



User Guide

C9500 Series
10G EPON (DPoE) OLT
(Optical Line Terminal)

User Guide



User Guide Version 1.04

CO-108250-EN

Copyright© CommScope Inc. All rights Reserved.

Although every effort has been taken to ensure the accuracy of this document it may be necessary, without notice, to make amendments or correct omissions. Specifications subject to change without notice.

Preface

This guide provides instructions for using the CommScope C9500 series 10G EPON (DPoE) OLT:

This preface describes the intended audience, conventions, and icons.

Audience

This guide is intended for network administrators and engineers responsible for configuring the C9500 series. This guide assumes you have the following background knowledge:

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



Notice

For further information about installing the C9500 series, refer to the *C9500 Installation Guide*.

Conventions

This guide uses the following conventions.

Convention	Description
Screen displays	Information that is displayed on the OAM terminal screen as a result of a command execution. Indicates command syntax.
Screen displays bold	Indicates how you would type a particular command.
[Key] Input	Indicates pressing a key of the keyboard (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>	Emphasizes a point or denotes new terms that are defined in the text. Indicates parameters that you would enter.

Icons

Icon	Type	Description
------	------	-------------

	Notice	Presents useful information related to <i>User Guide</i> contents, references, data, etc.
	Warning	Describes situations where data loss and incorrect product operation may occur, and provides proper actions to take in these situations.

Related Documents

For further information about the C9500 series, refer to the following manual:

- *C9500 Installation Guide*

**Notice**

Refer to the web page for up-to-date specifications: www.CommScope.com or www.mycommscope.com

Table of Contents

Preface.....	1
Audience.....	1
Conventions	1
Icons.....	1
Related Documents	2
Table of Contents	3
Chapter 1.Overview	19
Command Line Editor and Help	20
Command Syntax	20
Command Syntax Helper.....	20
Abbreviated Syntax	21
Command Symbols	22
Command Line Editing Key and Help Function.....	23
Switch Command Mode	24
Starting Up the C9500 Series	25
User Interface	26
Connection through Console Port	26
Connecting through Telnet.....	27
Connection through SSH	27
Connection through SNMP Network Manager	27
User Management.....	29
Adding/Deleting a User	29
Setting the User Password	30
AAA (Authentication Authorization Accounting)	32
Authentication.....	32
User Authentication	32
Setting User Authentication	34
Authorization	34
Accounting	36
Session Access Management.....	36
Privilege level Configuration.....	37
Server Configuration.....	38
RADIUS Server Configuration.....	38
TACACS+ Server Configuration	39
Setting Hostname.....	40

SNMP (Simple Network Management Protocol)	42
SNMP Configuration	42
SNMP Community.....	42
SNMP Trap host	43
SNMP Trap	44
SNMPv3 Configuration	45
SNMP engineID.....	46
User of SNMPv3.....	46
ACL (Access Control List)	48
Rules for ACL Creation	48
Configuration of Standard IP Access List	48
Configuration of Access List for Telnet Connection.....	49
Banner Configuration.....	50
AFSMGR (Alarm Fault Status Manager).....	52
Setting AFS Alarm.....	52
Clear AFS Alarm Event	53
Clearing AFS history.....	53
Setting AFS Masking Function.....	54
Setting AFS Severity Class.....	54
Setting AFS SNMP Trap	55
Changing AFS Configuration with default-config.....	57
Chapter 2.Interface environment setting	59
Overview.....	60
Common Commands	61
Interface name	61
Interface id.....	61
Interface mode prompt	62
Description Command.....	62
Show Interface Information.....	63
Show interface Command.....	63
Show Interface status Command	63
Show interface trunk Command	64
show idprom Command	64
Physical Port Configuration.....	67
Shutdown.....	67
Speed and duplex	67
Uplink Line Speed setting.....	67

Storm Control	69
Port mirroring	70
Layer 2 Interface Configuration.....	71
VLAN Trunking	71
Layer 2 Interface mode	71
Layer 2 Interface Defaults	71
Enabling/disabling Layer 2 Interface.....	71
Trunk port setting	72
Access port setting	72
Port group	74
Overview of Port Group.....	74
Port group configuration.....	74
MAC Filtering	75
MAC Filtering Overview	75
MAC Filtering Setting.....	75
MAC Filtering according to CPU Load.....	76
MAC Filtering according to CPU Load Overview.....	76
MAC Filtering according to CPU Load Setting	76
Traffic-control	77
Traffic-control Overview	77
Traffic-control Setting	77
Chapter 3.VLAN	78
VLAN overview.....	79
Advantages of VLAN	80
Efficient Traffic Control	80
Enhanced Network Security	80
Flexible Network and Device management	80
VLAN Types.....	81
Port-based VLANs	81
Tagged VLANs	83
Uses of Tagged VLANs	83
Assigning a VLAN Tag.....	83
Hybrid VLAN (Mixing Port-based VLAN and Tagged VLAN).....	84
VLAN Configuration	85
VLAN ID	85
Default VLAN	85
Native VLAN	85

VLAN Setting.....	86
Commands for VLAN Configuration.....	86
Examples of VLAN Configuration.....	87
Displaying VLAN Settings.....	91
Private Edge VLAN	92
Chapter 4.IP Configuration	93
Assigning an IP address	94
ARP (Address Resolution Protocol).....	95
Configuring Static Routes	96
IP Configuration Example	97
Chapter 5.DHCP.....	99
DHCP Server Features and Configuration	100
Overview of DHCP Server Functions.....	100
DHCP Pool Configuration	102
Enabling DHCP Server Function	106
DHCP relay agent Features and Configuration	107
DHCP relay agent Overview.....	107
Enabling DHCP Relay Function	107
DHCP Server Configuration on DHCP Relay Agent	108
DHCP relay information option (OPTION82) Configuration	109
DHCP Smart Relay Configuration.....	111
DHCP Relay Verify MAC-Address Configuration	112
DHCP relay rate-limit Set-up.....	113
DHCP Class based DHCP packet forwarding.....	115
DHCP Snooping Function	117
DHCP Snooping Function Overview.....	117
Activation of DHCP Snooping Function	117
DHCP Snooping Vlan Configuration	118
DHCP Snooping information option (OPTION82) Configuration	118
DHCP Snooping Trust Port Configuration	119
DHCP Snooping max-entry Configuration	120
DHCP Snooping Entry Time Configuration.....	120
DHCP Snooping Rate-Limit Configuration.....	121
DHCP Snooping Verify MAC-Address Configuration	121
DHCP Server Monitoring and Management.....	123

DHCP Server Pool Information Inquiry	123
DHCP Server Binding Information Search	123
DHCP Server Statistics Search	123
DHCP Server Conflict Search.....	123
DHCP Server Variables Initialization Command.....	124
DHCP Server Debug command	124
DHCP relay Monitoring and Control	124
DHCP Snooping Monitoring and Control.....	124
DHCP Configuration Examples	125
DHCP Network Pool Configuration	125
DHCP Server Monitoring and Control	125
DHCP Relay Agent Configuration.....	127
Chapter 6. ..RIP	129
Information about RIP	130
How to Configure RIP.....	131
Enabling RIP	131
Allowing Unicast updates for RIP	131
Passive interface	131
Applying Offsets to Routing metrics	132
Adjusting Timers	132
Specifying a RIP Version	132
Applying Distance	134
Enabling Split Horizon.....	134
Configuration Examples for RIP	135
RIP construction.....	135
Offset-list Set-UP.....	136
Passive-interface Configuration	136
Chapter 7.OSPF	138
OSPF Overview	139
Link-state Database	139
Areas	139
AREA 0	139
Stub areas	140
Virtual links	140
Route Redistribution	140
OSPF Configuration	141

