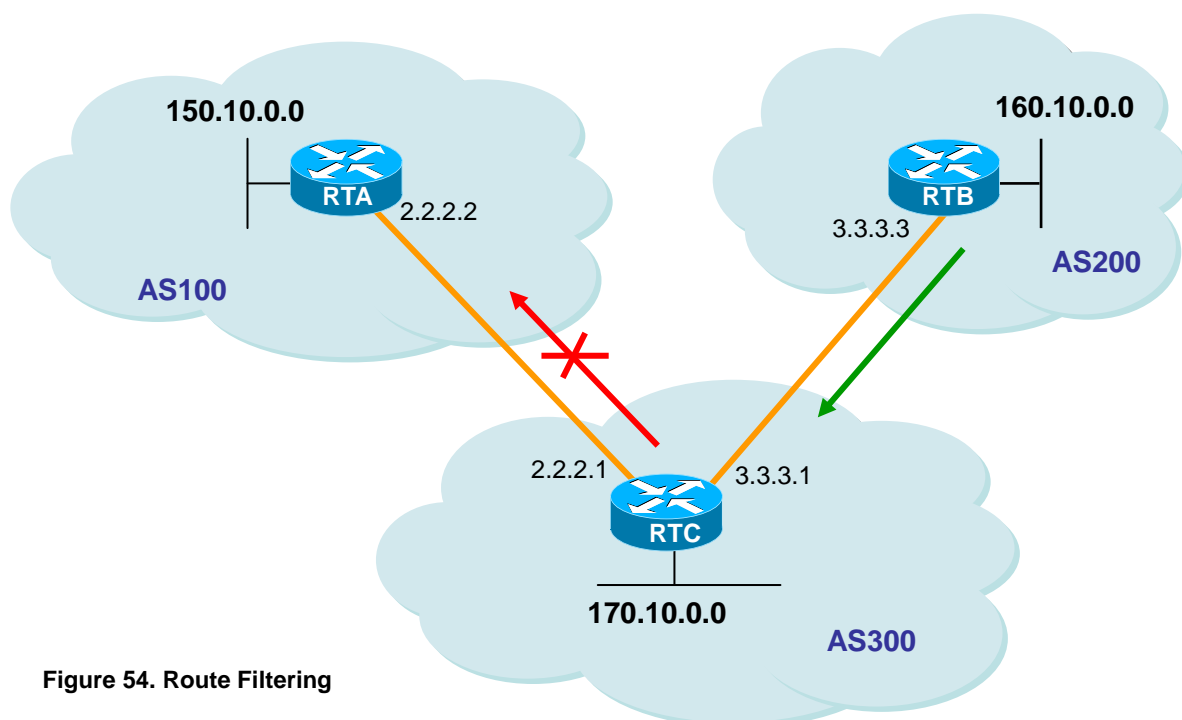


Figure 54. Route Filtering

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.

The following shows the construction of the operation.

```

/*-- 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}
```

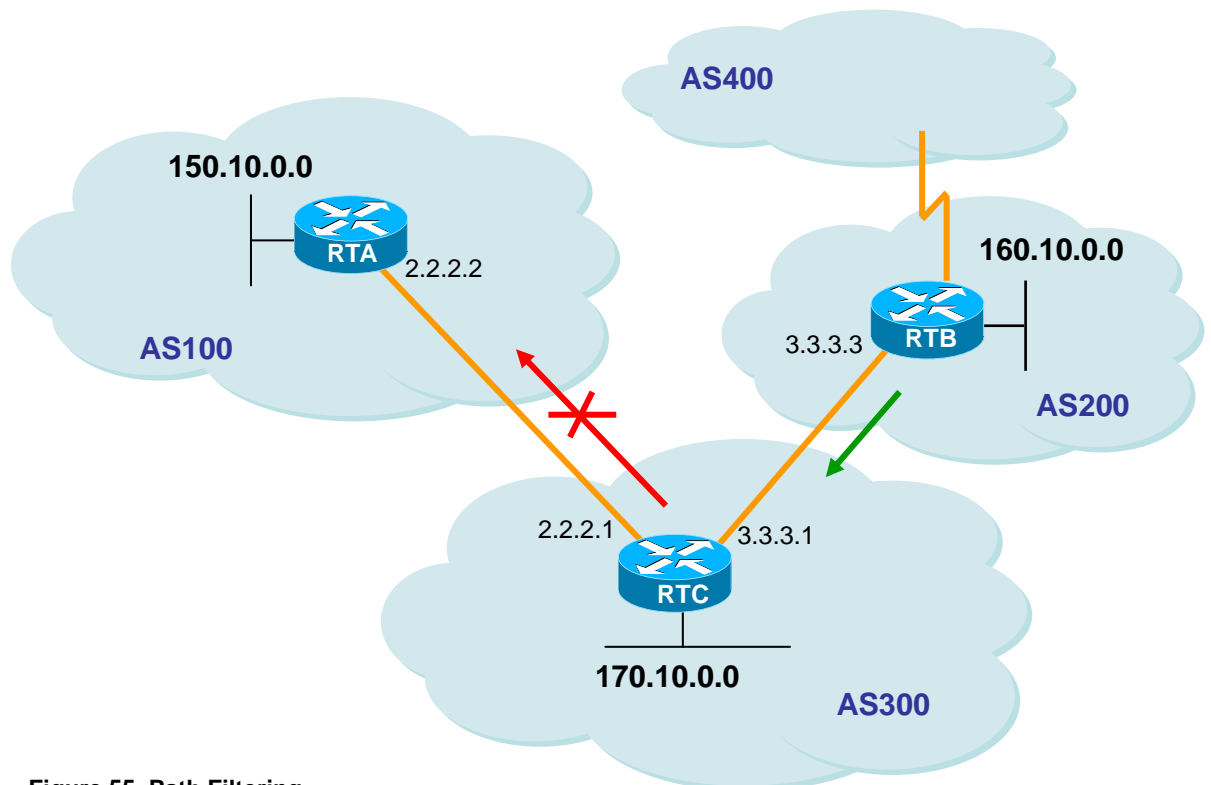


Figure 55. Path Filtering

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 community attribute is a way to group destinations into communities and apply routing decisions based on the communities