OSPF interface parameters.....	141
Different Physical Networks	141
OSPF Network type	141
Point-to-Multipoint, Broadcast Networks	142
Nonbroadcast Networks	142
OSPF Area parameters.....	143
OSPF NSSA	143
OSPF Area Route summarization	144
Route Summarization of Redistributed Routes	144
Virtual Links.....	145
Generating a Default Route	145
Router ID Choice with a Loopback Interface	145
Default metric	146
OSPF administrative Distance	146
Passive interface	146
Route Calculation Timers	146
Logging Neighbors Going Up/Down	147
Blocking LSA Flooding.....	147
Ignoring MOSPF LSA Packets	147
Monitoring and Maintaining OSPF	147

Chapter 8.IS-IS..... 149

IS-IS Overview	150
IS-IS PDU Types.....	150
LSPDB Synchronization.....	151
Shortest Path Calculation	152
Route Redistribution	152
Enabling IS-IS as an IP Routing Protocol on the Device.....	153

Chapter 9.BGP..... 158

BGP Configuration.....	159
Enabling BGP Protocol.....	159
Neighbor Configuration.....	159
BGP Filtering	159
BGP Attribute Configuration	164
Routing Policy Modification	174
BGP Peer Groups	175
BGP Multipath	176
BGP graceful-restart.....	177

BGP default-metric	178
BGP redistribute-internal	178
BGP Password encryption.....	178
BGP disable-adj-out	179
Use of set as-path prepend Command.....	179
Route Flap Dampening.....	180
Chapter 10.IGMP Snooping	181
IGMP Snooping Overview.....	182
IGMP Snooping Configuration.....	183
Enable IGMP Snooping on a VLAN	183
Configure IGMP Snooping Functionality	183
Display System and Network Statistics.....	189
Chapter 11.IP Multicast Routing	190
IP Multicast Routing Overview	191
IGMP Overview	192
PIM-SM Overview	193
IP Multicast Routing Configuration.....	194
Enable IP Multicast Routing.....	194
Enable IGMP and PIM on an interface	194
Configure Multicast Functionality	194
Configure IGMP Functionality.....	197
Configure PIM-SM Functionality	206
Display System and Network Statistics.....	214
Chapter 12.Statistics Monitoring	215
Status Monitoring	216
System Threshold Configuration	217
Temperature Configuration	217
CPU Usage Configuration	217
Memory Usage Configuration.....	217
Application Memory Usage Display.....	218
Port Statistics.....	219
RMON (Remote Monitoring)	222
RMON Overview	222
RMON Alarm and Event Group Configuration.....	223

Logging	226
System Log Message	226
Default Logging Value	226
Examples of Logging Configuration	227

Chapter 13. STP (Spanning Tree Protocol) & SLD (Self-loop Detection). 229

Understanding Spanning-Tree Features	230
STP Overview	230
Bridge Protocol Data Units	230
Election of Root Switch	231
Bridge ID, Switch Priority, and Extended System ID	232
Spanning-Tree Timers	232
Creating the Spanning-Tree Topology	232
Spanning-Tree Interface States	233
Understanding RSTP	235
RSTP Overview	235
Port Roles and the Active Topology	235
Rapid Convergence	235
Bridge Protocol Data Unit Format and Processing	236
Understanding MSTP	238
MST Region	238
IST, CST and CIST	238
Configuring Spanning-Tree Features	240
Default STP Configuration	240
STP Configuration Guidelines	240
Enabling STP	240
Enable STP in no default Bridge	241
Configuring the Port Priority	242
Configuring the Path Cost	243
Configuring the Switch Priority of a VLAN	245
Configuring the Hello Time	247
Configuring the Forwarding-Delay Time for a VLAN	248
Configuring the Maximum-Aging Time for a VLAN	249
Changing the Max-hops for switch	251
Changing the Spanning-Tree mode for switch	251
Configuring portfast for switch	253
Changing transmit-holdcount for switch	254
Changing Cisco-interoperability for switch	255
Configuring autoedge for port	255

Configuring the Port as Edge Port	256
Specifying the Link Type to Ensure Rapid Transitions.....	257
Configuring force-version for port.....	258
Configuring root guard for port	259
Configuring hello-time for port.....	260
Configuring portfast for port	260
Configuring transmit-holdcount for port.....	260
Configuring restricted-role for port	260
Configuring restricted-tcn for port	261
Configuring MSTP Features	263
Instance Creation and VLAN Connection.....	263
Instance and port configuration.....	264
Setting region and revision number for MST	267
Pathcost for MSTP	268
Displaying the Spanning-Tree Status.....	269
Configuring Bridge MAC Forwarding.....	271
Self-loop Detection.....	273
Understanding Self-loop Detection	273
Default SLD Configuration	273
Configuring Self-loop Detection	273
Displaying Self-loop Status	277

Chapter 14.BFD (Bidirectional Forwarding Detection) ***279***

Understanding BFD.....	280
BFD Operation	280
Benefits of using BFD for Failure Detection	280
BFD Session Type	280
BFD Version Interoperability.....	281
BFD Restrictions	282
Default BFD Configuration.....	283
Configuring BFD	284
Configuring BFD session parameters on the interface	284
Configuring multi-hop BFD session parameters	284
Configuring BFD support for BGP	285
Configuring BFD support for OSPF.....	285
Configuring BFD support for Static routing	287
Configuring Passive Mode on the Interface	287
Configuring BFD Echo Mode.....	288

Configuring BFD slow timer	288
Displaying BFD information	288
BFD Configuration Samples	289

Sample One: Configuring BFD in an OSPF Network	289
Sample Two: Configuring BFD in a BGP Network	291
Sample Three: Configuring BFD for static routing	293

Chapter 15.LACP (Link Aggregation Control Protocol).....295

Understanding Link Aggregation Control Protocol.....	296
LACP Operation Principle	296
LACPDU Composition	296
LACP Modes	297
LACP Parameters.....	297
Configuring LACP and SLA	298
Specifying the System Priority	298
Specifying the Port Priority	298
Specifying the Timeout Value	299
Configuring LACP and static port group	299
Clearing LACP Statistics.....	300
Displaying 802.3ad Statistics and Status.....	301

Chapter 16.IP-OPTION.....303

IP OPTION Command Parameters	304
------------------------------------	-----

Chapter 17.VRRP (Virtual Router Redundancy Protocol).....306

Information about VRRP	307
------------------------------	-----

VRRP Operation.....	307
VRRP Benefits	308
Multiple Virtual Router Support.....	309
VRRP Router Priority and Preemption	309
VRRP Advertisements.....	309
VRRP Object Tracking	309

How to Configure VRRP	311
-----------------------------	-----

Enabling VRRP	311
Disabling VRRP on an Interface	311
Configuring VRRP Object Tracking	312

Configuration Examples for VRRP	314
---------------------------------------	-----

Configuring VRRP: Example	314
---------------------------------	-----

VRRP Object Tracking: Example	315
VRRP Object Tracking Verification: Example.....	315
Disabling a VRRP Group on an Interface: Example	316

Chapter 18.NTP.....317

Understanding Time Sources	318
Network Time Protocol	318
Hardware Clock.....	318
Configuring NTP	319
Configuring Poll-Based NTP Associations.....	319
Configuring NTP Authentication	319
Configuring the Source IP Address for NTP Packets	320
Configuring the System as an Authoritative NTP Server.....	320
Updating the Hardware Clock.....	320
Configuring Time and Date Manually.....	321
Configuring the Time Zone	321
Configuring Summer Time (Daylight Savings Time).....	321
Manually Setting the Software Clock.....	321
Using the Hardware Clock	322
Setting the Hardware Clock.....	322
Setting the Software Clock from the Hardware Clock.....	322
Setting the Hardware Clock from the Software Clock.....	322
Monitoring Time and Calendar Services.....	323
Clock Calendar and NTP Configuration Examples.....	323

Chapter 19.Dynamic ARP Inspection324

Understanding DAI	325
Understanding ARP	325
Understanding ARP Spoofing Attacks	325
Understanding DAI and ARP Spoofing Attacks	326
Interface Trust States and Network Security.....	327
Rate Limiting of ARP Packets	328
Relative Priority of ARP ACLs and DHCP Snooping Entries.....	329
Logging of Dropped Packets	329
Default DAI Configuration	329
DAI Configuration Guidelines and Restriction	330
Configuring DAI.....	331
Enabling DAI on VLANs	331

Configuring the DAI Interface Trust State	332
Applying ARP ACLs for DAI Filtering	333
Configuring ARP Packet Rate Limiting	334
Enabling DAI Error-Disabled Recovery	335
Enabling Additional Validation	335
Configuring DAI Logging	338
DAI Logging Overview	338
Configuring the DAI Logging Buffer Size	338
Configuring the DAI Logging System Messages	338
Configuring the DAI Log Filtering	339
Displaying DAI Information	340
DAI Configuration Samples	341
Sample: Interoperate with DHCP Relay	341

Chapter 20. QoS and ACL 343

QOS	344
Global Configuration	344
TX Scheduling Configuration	344
Port trust mode	345
DSCP Conversion Map Configuration	346
COS Conversion Map Configuration	347
ACL Configuration	348
Standard IP ACL	348
Extended IP ACL	349
MAC ACL	350
Application of ACL to Interface	350
Service-policy Configuration	352
Class-map	352
Policy-map	353
Service-policy	354
COPP	355
Service-policy on COPP	355
Rate-limit on COPP	355
Equipment Protection feature	355

Chapter 21. Utilities 356

Status dump command	357
Commands used	357

Command history Function	359
--------------------------------	-----

Output Post Processing	360
------------------------------	-----

Overview of output post processing.....	360
---	-----

Examples of output post processing.....	360
---	-----

DDM (Digital Diagnostic Monitoring)	361
---	-----

SFP DDM Monitoring.....	361
-------------------------	-----

Chapter 22.Saving Config File and Software Upgrade ***362***

File System	363
-------------------	-----

Image/Configuration/BSP Down/Up Load	364
--	-----

Download/Upload with the FTP.....	364
-----------------------------------	-----

Down/Up Loading File with the TFTP server.....	365
--	-----

Configuration File Management.....	366
------------------------------------	-----

Running configuration	366
-----------------------------	-----

Startup configuration	366
-----------------------------	-----

Saving Configuration File.....	366
--------------------------------	-----

Configuration File Erase	366
--------------------------------	-----

Boot Mode Setting and System Restart.....	368
---	-----

Boot Mode Setting	368
-------------------------	-----

Restarting an SCM.....	368
------------------------	-----

Restarting entire system	370
--------------------------------	-----

Chapter 23.DPoE Provisioning ***371***

Background and Theory of Operations	372
---	-----

Cable and Bundle Interface management	373
---	-----

Bundle Create and View.....	373
-----------------------------	-----

Bundle VLAN	374
-------------------	-----

IP(HSD) and L2HSD Services	374
----------------------------------	-----

Bundle Sub-Interface	374
----------------------------	-----

Cable Bundle Setting and View	375
-------------------------------------	-----

vCM and CPE's DHCP Relay management.....	377
--	-----

vCM's DHCP helper-address Setting and View	377
--	-----

CPE's DHCP helper-address Setting and View	377
--	-----

CPE's DHCP Option82 Setting	378
-----------------------------------	-----

Cable GIADDR	378
--------------------	-----

DHCP Option 43/17 for Vendor Specific Information.....	379
--	-----

DHCP Option 6 for MSO defined text.....	380
---	-----

DHCP Option 82 Sub-option for DPoE Version	381
Source Address Verification (SAV) management	382
CPE's SAV Setting	382
Static SAV Setting	382
Subscriber Management	384
CPE Learning Control at the DPoE System	384
CPE Learning Control at the ONU	385
Filtering at the DPoE System.....	385
ONU Encryption and Authentication	388
Security and Certificate Settings	388
CA Certificate.....	389
CM Certificate.....	389
Certificate Revocation List	391
Online Certificate Status Protocol	393
EAE Exclusion List	394
ONU White List	395
CM Offline List	396
CM Offline List	396
CM Flap List.....	396
Optical Monitoring	398
CM Power Levels.....	398
CM TFTP Client Settings	400
CM Event Management	401
Event Log Control.....	401
Event Log Size	403
Event Throttling	404
CM Secure Software Download.....	406
MEF-MN Interface.....	407
Subscriber's Provider Bridging (PB) Services.....	408
Provider Bridging Services.....	408
802.1ad PB Encapsulation Mode	408
802.1Q PB Encapsulation Mode.....	409
PB Transport Mode	410
Subscriber's Provider Backbone Bridging (PBB) Services.....	412
PBB Encapsulation Mode	412
PBB Transport Mode	412
IP(HSD) Services	415

DPoE IP(HSD)	415
Serving Groups	415
Legacy IP(HSD).....	416
Quality of Service (QoS)	417
Service Flows.....	417
Statistics per Service Flow	420
Classifiers	423
Downstream.....	423
Upstream	423
Upstream Drop Classifiers	423
DPoEv2.0 Multicast.....	425
Multicast Operation	425
Single Session vs Aggregate Session	425
Multicast QoS	425
Rate setting for PON interface port	427
Available rates for PIM-8XE	427
Setting for Turbo PON mode	427
Chapter 24. Netflow.....	429
Netflow Overview	430
Introduction to Netflow	430
Netflow Deployment	4 3 0
Netflow Flow	4 3 1
Netflow Packets	4 3 1
U9500 Netflow.....	4 3 3
Requirements and Characteristics.....	4 3 3
Creating Flows	4 3 3
Removing Flows.....	4 3 3
Restrictions	4 3 3
U9500 Default Netflow Settings.....	4 3 4
Commands for Collecting Statistical Data about Netflow Traffic	4 3 5
Configuring the Settings for Collecting Statistical Data about Netflow Traffic. 4 3 5	4 3 5
Enabling/Disabling the Collection of Statistical Data for Netflow Traffic	4 3 5
Setting the Flow Aging Out Time.....	4 3 5
Setting the Maximum Number of Flows	4 3 7
Commands for Viewing Statistical Data about Netflow Traffic	4 3 8
Viewing Statistical Data about Netflow Traffic	4 3 8
Commands for Viewing Flows.....	4 3 8
Purging All Flows.....	4 4 0

Commands for the Settings for Sending Statistical Data.....	4 4 1
Sending Statistical Data about Netflow Traffic	4 4 1
Configuring the Settings for Sending Statistical Data about Netflow Traffic....	4 4 1
Setting the Receiver of Statistical Data about Netflow Traffic.....	4 4 1
Setting the Source Interface to Send Statistical Data	4 4 2
Viewing the Export Status of Statistical Data about Netflow Traffic.....	4 4 2

Chapter 1. *Overview*

This chapter provides the following information required for system operators to configure and start up the C9500 series.

- Command line edit and help
- Switch command mode
- Switch startup
- The C9500 series 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 discusses the command line editor and built-in help features.

Command Syntax

Follow these steps to enter a command. Refer to Chapter 2 for further information about using the CLI.