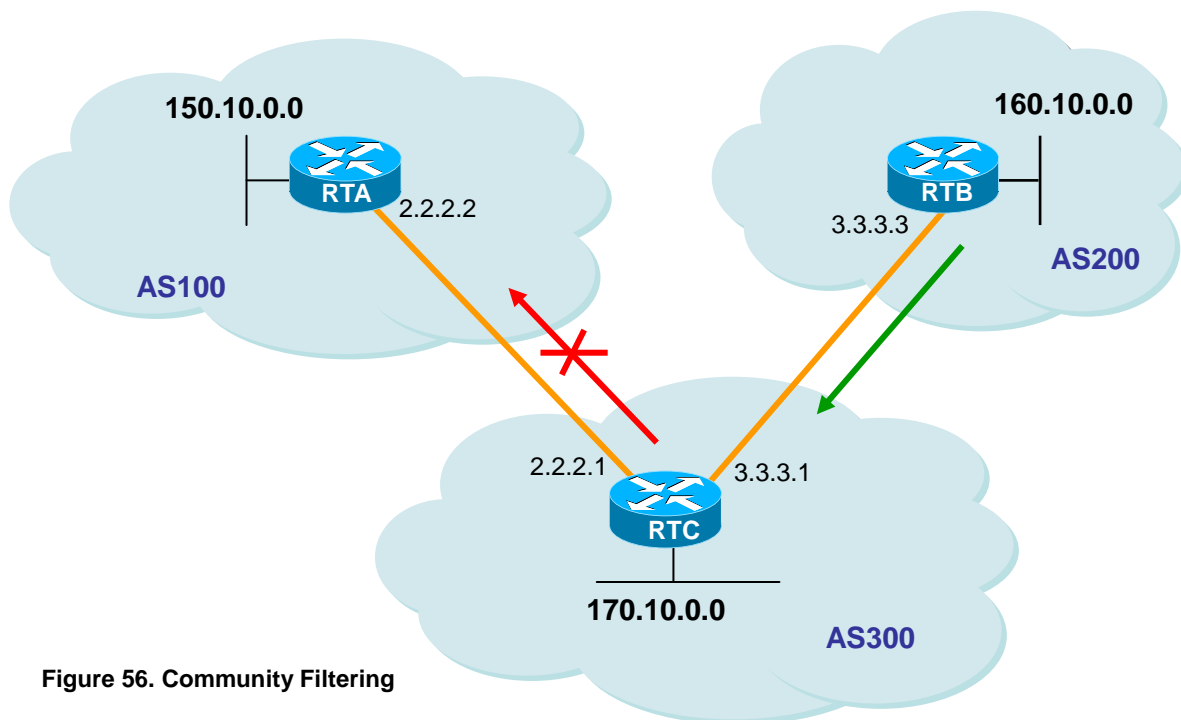


Figure 56. Community Filtering

As in the figure above, RTB sets Community attribute not to update routes from RTB to its dBGP Peer with 'no-export' community 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 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 receives an update with no-export attribute.

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 transmitting to RTC, or replacing the current community value with the value 100 200 when no additive 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 a route not matched is dropped to the default. The keyword “internet” is all routes because this 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

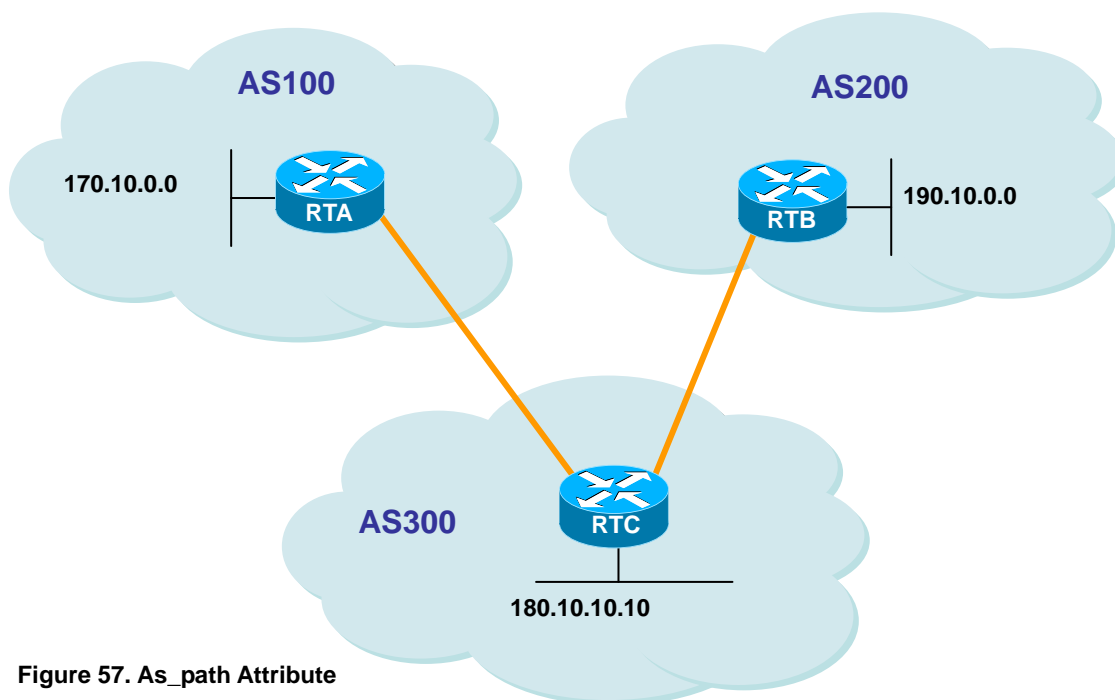


Figure 57. As_path Attribute

When one route passes one AS, the AS number is added to the update of route.

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). The same applies to 170.10.0.0 and 180.10.0.0. RTB should pass AS300 and AS100 to reach 170.0.0. RTC should pass AS200 to reach 190.0.0, and AS100 to reach 170.10.0.0.

Origin Attribute

This is an attribute to define Pass Information Source and there are three mechanisms.

- **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 unknown or got through the miscellaneous ways. This is used when the static route is redistributed to BGP and displayed "?" in the BGP table.