1. Before entering a command at the prompt, ensure you have the appropriate privilege level. Most configuration commands require the administrator privilege level.
2. Enter a command. If no sub-command follows and 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. After you have entered the correct syntax, press [Return] to execute.



Notice

After entering commands, you may receive error messages such as "% Incomplete command". This means that the command you entered failed to execute. If you press the up arrow key, your last command will be displayed.

The following shows an example that a command was not fully entered.

```
Switch# show ↵
% Incomplete command.
Switch #
```

Command Syntax Helper

The CLI of the C9500 series has a built-in command syntax helper. Help may be requested at any point in a command by entering a question mark '?'. The C9500 series provides two styles of help.

Full Help

- Provides a full list of available sub-commands or parameters.
- Enter a command, and leave a blank space, and then enter a question mark.
- For example, **show ?**.

Partial Help

- Provides a list of sub-commands or parameters with the same sequence of characters.
- Enter a command, and then immediately follow with a question mark.
- For example, **show p?**.

The following is an example of the full help feature for the 'show' command.

```
Switch# show ?
 10gpon          10G PON information
 access-list      List IP access lists
 afs             AFS (Alarm, Fault, Status) information or configuration
 arp             Address Resolution Protocol (ARP)
 auth-mac        IPI MAC-Based Authentication
 authentication   Shows Auth Manager registrations or sessions
```

auto-config-write	write running-config automatically
bfd	Bidirectional Forwarding Detection (BFD)
bgp	Border Gateway Protocol (BGP)
bootvar	Boot and related environment variable
bridge	Bridge information
buffers	Adjust system buffer pool parameters
cal	CAL show
calendar	Display the hardware calendar
ce-vlan	COS Preservation for Customer Edge VLAN
class-map	Class map entry
cli	Show CLI tree of current mode
clns	Connectionless-Mode Network Service (CLNS)
clock	Display the system clock
command	shell command
config	Config file information
control-plane	Control-plane
cpu	cpu status and configuration
cpu-mac-filter	CPU rate limit based on Source MAC address
cpu-packet-counter	CPU packet-counter
cpu-rx-queue	Cpu rx packet queue
customer	Display Customer spanning-tree
cvlan	Display CVLAN information
debugging	Debugging functions (see also 'undebbug')
dot1x	IEEE 802.1X Port-Based Access Control
enhanced-hash	Enhanced Hashing Algorithm (RTAG7)
environment	Temperature and FAN status information
etherchannel	EtherChannel information
ethernet	ethernet service parameters
flash:	display information about flash: file system
flow-sampler	Display the flow samplers configured
flowcontrol	IEEE 802.3x Flow Control
fm-status	Show the current status
gw-ping-check	Specifies the Gateway Ping Check
ha-fib-summary	HA FIB summary

Switch# show_

The following is an example of the partial help feature for the **show** command.

Switch# show?	
	show Show running system information

Switch# show_

The following is an example of the partial help feature for the **show p** command. It assumes you want to check a port status, but do not know the right command. The CLI helper provides a list of options for the remainder of the command. 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
	pon PON Information
	port Port status and configuration
	port-mib Port-Mib Count
	pppoe Point-to-Point over Ethernet (PPPoE)
	privilege Show current privilege level

Switch# show p_

Abbreviated Syntax

CLI for the C9500 series 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, you must enter enough characters to make the command unambiguous and distinguishable to the C9500 series. After entering commands, you may receive the error message "% Ambiguous command: <typed command>". This means that there is more than one command with the same prefix that you have entered in the mode.

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

Switch# show i?
  idprom      show IDPROMs for FRUs
  imi         Integrated Management Interface (IMI)
  inet-service Display enabled internet services
  interface    IP interface status and configuration
  ip          IP information
  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 brackets	Enclose a variable or value in the command syntax. You must specify the variable or value. For example, in the syntax access-list <1-99> {deny/permit} address You must supply standard access control list number for <1-99> when entering the command.
{ }:	Braces	Enclose a required value or list of parameters in the command syntax. The administrator must enter at least one necessary item among the parameter list. For example, in the syntax router {rip/ospf} You must enter one of the two parameter 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)
X:X::X:X/M		IPv6 address

Command Line Editing Key and Help Function

The CLI of C9500 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 left character.
[Ctrl] + [F]	Moves the cursor to the right 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

The C9500 series provides the following various CLI 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-Giga7/1)# 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 C9500 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.

The character that follows the host name denotes the access mode type.

When you configure the C9500 series, you will face various kinds of prompts. The prompt shows your current mode and sub-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. Changing 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 {bgp rip ospf isis}	Moves from the Config mode to the Router mode.
pon	Moves from the Config mode to PON mode.
ip dhcp pool <i>name</i>	Moves from the Config mode to the DHCP Pool mode.
exit	Moves back to the previous mode.
end	Moves from any mode to the Privileged mode. Do not move from the User mode.

Starting Up the C9500 Series

When the C9500 series starts up for the first time, the boot loader performs a self test and loads the OS image from flash memory. After it has finished booting, it loads the previous configuration (startup-config) stored in flash memory.



Notice

For the purpose of system reliability, C9500 manages two OS images including Primary and Secondary. The Primary OS image can be loaded by the default settings. The system administrator can choose to load the Primary or Secondary image in either switch boot mode (only through a terminal connected to the console) or privileged mode.

User Interface

System administrators can access the C9500 series for system maintenance purposes, such as configuring, verifying, and collecting statistics, etc.

The simplest way to do this is to use a local OAM terminal connected to a separate console port that is provided by the C9500 series (Out-of-band management).

You can also use a Telnet program from a remote site. Use the service port (In-band management), as the C9500 series does not support a separate port for Telnet connections.

The system administrator can use the following methods to access the C9500 series.

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

The C9500 series supports multiple user sessions concurrently:

- 1 console session
- Up to 16 Telnet or SSH sessions

Connection through Console Port

The CLI is accessible through a RJ-45 type Ethernet port console. The console cable included in the C9500 series supports 9 pin. If your console port does not support DB9, use a USB-to-serial converter. The console port is located in the SCM at the front of the C9500 series.

The following figure shows the C9500 OLT terminal connected to the console port. Once a connection is established, you will see the switch prompt and you can log in.

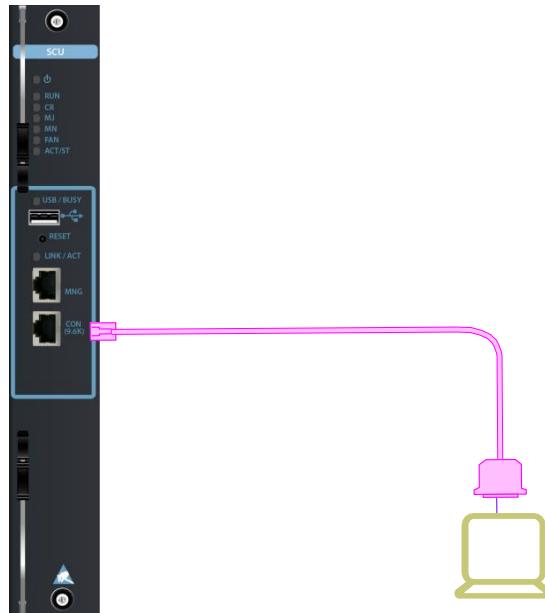


Figure 1 Connection of the C9500 and OAM Terminal



Notice

For the information on the terminal configuration and console port pinouts, refer to the C9500 Hardware Installation Guide.

Connecting through Telnet

Telnet connection allows multiple user access, access from remote locations, and faster access than the console. You can connect to the C9500 series at a workstation with a Telnet client using the preconfigured IP address. For further information about configuring the IP, refer to the *C9500 Installation Guide* or *C9516 Installation Guide*.

The default ID and password are as follows:

- ID: root
- Password: frontier

Enter the following command at the Telnet client.

```
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.

For security purposes, you can use access list to restrict the Telnet connection. For this refer to chapter <ACL (Access Control List)> in this manual.

Connection through SSH

SSH connection provides strengthened user security. You can connect to the C9500 series at a workstation with an SSH client using the preconfigured IP address. For further information about configuring the IP, refer to the *C9500 Installation Guide* or *C9516 Installation Guide*. For SSH to be used, the operator should set an ID and password, and the switch must have more than one IP address.

```
ssh [<ipaddress> | <hostname>]
```

When SSH connection is successfully established, the prompt for entering a password is shown on screen. Once you enter the password, the switch gets in User mode.

In addition, for the sake of system security the users who access via SSH can be limited by using of Access Control List. Refer to the section <ACL(Access Control List)>.

To use SSH, SSH must be enabled.

```
Switch(config)#service ssh
```

Connection through SNMP Network Manager

Any network manager running the Simple Network Management Protocol (SNMP) can manage the C9500.



Notice

For more information refer to SNMP (Simple Network Management Protocol)SNMP (Simple Network Management Protocol) Network Manager.

User Management

Adding/Deleting a User

The system operator can connect to the C9500 series through a console port or Telnet session. To log in, users need to be registered first. You can add/delete users, set user passwords/privileges, configure session timeout and access list.

A user's privilege is denoted as the privilege level. The following privilege levels are available:

- Privilege level 0 has a non-privileged status.
- Privilege levels 1-14 can execute user mode commands.
- Privilege level 15 can execute privileged mode commands.

A new user has the privilege level 1 by default and can enter privileged mode. You can enter privileged mode by executing the **enable** command in user mode.

Table 5 Commands for Adding or Deleting Users

Command	Description	Mode
<code>username name { nopassword password [0 7] password secret [0 5] password}</code>	Creates a user ID. nopassword : Does not require password upon login. Password or secret : Requires password upon login. The following values are available: 0 – No encryption. 5 – MD5 encryption. 7 – DES encryption.	Config
<code>no username name</code>	Deletes a user ID. If the user ID is <i>root</i> , the password is reset to the default, <i>frontier</i> .	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>	Disables access-list.	Config
<code>username name user-maxlinks value</code>	Sets the maximum number of sessions	Config
<code>no username name user-maxlinks value</code>	Resets the maximum number of sessions to the 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

Adding a User

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

```
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#
```

The following example shows **testuser3** with privilege level 15, entering privileged mode.

```
CommScope 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.

Setting the User Password

The C9500 series provides the following two types of passwords for system security.

Enable password

- Used for enhanced security in privileged mode.

User password

- Used to access through the console port or a Telnet session in user mode.

The following table lists commands for configuring the Enable password.

Table 6 Commands for Configuring the Enable Password

Command	Description	Mode
<code>enable password [0 7] password</code>	Specifies the password necessary for entering privileged mode. An encrypted or DES encrypted password is required to enter privileged mode: 0 – No Encryption. 7 – DES Encryption	Config
<code>enable secret [0 5] password</code>	Enables the password to enter privileged mode. An encrypted or DES encrypted password is required to enter privileged mode. 0 – No Encryption. 5 – MD5 Encryption	Config
<code>no enable password</code>	Disables the password from entering privileged mode.	Config

Setting the Enable password

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

```

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

The following example shows the password above 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.

Password Encryption Mode Setting

As seen above the assigned password is visible. Anyone can retrieve it by a command, like **show running-config**. To prevent this C9500 Series provides encryption capability while assigning the passwords.

```

Switch# configure terminal
Switch(config)# service password-encryption
Switch(config)# end
Switch# show running-config
!
enable password 7 xxEp88GxHJIgc
username lns nopassword
username test password 7 XX1LtbDbOY4/E
username admin privilege 15 password 7 xxiz1FI3TBLPs
!
Switch#
```

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 other authentication. In the case of trying authentication with Local system, if the information about the user who wants to log in or enter privileged mode does not exist, the system attempts authentication with the next set.

Local authentication is always enabled. In case that you do not specify an authentication setting, the system defaults to user authentication with Local authentication.

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. fault: 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. fault: Ascii	Config
no aaa authentication login authen-type	Clears the account of users without account	Config
aaa authentication login console	Applies RADIUS or TACACS+ authentication to the console (By default, local authentication is applied to the console. This configuration applies RADIUS or TACACS+ authentication first,	config

	and then applies local authentication (if RADIUS or TACACS+ authentication fails.).)	
no aaa authentication login console	Disables RADIUS or TACACS+ authentication.	

Setting User Authentication

Three ways of user authentication are as following:

- Check access 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, allow login. 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 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 a password to the local system, the authentication method always succeeds. So you must enable a 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 with 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 a response from the RADIUS server, it tries 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 using the system resources via privilege 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. Also, when you execute a specific command, the system compares the privilege level of each command with the privilege level set. Then the system can check the executive authorization of relevant commands 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 failing authorization verification with the local system, changes will need to be made 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 the user definition shell. The authorization that can execute 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).

```
username: 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 the command is executed. The system can check the executable authorization from the local system or TACACS+ server to verify if 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. <0-15>: privilege level	Config
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 the **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 a 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 around a specific command, each command refers to the executed mode of the privilege level.

Table 13 Privilege level Configuration

Command	Description	Mode
privilege node level <0-15> command	Assigns privilege level about specific command. <0-15>: privilege level	Config
no privilege node level <0-15> command	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

The C9500 series provides 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 TACACS+ servers.

RADIUS Server Configuration

Table 14 RADIUS Server Configuration Commands

Command	Description	Mode
radius-server host (A.B.C.D/X:X::X:X) [key [0 7] key-string]	Sets RADIUS server. <i>A.B.C.D</i> : RADIUS server address <i>X:X::X:X</i> : RADIUS server IPv6 address <i>key</i> : Sets encryption key. 0 – Does not encryption 7 – DES encryption	Config
no radius-server host (A.B.C.D/X:X::X:X)	Deletes the set RADIUS server. <i>A.B.C.D</i> : RADIUS server address <i>X:X::X:X</i> : RADIUS server IPv6 address	Config
radius-server host (A.B.C.D/X:X::X:X) [auth-port PORT]	Sets RADIUS server and auth-port for using to server. <i>A.B.C.D</i> : RADIUS server address <i>X:X::X:X</i> : RADIUS server IPv6 address <i>PORT</i> : auth-port number	Config
no radius-server host (A.B.C.D/X:X::X:X) auth-port PORT	Sets auth-port for using to server with default value. default: 1812	Config
radius-server key [0 7] key-string	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 count	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 seconds	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 ifname	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 keys with test 123. It sends AAA information to server. If the system does not receive a response, the system 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 (<i>A.B.C.D/X:X::X:X</i>) key [0 7] <i>key-string</i>	Sets TACACS+ server. <i>B.C.D</i> : TACACS+ server address <i>X::X:X</i> : RADIUS server IPv6 address <i>y</i> : Sets security key. 0 – None Encryption 7 – DES Encryption	Config
no tacacs-server host (<i>A.B.C.D/X:X::X:X</i>)	Deletes tacacs+ server setting. <i>B.C.D</i> : TACACS+ server address <i>X::X:X</i> : RADIUS server IPv6 address	Config
tacacs-server host (<i>A.B.C.D/X:X::X:X</i>) timeout <i>seconds</i>	Sets timeout value with TACACS+ server. <i>conds</i> : Timeout value	Config
tacacs-server host (<i>A.B.C.D/X:X::X:X</i>) timeout	Sets default timeout <i>fault</i> : 5 seconds	Config
ip tacacs source-interface <i>ifname</i>	Sets source IP address of information sent to TACACS+ server. <i>ame</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 the C9500 series, the system model name is the **default** hostname and the administrator can change the default hostname to a new hostname.