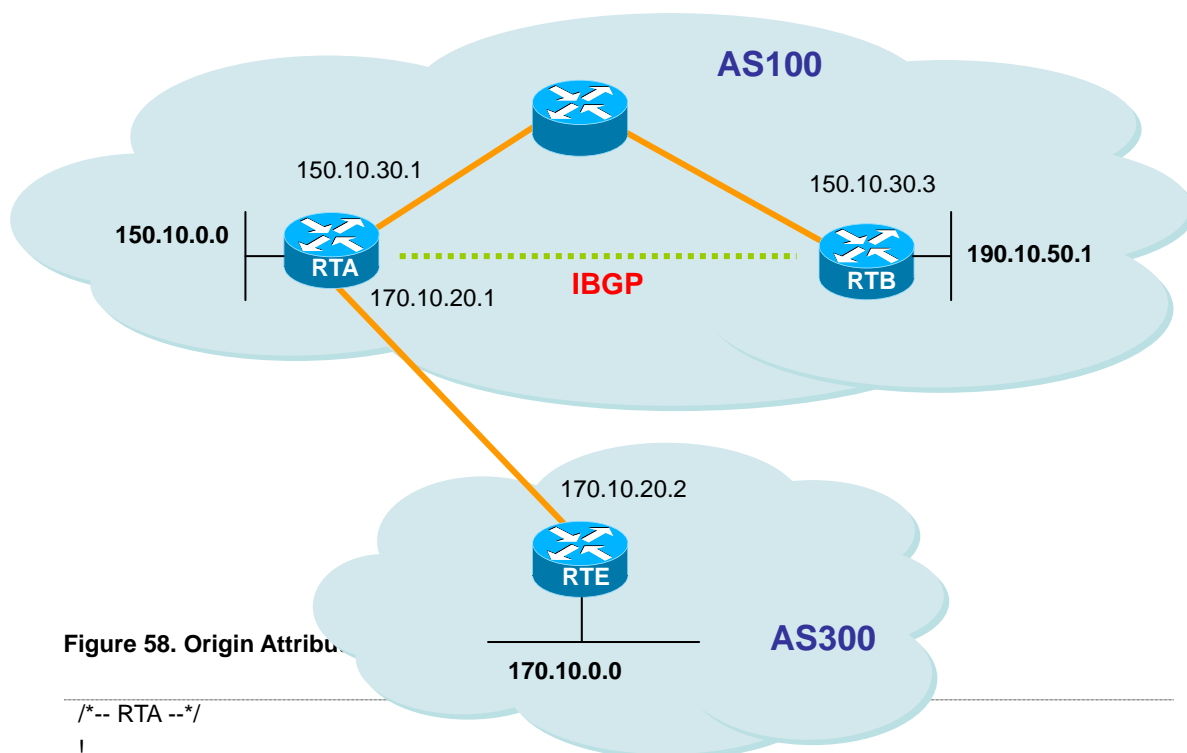


Figure 58. Origin Attribution

```

/*-- RTA --*/
!
router bgp 100
network 150.10.0.0
redistribute static
neighbor 150.10.30.3 remote-as 100
neighbor 170.10.20.2 remote-as 300
!
ip route 190.10.0.0/24 null
!

/*-- RTB --*/
!
router bgp 100
network 190.10.50.0
neighbor 150.10.30.1 remote-as 100
!

/*-- RTE --*/
!
router bgp 300
network 170.10.0.0
neighbor 170.10.20.1 remote-as 100
!

```

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 the route origin is Incomplete.)

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 should 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.

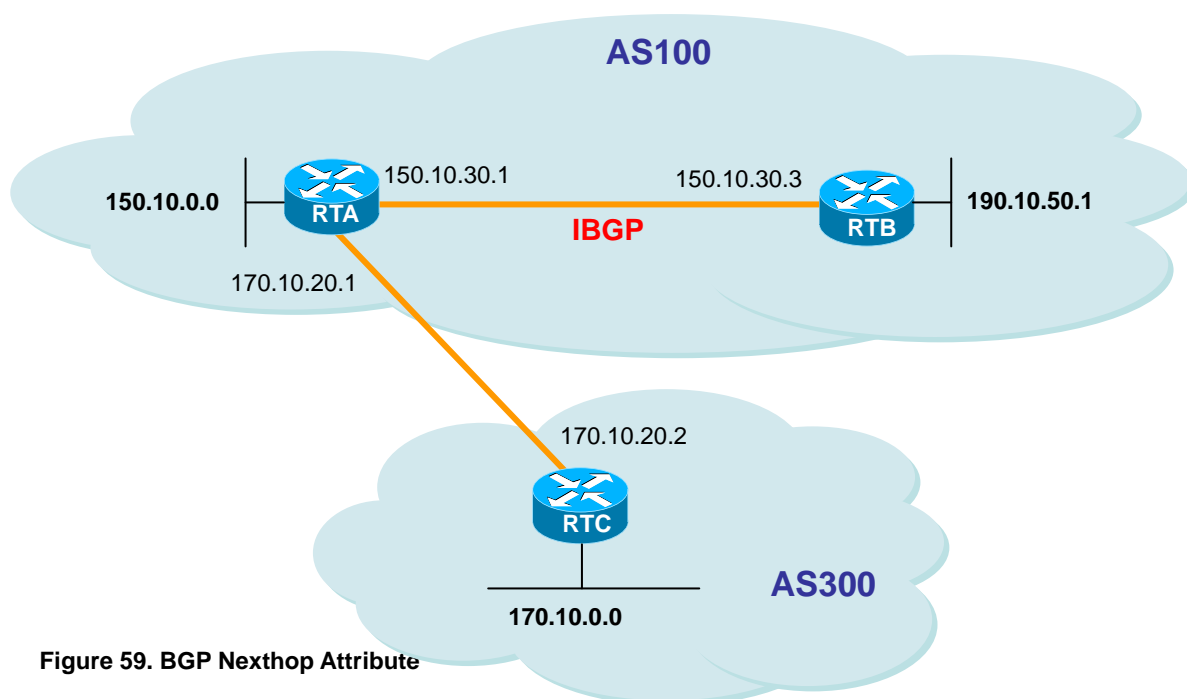


Figure 59. BGP Nexthop Attribute

```

/*-- RTA --*/
!
router bgp 100
network 150.10.0.0
neighbor 170.10.20.2 remote-as 300
neighbor 150.10.30.3 remote-as 100
!

/*-- RTB --*/
!
router bgp 100
neighbor 150.10.30.1 remote-as 100
!

/*-- RTC --*/
!
router bgp 300
network 170.10.0.0

```

```
neighbor 170.10.20.1 remote-as 100
```

When RTC transmits 170.10.0.0 to RTA, the nexthop turns into 170.10.20.2.

When RTA transmits 170.10.0.0 to RTB, the nexthop turns into 170.10.20.2.

The following shows you should be careful in the multi access network and NBMA network.

BGP Nexthop (Multiple access networks)