Table 16 Hostname setting command

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 C9500
C9500 (config)# end
C9500 #
C9500 # configure terminal
C9500 (config)# no hostname
Switch(config)# end
Switch(config)#

```

SCM information in prompt

The control unit of the C9500 series is implemented to be redundant, which means it has two SCM cards in a system. The currently active SCM is indicated in a prompt string. The acronym which represents the operation status (i.e. Active or Standby) and position of SCM (i.e. Left or Right) is present next to the hostname information in a prompt string.

Acronym	Meaning
[A/L]	SCM1 (Left position) with active status
[A/R]	SCM2 (Right position) with active status
[S/L]	SCM1 (Left position) with standby status
[S/R]	SCM2 (Right position) with standby status

The prompts look like the following examples.

```
Switch[A/L]>
Switch[A/L]>enable
Switch[A/L]#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch[A/L] (config)#telnet scu2
telnet scu2

Trying 169.254.253.2...
Connected to scu2.
Escape character is '^]'.

Switch login: root
Password:
```

Hello.

Switch[S/R]>



Notice

Not all the examples in this manual have applied this prompt generation rule.

SNMP (Simple Network Management Protocol)

SNMP network manager can manage the switch that provides the 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
<code>snmp-server contact <i>string</i></code>	Enters the information of system manager	Config
<code>no snmp-server contact</code>	Deletes the information of system manager	Config
<code>snmp-server location <i>string</i></code>	Enters the location information where switch is installed.	Config
<code>no snmp-server location</code>	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@CommScope.com"
Switch(config)# end
Switch# show running-config
!
snmp-server contact "gil-dong hong. hong@CommScope.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 the C9500 series.

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 cess-type: SNMP Agent access type ro: read only rw: read write ew: designates MIB access scope, the detail information refers to snmp-server view setting. <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 cannot 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 alarm.	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 a trap of fan, 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 sec-level}[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. <i>read</i> : Read view setting. In case that you do not specify Read-view, the system sets default value with internet (1.3.6.1). <i>write</i> : Write view setting	Config
no snmp-server group <i>groupname</i> {v1 v2c v3 sec-level}	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>] [<i>priv</i> (des aes) <i>priv-passwd</i>] [<i>access</i> <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. <i>priv</i> : You can encrypt SNMP PDU, set DES or AES with the specified method of encryption. <i>priv-passwd</i> : Setting password for encryption. <i>access</i> : applies access-list about user. <1-99> : IP standard access list	Config
no snmp-server user <i>username</i> <i>groupname</i> {v1 v2c v3}	Removes SNMP user	Config
show snmp user	Shows SNMP user.	Privileged

	Sets SNMP view.	
snmp-server view <i>viewname</i> <i>viewoid</i> {excluded included}	<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 <i>viewname</i> <i>viewoid</i>	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
```

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 verify using the **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

Permitting any access

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

Denying 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

The C9500 series can register a login banner and MOTD banner. The login banner is a message displayed before a user logs into the system, while a MOTD banner is a message displayed after logging into the system. You can send messages like cautions to the user via a 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 the logging in a banner. The banner can be 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 .
Enter TEXT message. End with the character '.'.

C9500  Switch

Login Banner TEST!

.

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

C9500  Switch

Login Banner TEST!

^C
!
```

**Notice**

When you show 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:

C9500 Switch

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 the SNMP trap event occurring from the 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
afs current clear [alarm-index]	Clears alarm that does not clear in the AFS event. <i>alarm-index</i> : index <1-99999>	Config
afs history clear	moves the history of AFS event	Config
afs mask enable/disable [afs-type [event-type [afs-id]]]	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
afs severity critical/major/minor afs-id	Changes class about AFS event. <i>afs-id</i> : A01001, S01001, F01001,...	Config
afs snmp enable/disable [afs-type [event-type [afs-id]]]	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
afs factory-default running-config [mask/snmp]	Changes the mask set to current afs running-config and snmp value with default-config. <i>mask</i> : changes mask configuration only <i>snmp</i> : changes snmp configuration only	

Clear AFS Alarm Event

You can forcefully clear the Alarm when the error is not cleared while there is still 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 value<45> thres<50>  
-----  
Switch# configure terminal  
Switch(config)# afs current clear  
Switch# show afs current
-----
-----  
no id type level date  
-----  
-----
```

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> value<4>
thres<1>
2006-08-06 09:21:22 A04001 processing maj on sys<1> value<4>
thres<3>
2006-08-06 09:21:22 A04003 processing maj on sys<1> value<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 the setting value of default-config.

The default value of some messages (S02009, S06002, and F02003) are 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 the AFS default-config.

Setting AFS SNMP Trap

You can set SNMP Trap about an AFS event. Moreover, you can set All for AFS events or else set 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 values when running 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 environment setting*

This chapter describes the system interface.

Overview

The interfaces supported in the C9500 series are as follows:

Table 25 Interfaces Supported in the C9500 series

Interface	Type
Physical interfaces	<ul style="list-style-type: none">■ Gigabit Ethernet• 1000Base-X■ TenGigabit Ethernet• 10GBase-X
PON interface	<ul style="list-style-type: none">■ GE-PON■ 10GE-PON
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 should be performed in advance:

1. Enter the config mode from the privileged mode using **configure terminal** command.
2. Enter into the interface mode using **interface** command.
3. 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 IFNAME	Enters into the interface. <i>IFNAME</i> : Name of the specific interface for configuration.
description string	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

The C9500 series 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	"gi" + slot_id + "/" + port_id	gi7/1
	TenGigabit Ethernet	"te" + slot_id + "/" + port_id	te7/1
PON interface	General PON	"pon" + slot_id + "/" + port_id	pon1/1
	GE-PON	"ep" + slot_id + "/" + port_id	ep1/1
	10GE-PON	"tp" + slot_id + "/" + port_id	tp1/1
Port-group interface	Port group	"po" + port-group id	po1
VLAN interface	VLAN	"vlan" + vlan id	vlan10
Loopback interface	Loopback	"lo" + id	lo0
Management interface	Fast Ethernet	"eth" + id	eth0

Interface id

Interface name consists of interface type and id. The following shows the naming of the C9500 series interface and range supported.

Table 28 Interface ID and Range Supported

Interface Type	ID	ID Range	Name
Gigabit ethernet	slot id/port id	slot id:6~7, port id: 1-8	gi7/1
TenGigabit ethernet	slot id/port id	slot id:6~7, port id: 1-8	te6/1
General PON	slot id/port id	slot id:1~5 & 8~12, port id: 1-8	pon1/1
GEAPON	slot id/port id	slot id:1~5 & 8~12, port id: 1-8	ep1/1
10GEAPON	slot id/port id	slot id:1~5 & 8~12, port id: 1-8	tp1/1
Port group	port-group id	slot id:1~5 & 8~12, port id: 1-81 – 255	po1, po255
VLAN	vlan id	1 – 4094	vlan4094
LoopBack	interface id	0 – 3	lo0, lo3
management	interface id	0	eth0



Notice

PON cards are to be placed in slot #1~#5 and #8~#12 meanwhile Ethernet Line interface cards should be placed in slot #6 and #7.