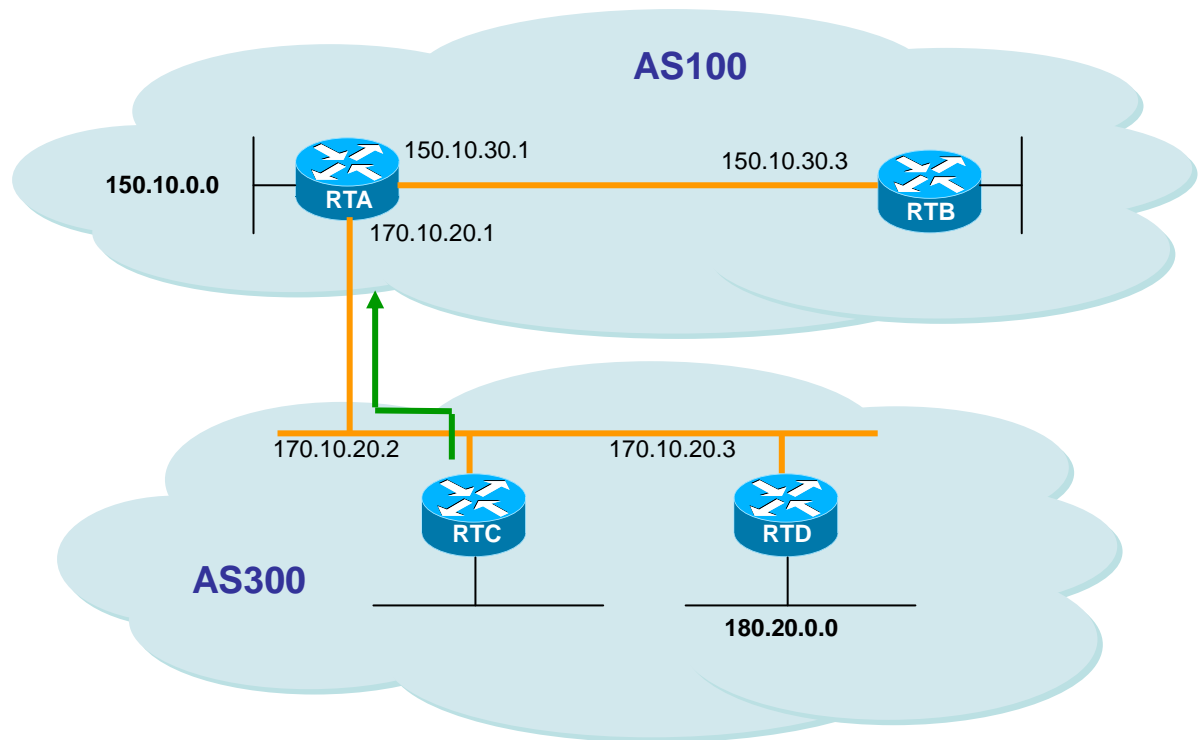


Figure 60. BGP Nexthop (Multiple access networks)

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.

BGP Nexthop (NBMA)

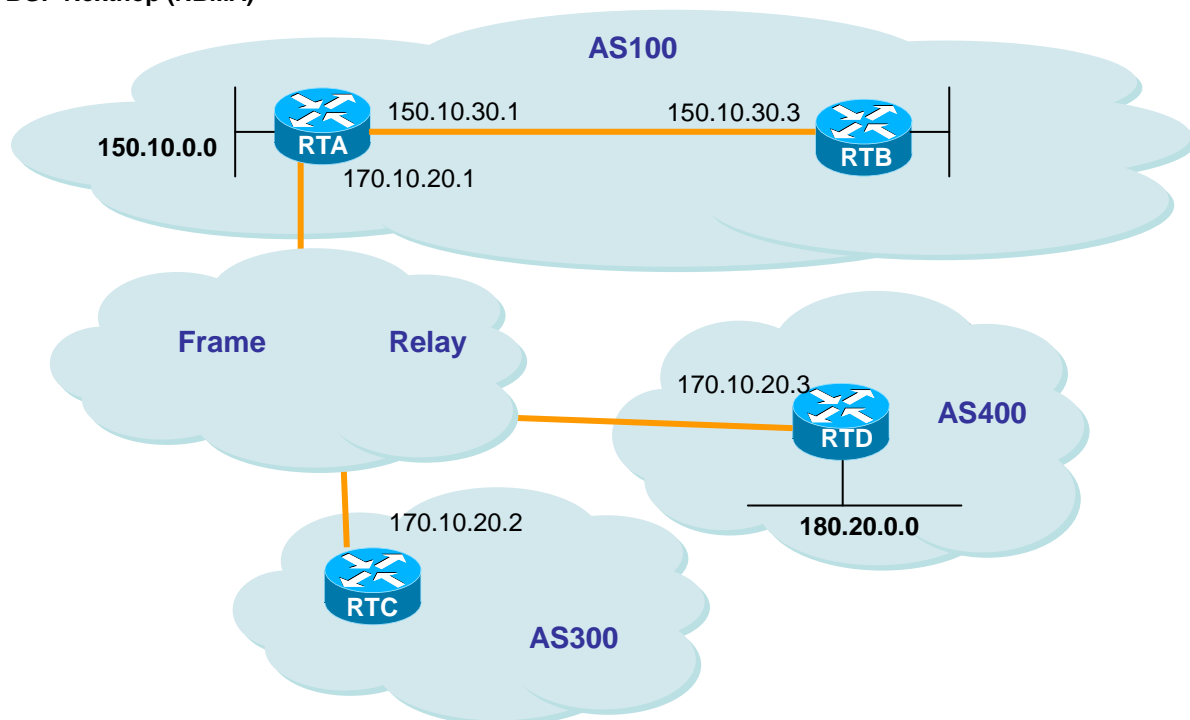


Figure 61. BGP Nexthop (NBMA)

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 kind of situation the Next-hop-self command was created

Next-hop-self

With the next-hop-self 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 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 local 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 weight 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.

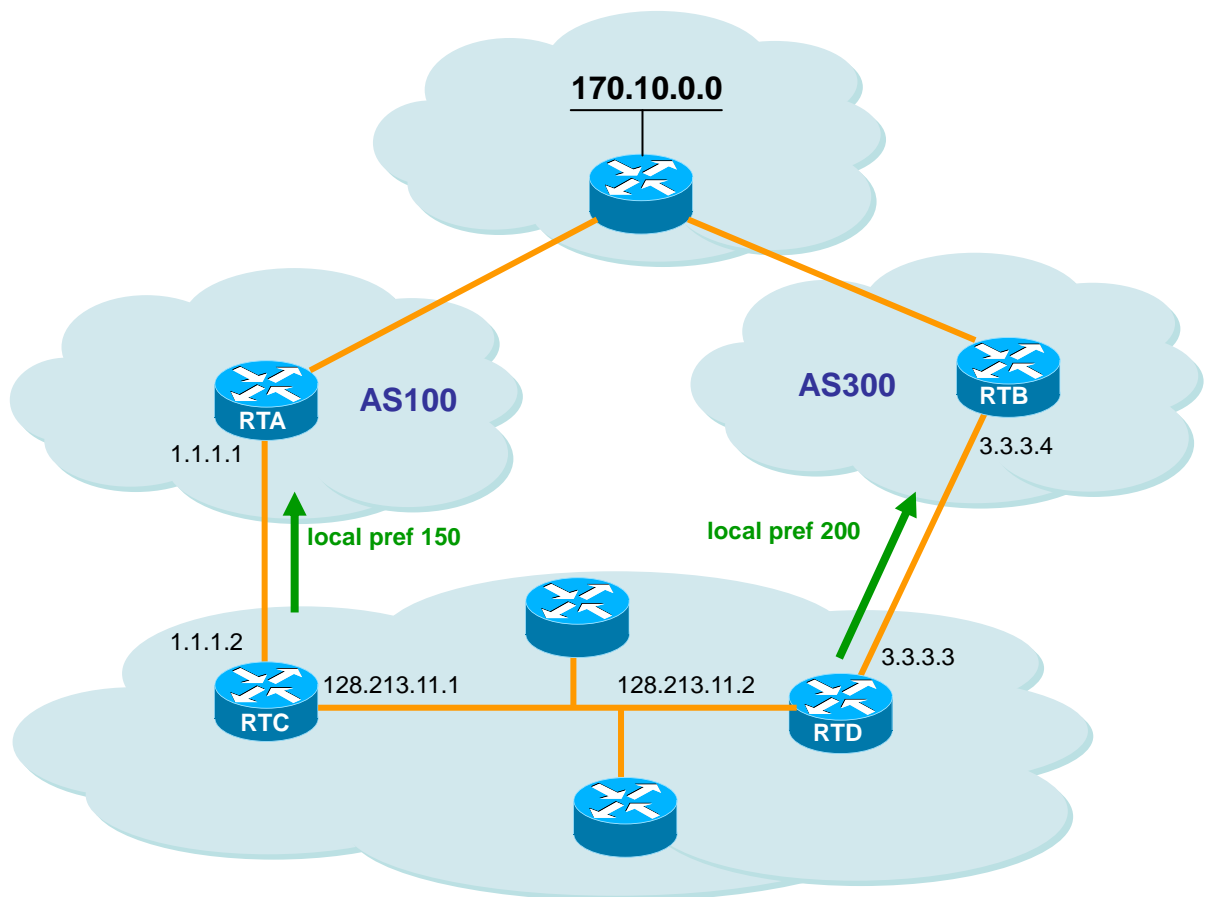


Figure 62. Local Preference Attribute

```

/*-- RTC --*/
!
router bgp 256
  bgp default local-preference 150
  neighbor 1.1.1.1 remote-as 100
  neighbor 128.213.11.2 remote-as 256
!

/*-- RTD --*/
!
router bgp 256
  bgp default local-preference 200
  neighbor 3.3.3.4 remote-as 300
  neighbor 128.213.11.1 remote-as 256
!

```


RTC sets the local preference of all update as 150 and RTD as 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.

However, using route map provides flexibility. In the example above, all updates that RTD receives are set for local preference 200. This can be inappropriate. As you can see in the box below, a specific update uses the route map only when setting as specific local preference.

```

/*-- 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 preference 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 configuration command "bgp always-compare-med" to compare metric from neighbor in different AS.

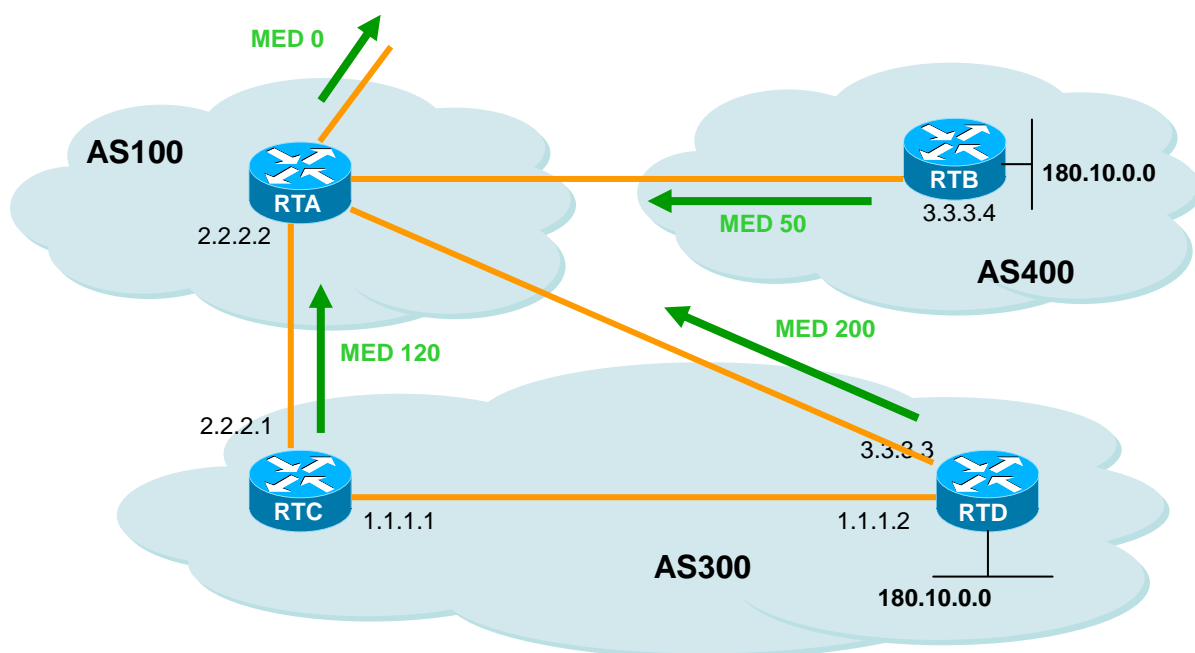


Figure 63. Metric Attribute

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.

Suppose that 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 ASs (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
!
/*-- 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
!

/*-- 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
!

```

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
bgp always-compare-med
neighbor 2.2.2.1 remote-as 300
neighbor 3.3.3.3 remote-as 300
neighbor 4.4.4.3 remote-as 400
!

```

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 attribute, 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
- route-map setcommunity
- match as-path 1
- set community 200 additive

If additive keyword is set, the value 200 replaces the current community value, and if additive keyword is not 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 needed.

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.

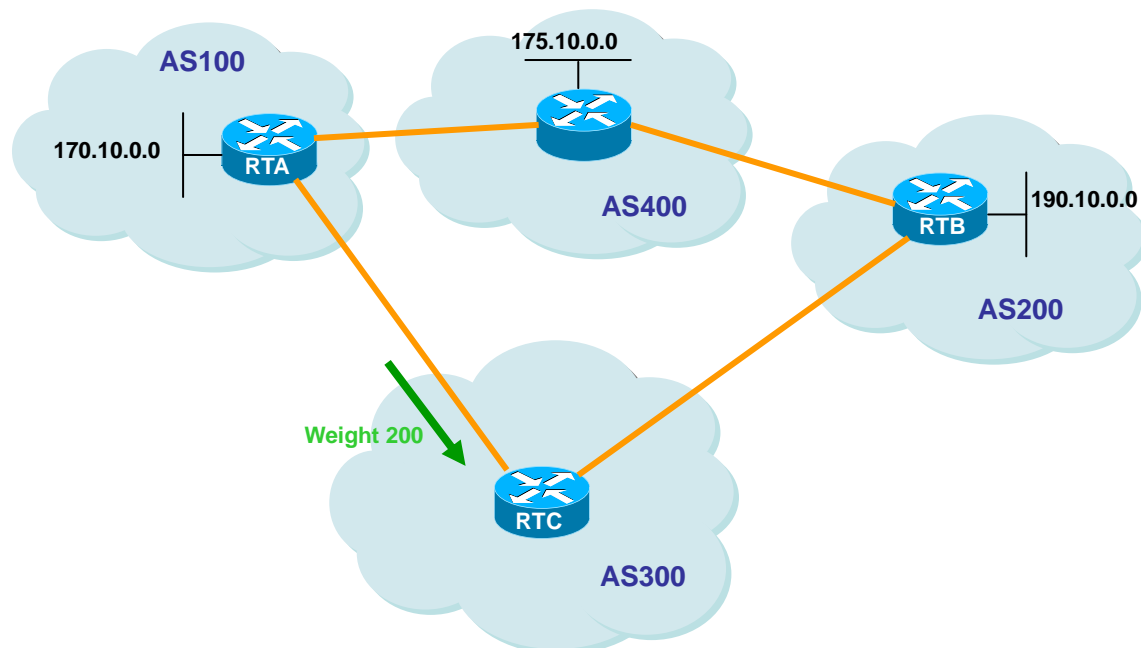


Figure 64. Weight Attribute

RTA and RTB get the information of network 175.10.0.0 from AS4 and transmits 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 next hop. This can be done by several methods:

- 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

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
!
```