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 [A/L] (config-if-Giga6/1)#

Description Command

The **description** command is used to add a description on each interface. The description is the comment used to help the administrator remember the interface purpose and you can see the result with the **show interface description** 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 [ifname]	■ Displays the status and configuration of the interface.	Privileged
show interface status	■ Displays the status of all the physical interface	Privileged
show interface transceiver [detail]	■ Displays the information of DDM (Digital Diagnostic Monitoring).	Privileged
show interface trunk	■ Displays the switchport of physical/port-group interface	Privileged

Show interface Command

The **show interface** command is used to view the interface configuration information, the link status, and the interface-related statistics. The **show interface** command shows the information on all the interfaces defined. In the case of the GBIC interface if the DDM feature is supported the Diagnostic of the corresponding GBIC can be retrieved also. (Refer to DDM feature in DDM (Digital Diagnostic Monitoring))

```
Switch# show interface
gi1/1 is down
type 1000Base-GBIC,LC, 10,000M, 1,490nm
gbic inserted
vendor EZCONN
part name ETB43341-8LNT
Rev No Info
SN R00169
Date 061218
gbic diagnostic
temperature 47.0 'C vcc 3.25 Volt
rx power -inf dBm tx power -6.10 dBm
bias 14.1 mA
no auto-negotiation
speed set 1G
duplex set full
vlan ingress check enabled

Last clearing of counters 00:03:54
1 minutes input rate 0 bytes/sec, 0 packets/sec
1 minutes output rate 0 bytes/sec, 0 packets/sec
0 packets input, 0 bytes
Received 0 broadcasts, 0 multicasts
0 CRC, 0 oversize, 0 dropped
    0 packets output, 0 bytes
    Sent 0 broadcasts, 0 multicasts
```

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

-						
Gi6/1		connected	100	full	a-1000	1000BaseLX
Gi6/2		connected	100	full	a-1000	1000BaseLX
Gi6/3		connected	100	full	a-1000	1000BaseLX
Gi6/4		connected	100	full	a-1000	1000BaseLX
Gi6/5		connected	200	full	a-1000	1000BaseLX
Gi6/6		connected	200	full	a-1000	1000BaseLX
Gi6/7		connected	200	full	a-1000	1000BaseLX
Gi6/8		connected	200	full	a-1000	1000BaseLX



Notice

The Captured image of CLI execution per each configuration case may be different according to equipped interface module and name. Refer to the interface id in 오류! 참조 원본을 찾을 수 없습니다..

Show interface trunk Command

Switchport means the port and port-group which operate at layer 2 switching mode. The command, **Show interface trunk**, displays the switchport information of physical port and port-group. The mode, native and tagged vlan lists are included in this Switchport information.

Switch#show interface trunk		
Port	Mode	Native vlan
Gi6/1	access	100
Gi6/2	access	100
Gi6/3	access	100
Gi6/4	access	100
Gi6/5	access	200
Gi6/6	access	200
Gi6/7	access	200
Gi6/8	access	200
Po10	access	100
Po20	access	200
Port	Vlans allowed on trunk	
Gi6/1	none	
Gi6/2	none	
Gi6/3	none	
Gi6/4	none	
Gi6/5	none	
Gi6/6	none	
Gi6/7	none	
Gi6/8	none	
Po10	none	
Po20	none	

show idprom Command

show idprom command is used to display the FRU (Field Replaceable Unit) information of the system. The C9500 series presents relevant information for the following modules of FRU type.

- Chassis
- FAN

- FMU
- Module
- SCM
- PMU
- Power
- Slot
- Transceiver

Below is the message to be displayed on the console window when **show idprom all is executed.**

```

Switch#show idprom all
IDPROM for chassis
  Name = 'CommScope Epon System'
  Description = 'CommScope Chassis System'
  SNMP index = '1'

IDPROM for scu 1
  Name = 'Physical Module SCM 1'
  Description = 'CommScope Physical Module SCM 1'
  SNMP index = '2'

IDPROM for scu 2
  Name = 'Physical Module SCM 2'
  Description = 'CommScope Physical Module SCM 2'
  SNMP index = '3'

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

IDPROM for slot 3
  Name = 'Physical Slot 3'
  Description = 'CommScope Physical Slot 3'
  SNMP index = '14'

IDPROM for slot 4
  Name = 'Physical Slot 4'
  Description = 'CommScope Physical Slot 4'
  SNMP index = '16'

IDPROM for slot 5
  Name = 'Physical Slot 5'
  Description = 'CommScope Physical Slot 5'
  SNMP index = '18'

IDPROM for slot 6
  Name = 'Physical Slot 6'
  Description = 'CommScope Physical Slot 6'
  SNMP index = '20'

IDPROM for slot 7
  Name = 'Physical Slot 7'
  Description = 'CommScope Physical Slot 7'
  SNMP index = '22'

IDPROM for slot 8
  Name = 'Physical Slot 8'
  Description = 'CommScope Physical Slot 8'
  SNMP index = '24'

IDPROM for pmu 1
  Name = 'Container of Power Module 1'
  Description = 'Container of Power Module 1'
  SNMP index = '30'

IDPROM for pwr 1
  Name = 'Power 1'
```

```
Description = 'Power 1'
SNMP index = '31'

IDPROM for slot 12
Name = 'Physical Slot 12'
Description = 'CommScope Physical Slot 12'
SNMP index = '32'

IDPROM for pmu 2
Name = 'Container of Power Module 2'
Description = 'Container of Power Module 2'
SNMP index = '40'
```

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
auto-negotiation no auto-negotiation	Enable/Disable speed auto-negotiation.	Interface
speed (10 100 1000) speed auto	■ Speed setting (Unit: Mbps)	Interface
duplex (full-duplex half-duplex) duplex auto	■ Duplex mode setting	Interface
flowcontrol no flowcontrol	■ Turn flow-control On and Off	Interface
carrier-delay <0-60> carrier-delay msec <0-1000>	Configure Carrier-delay with the unit of second and milli second.	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 TenGigabitEthernet 7/1
Switch (config-if-TenGi7/1)# shutdown           <- disable port
Switch (config-if-TenGi7/1)no shutdown        <- enable port
Switch (config-if-TenGi7/1)#

```

Speed and duplex

The speed options supported in each interface of the C9500 series are as follows:

Type	auto-negotiation	speed	Duplex
1000Base-X	on	1000	Full
	off	1000	Full
10GBase-X	off	10000	Full

When configuring speed or duplex, note the following:

- In case of 1000Base-X, speed configuration is not available. But auto-negotiation can be configured as either on or off. When auto-negotiation is set to "on" if any one optic cable is disconnected, both end will detect the disconnection. (remote fault detection)
- If both ends support auto-negotiation, we recommend auto-negotiation. However, either end of the link does not support auto-negotiation mode then you should operate them as manual mode at both ends.

Uplink Line Speed setting

LIM-8X+ card, which takes care of uplink interface in the C9500 series system, can support either 1Gbps or 10 Gbps transmission speed. The actual speed of any port is determined by two factors; its position in a card and the optic module to be plugged in. Eight ports are available on a LIM-8X+ card but not all of them can support 1Gbps speed. Only the second half of the eight, i.e. from port #5 to #8, can.

Port	Rates available	Remark
#1 ~ #4	10 Gbps only	SFP+ type optic module should be used.
#5 ~ #8	Either 1Gbps or 10 Gbps	To make it work at 1Gbps, SFP type module should be used and relevant setting is required.

The following example shows how to configure a LIM-8X+ card to support 1Gbps operation.