IP as-path and 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$
!
```

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 "Inbound reset". The following shows the advantages of routing reset.

- Needless additional operation setting of operator
- Needless additional memory for routing 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 routers, 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 create 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]
```

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

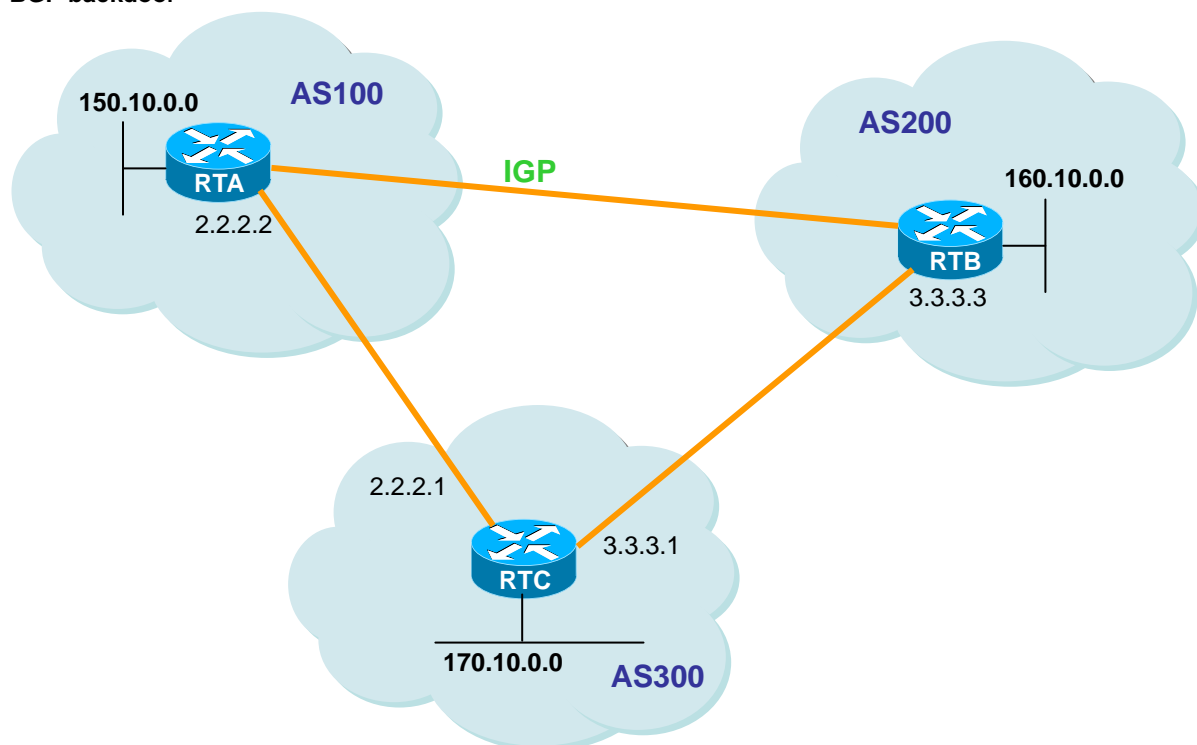


Figure 65. BGP backdoor

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. 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 recommended)
- 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 chosen due to backdoor command.

BGP Multipath

The BGP Multipath allows several BGP paths for the same destination. These paths are set on the routing table with the best path for load sharing. The BGP Multipath has no impact on the selection of the best path. For example, a router specifies one path among multi paths as its best path. It then advertises the best path to its neighbors.

To be a candidate of the multi paths, the paths with the same destination should have the following conditions same with the best path:

- Weight
- Local preference
- AS-PATH length
- Origin
- MED

One of these:

- Neighboring AS or sub-AS (before the addition of the eBGP Multipath feature)
- AS-PATH (after the addition of the eBGP Multipath feature)

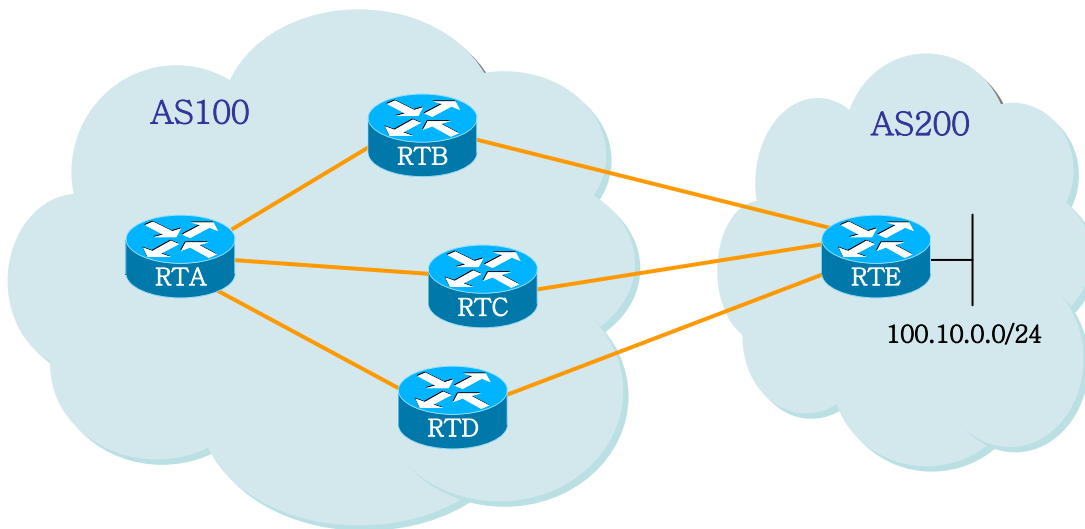
Some characteristics of BGP multipath have the additional requirements for the candidates of multipath.

The following details the requirements of the eBGP multipath.

- The path should be learned from the external or confederation-external neighbor.
- The IGP metric for the BGP nexthop should be identical with the IGP metric of the best path.

The following details the requirements of the iBGP multipath.

- The path should be learned from the internal neighbor.
- The IGP metric for the BGP nexthop should be identical with the IGP metric of the best path.



In the above figure, the RTA receives the network 100.1.1.0/24 from RTB, RTC, and RTD. The multipath function for a router is disabled by default. Therefore, use the following command to use the multipath function.

Maximum path [ibgp] number

To use Multipath function, set the following commands to RTA.

```

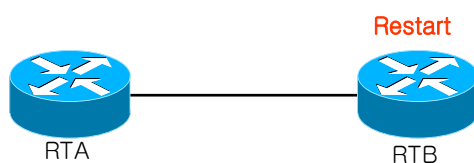
/*-- RTA --*/
!
router bgp 100
maximum-paths ibgp 3
neighbor 10.1.1.1 remote-as 200 /* RTB */
neighbor 20.1.1.1 remote-as 200 /* RTC */
neighbor 30.1.1.1 remote-as 200 /* RTD */
!

```

BGP graceful-restart

Generally, when the BGP of a router has restarted, all BGP peers linked to the BGP detect that the session is down and then up again. This “down/up” causes “routing flap” and recalculation of the BGP route. In addition, “routing flaps” may temporally generate the forwarding black hole and the forwarding loop. These phenomena have a negative impact on the performance of the entire network.

BGP graceful restart is a mechanism that helps minimizing the negative impacts caused by BGP restart. This mechanism makes the BGP speaker reserve the forwarding state while the BGP is restarting.



In the above figure, the RTB executes BGP restart and the RTA processes BGP graceful-restart. BGP graceful-restart is disabled by default. Therefore, use the following command to use this function. The stalepath-time is the maximum time period that the local BGP holds the stale-path for the restarting peer. If the restarting peer does not update the route for the time specified in the stalepath-time, the stale path is erased.

bgp graceful-restart [stalepath-time seconds]

To use BGP graceful-restart, you set the following commands in RTA.

```
/*-- RTA --*/  
!  
router bgp 100  
bgp graceful-restart stalepath-time 200  
neighbor 10.1.1.1 remote-as 200 /* RTB */
```

BGP default-metric

The default metric is used to solve problems of routes redistributed with the incompatible metric. This value is the Multi Exit Discriminator (MED) which has an impact on calculating the best path selection. The MED is a non-transitive value which can be processed by the local AS only. Therefore, this value is not forwarded to the external AS.

The following details the basic metric settings when this function has not been set.

- The metric of the redistributed IGP route is set identically with the interior BGP metric.
- The metric of the redistributed connected route and the static route is set to 0.
- The metric of the redistributed connected route is set to when this function is set.

To use this function, you set the following command.

default-metric number

BGP redistribute-internal

When the redistribute BGP is set in the IGP such as RIP, a loop can occur because the iBGP route is redistributed to the same IGP, such as OSPF or RIP. To prevent the situation, the iBGP route should not be redistributed even when the redistribute BGP is set by default.

To redistribute the iBGP route by force, use this command.

bgp redistribute-internal

bgp redistribute-internal

BGP Password encryption

You can use the authentication of TCP connection by specifying a password to the function neighbor.

When the passwords match, a TCP session is connected between neighbors and the neighbors communicate by using messages.

```
neighbor ip-address password KEY
neighbor ip-address password 0 KEY
neighbor ip-address password 7 KEY
```

You can encrypt password of neighbor. The password level before encryption is 0. After encryption, password level changes to 7. But you can not set password level 7 before encryption.

BGP disable-adj-out

The system does not maintain out bound table basically. It is for reducing overhead of memory. To disable this function, use the following command in the configuration mode.

```
no bgp disable-adj-out
```



Notice

When the system does not maintain Out bound table, you do not use “show ip bgp neighbors *ip-address* advertised-routes” command.

Use of set as-path prepend Command

You will change the path information to adjust BGP decision process sometimes.

To change path information, use the following command.

```
set as-path prepend <As-path#><As-path#>
```

Route Flap Dampening

Route Dampening minimizes the instability 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 seconds. 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 350 Terminology used in route dampening

Terminology	Description
History state	This does not include the best path for the route but information for the route flapping
Damp state	This shows the penalty 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 penalty 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 Invalid is performed every 10 seconds.
Maximum suppress limit	This is the maximum period that route can be invalid and the default is 4 times than half-lif-time.

Chapter 24. 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

- 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 host makes its routing table with using update information of dynamic routing protocol.
- IRDP (ICMP Router Discovery Protocol) client – The client runs Internet Control Message Protocol (ICMP) router discover client.

If you use dynamic protocol, need to set about host and it occurs overhead by running protocol. Moreover, when router has trouble, the switching may be delayed to another 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.

The following figure describes 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).

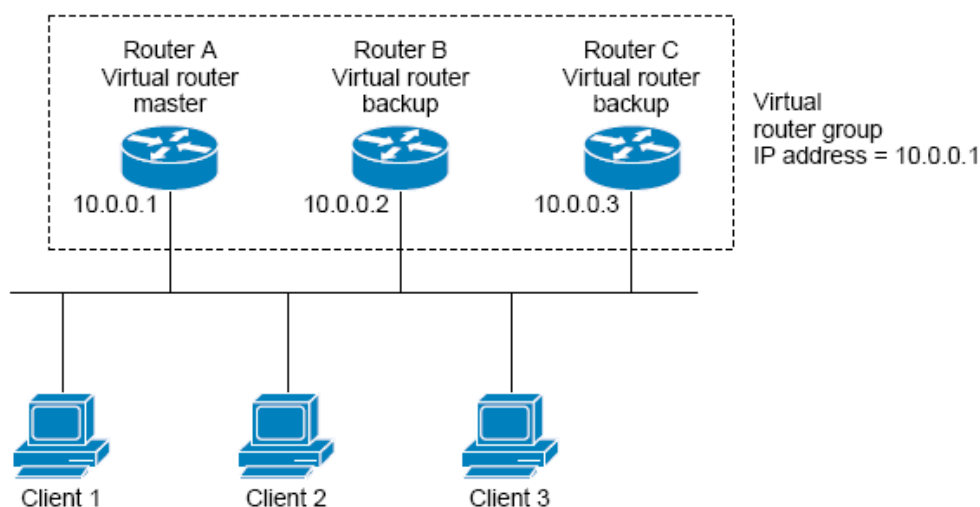


Figure 66. Basic VRRP Topology

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.

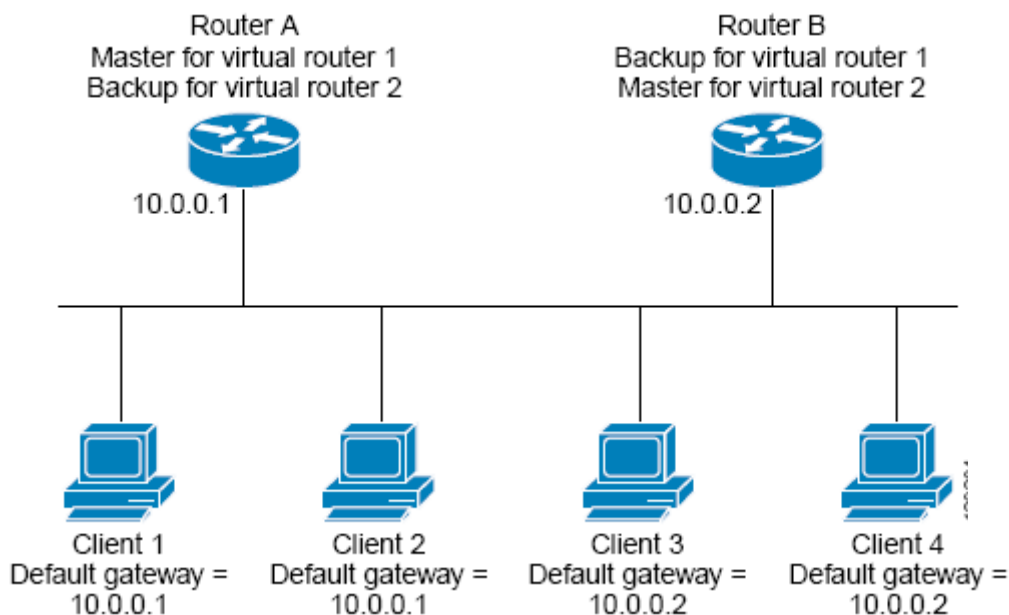


Figure 67. Load Sharing and Redundancy VRRP Topology

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 distributed 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 circuit fail-over

By changing VRRP priority according to status of interface, VRRP circuit fail-over supports that optimum VRRP router becomes master virtual router.

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 redundancy 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 backup 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 Advertisements

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 transmitted 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 Circuit failover

The circuit failover function of VRRP monitors interface status. You can set interface for monitoring with **circuit-falover** command. VRRP reduces or increase priority value of virtual router according to tracking interface status

How to Configure VRRP

This section covers the following procedures:

- Enabling VRRP
- Disabling VRRP
- Customizing VRRP
- Configuring VRRP circuit fail-over

Enabling VRRP

To enable VRRP, do the following steps.

Table 351 Enabling VRRP

Step	Command or Action	Purpose
Step 1	configure terminal Example: Switch# configure terminal	Enters Global configure mode
Step 2	interface <i>interface-name</i> Example: Switch(config)# interface gi2/2/10	Enters Interface configuration mode
Step 3	ip address <i>ip-address/prefix-length</i> Example: Switch(config-if-Gi2/2/10)# ip address 33.1.1.1/24	Specifies the IP address of interface
Step 4	router vrrp <i>virtual-ID interface-name</i> Example: Switch(config)# router vrrp 3 gi2/2/10	Enters the Router configuration mode
Step 5	virtual-ip <i>ip-address</i> Example: Switch(config-router)# virtual-ip 33.1.1.1	Enables VRRP on the interface and set virtual-ip 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 6	enable Example: Switch(config-router)# enable	Enables vrrp session
Step 7	End Example: Switch(config-router)# end	Returns the privileged EXEC mode
Step 8	show vrrp Example:	Shows the status of VRRP group of the router (Optional)

	Switch# show vrrp	
Step 9	show vrrp virtual-ID <i>interface-name</i> Example: Switch# show vrrp gi2/2/10	Shows information of VRRP group set in a specific interface (Optional)

Disabling VRRP on an Interface

It is possible to disable only the protocol operation while keeping VRRP settings, by disabling VRRP on the interface. Using **show running-config** command you can check the settings of VRRP group and whether or not VRRP is working.

Table 352 Disabling VRRP on an Interface

Step	Command or Action	Purpose
Step 1	configure terminal Example: Switch# configure terminal	Enters the Global configure mode
Step 2	router vrrp virtual-ID <i>interface-name</i> Example: Switch(config)# router vrrp 3 gi2/2/10	Enters the Router configuration mode
Step 3	disable Example: Switch(config-router)# disable	Disables a specific vrrp session

Customizing VRRP

To customize options, follow the steps below.

Table 353 Customizing VRRP

Step	Command or Action	Purpose
Step 1	configure terminal Example: Switch# configure terminal	Enters the Global configure mode
Step 2	router vrrp virtual-ID <i>interface-name</i> Example: Switch(config)# router vrrp 3 gi2/2/10	Enters the Router configuration mode
Step 3	advertisement-interval interval Example: Switch(config-router)# advertisement-interval 3	Sets VRRP advertiment period sending from VRRP master. - default : 1 second Note: You must set routers in one VRRP group with the same period.
Step 4	preempt-mode [true false] Example:	Sets to allow if the router that is higher priority than current virtual master router as a new master.

	Switch(config-router)# preempt-mode true	
Step 5	priority <i>level</i> Example: Switch(config-router)# priority 200	Sets the priority of VRRP router - default is 100

Configuring VRRP circuit failover

If you set VRRP circuit failover, do the following task. If the set interface is down with this command, the VRRP reduce priority value of router as much as specific value.

If VRRP group is owner of IP address, the priority of VRRP group fixes 255. The priority does not change with circuit failover.

Table 354 Configuring VRRP circuit failover

Step	Command or Action	Purpose
Step 1	configure terminal Example: Switch# configure terminal	Enters the Global configure mode
Step 2	router vrrp <i>virtual-ID interface-name</i> Example: Switch(config)# router vrrp 1 gi2/2/1	Enters the Router configuration mode
Step 3	circuit-failover <i>interface-name PriorityDelta</i> Example: Switch(config-router)# circuit-failover gi1/1/1 10	Sets the interface that effect to priority of VRRP group with interface status and value reducing priority value.
Step 4	show vrrp Example: Switch# show vrrp	Shows the status of VRRP group of the router (Optional)

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 10 seconds.

Preemption is activated

- 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

```
router vrrp 1 vlan1
    virtual-ip 10.1.0.10 backup
advertisement-interval 3
priority 120
router vrrp 5 vlan1
    virtual-ip 10.1.0.50 backup
advertisement-interval 10
router vrrp 100 vlan1
    virtual-ip 10.1.0.100 backup
preempt-mode false
```

Router B

```
router vrrp 1 vlan1
    virtual-ip 10.1.0.10 backup
advertisement-interval 3
router vrrp 5 vlan1
    virtual-ip 10.1.0.50 backup
priority 200
advertisement-interval 10
router vrrp 100 vlan1
```

```
virtual-ip 10.1.0.100 backup
preempt-mode false
```

VRRP circuit failover: 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.

```
router vrrp 3 vlan1
  virtual-ip 33.1.1.1 backup
  priority 120
  circuit-failover vlan10 15
```

VRRP Circuit fail-over Verification: Example

The following example is to track the settings made in “VRRP circuit failover: Example” section.

```
Switch# show vrrp
Address family IPv4
  State is Master
Virtual IP address is 33.1.1.1 (Not-owner)
Virtual MAC address is 0000.5e00.0101
Advertisement interval is 1 sec
Preemption is enabled
Priority is 120, Current priority is 120
Master Router is 33.1.1.3 (), priority is 120
Master Advertisement interval is 1 sec
Master Down interval is 4 sec
Circuit failover interface vlan10, Priority Delta 15, Status UP
```

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.

```
router vrrp 3 vlan1
  virtual-ip 33.1.1.1 backup
  priority 120
  disable
```