```
Switch[A/L] (config) #liu10g 7 setmode ?
10g_1g           ports 1~4 are 10GE mode, ports 5~8 are 1GE mode
default_all_10g  all 8 ports are 10GE mode(default)
Switch[A/L] (config) #liu10g 7 setmode 10g_1g
```

Storm Control

Broadcast suppression refers to a function that limits broadcast traffic from flowing in the system in order to prevent the system overload caused by a 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 a 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 31 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 broadcast
Switch(config-if-Giga5/3)# storm-control multicast
Switch# show interface counters storm-control
Port          UniLvl  MullLvl  BrdLvl    UcastDiscards   McastDiscards
BcastDiscards
-----  -----  -----  -----  -----
-----  -----
Tp1/1      0       0       0       0       0       0
Tp1/2      0       0       0       0       0       0
Tp1/3      0       0       0       0       0       0
Tp1/4      0       0       0       0       0       0
Tp1/5      0       0       0       0       0       0
Tp1/6      0       0       0       0       0       0
Tp1/7      0       0       0       0       0       0
Tp1/8      0       0       0       0       0       0
Ep4/1      0       0       0       0       0       0
Ep4/2      0       0       0       0       0       0
.....
Switch#
```

To disable storm-control, use **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) which the administrator has set so that the administrator can monitor all the packets of the port.

The C9500 series can monitor RX/TX traffic from different source ports to any one port by mirroring.

Table 32 Port Mirroring

Command	Description	Mode
mirror interface IFNAME direction (receive transmit both)	Specifies the port which will be mirrored and traffic direction.	Interface
no mirror interface IFNAME direction (receive transmit)	Release the port which is mirrored	Interface

The following is an example of port mirroring.

```
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# int TenGigabitEthernet 7/1
Switch (config-if-TenGi7/1)# mirror interface Te7/2 direction
receive
Switch (config-if-TenGi7/1)# mirror interface Te7/3 direction
receive
Switch (config-if-TenGi7/1)# mirror interface Te7/4 direction
receive
Switch (config-if-TenGi7/1)# end
Switch#show mirror
Mirror Test Port Name: TenGi7/1
Mirror option: Enabled
Mirror direction: receive
Monitored Port Name: TenGi7/2
Mirror Test Port Name: TenGi7/1
Mirror option: Enabled
Mirror direction: receive
Monitored Port Name: TenGi7/3
Mirror Test Port Name: TenGi7/1
Mirror option: Enabled
Mirror direction: receive
Monitored Port Name: TenGi7/4
Switch(config)#

```



Notice

Port mirroring cannot be configured at the same time with netflow. In case netflow is enabled, mirroring should be tried only after ‘**no mls netflow**’ is executed in config mode.

Layer 2 Interface Configuration

Layer 2 is an interface that works in the Layer 2 switching mode (IEEE 802.3 Bridged VLAN). In the C9500 series, 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.

The C9500 series 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 the C9500 series are the trunk mode and the access mode.

Table 33 Layer 2 Interface mode supported in the C9500 series

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

Layer 2 Interface Defaults

The C9500 series has the following default values when a physical port or a port-group is set as Layer 2 interface:

Table 34 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 35 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 the C9500 series 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 36 Commands for Trunk port configuration

Command	Description	Mode
<code>switchport mode trunk</code>	Configures trunk mode	Interface
<code>switchport trunk native <1-4094></code>	Configures trunk port native VLAN	Interface
<code>no switchport trunk native</code>	Sets trunk port native VLAN to default	Interface
<code>switchport trunk allowed vlan add <2-4094></code>	Adds the trunk port as tagged VLAN	Interface
<code>switchport trunk remove <2-4094></code>	Removes the trunk port from the tagged VLAN	Interface
<code>switchport trunk remove all</code>		

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

```
Switch#configure terminal
Switch(config)# interface TenGigabitEthernet 7/1
Switch (config-if- TenGi7/1)# switchport mode trunk      ! trunk port set
Switch (config-if- TenGi7/1)# switchport trunk allowed vlan add 2      ! tagged vlan set
Switch (config-if- TenGi7/1)# switchport trunk native 2      ! native vlan set
Switch (config-if- TenGi7/1)# switchport trunk allowed vlan add 3      ! tagged vlan set
Switch (config-if- TenGi7/1)# switchport trunk allowed vlan add 4
Switch (config-if- TenGi7/1)# 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 mode trunk      ! trunk port set
Switch (config-if- TenGi7/1)# switchport trunk allowed vlan add 2      ! tagged vlan set
Switch (config-if-po2)# switchport trunk native 2      ! native VLAN set
Switch (config-if-po2)# switchport trunk allowed vlan add 3      ! tagged vlan set
Switch (config-if-po2)# switchport trunk allowed vlan 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 37 Commands for Access port configuration

Command	Description	Mode
<code>switchport mode access</code>	Sets to access mode	Interface
<code>switchport access VLAN <1-4094></code>	Sets native VLAN	Interface
<code>no switchport access VLAN</code>	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 TenGigabitEthernet 7/1
Switch (config-if- TenGi7/1)# switchport          ! layer2 interface set
Switch (config-if- TenGi7/1)# switchport mode access    ! access port
set
Switch (config-if- TenGi7/1)# 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 mode access      ! access port set
Switch (config-if-po2)# switchport access vlan 5    ! native vlan set
```

Port group

Overview of Port Group

Port group is used to bring together more than one physical ports into a logical group to increase bandwidth and to get the link redundancy. A port group interface in the C9500 series can be used as Layer 2 interface.

The following table shows the number of port groups available in the C9500 series by model:

Model	Number of port groups	Max. no of ports per group
C9500 Series	256	8

Port group configuration

The commands for configuring Port group are as follows:

Table 38 Port Group Configuration Commands

Command	Description	Mode
channel-group key mode on	■ Create a static port group.	Interface
no port-group ifname	Remove a port-group	config
port-channel load-balance dst-ip-port	Conduct load-balancing per destination ip and port address	Interface
port-channel load-balance dst-mac	Conduct load-balancing per destination MAC address	Interface
port-channel load-balance enhanced-hash	Conduct load-balancing based on improved hashing (RTAG7)	Interface
port-channel load-balance src-dst-mac	Conduct load-balancing per MAC address	interface
port-channel load-balance src-dst-ip	Conduct load-balancing per ip field	interface
port-channel load-balance src-dst-port	Conduct load-balancing per tcp/udp port	interface
no channel group	Remove the specified interface from the port-group.	Interface *
no interface port-channel <1-256>	Remove the specified Port group interface. Executed only when no member is present in the Port group	config
show etherchannel	Shows port group configuration	Privileged

MAC Filtering

MAC Filtering Overview

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

MAC Filtering Setting

The commands used for setting MAC filtering are given below.

Table 39 Commands for Setting MAC-filter

Command	Description	Mode
mac-filter <i>vlan-id mac-addr</i> (all-drop dst-drop trap)	■ MAC Filter add	Config
no mac-filter <i>vlan-id mac-addr</i>	■ MAC Filter delete	Config

MAC Filtering according to CPU Load

MAC Filtering according to CPU Load Overview

The C9500 series supports MAC Filtering for preset VLAN based on the CPU Load. The switch does not allow traffic for the Source MAC over the specific rate for specified time. So the abnormal activity like excessive traffic rate can be blocked in advance.

MAC Filtering according to CPU Load Setting

Table 40 CPU-MAC-FILTER related commands

Command	Description	Mode
<code>cpu-mac-filter</code>	■ Enable cpu-mac-filter function for specific vlan.	Interface
<code>cpu-mac-filter (broadcast multicast)</code>	■ Enable cpu-mac-filter function for broadcast/multicast packets of specific vlan.	Interface
<code>no cpu-mac-filter</code>	■ Disable cpu-mac-filter function for specific vlan.	Interface
<code>no cpu-mac-filter (broadcast multicast)</code>	■ Disable cpu-mac-filter function for broadcast/multicast packets of specific vlan.	Interface
<code>cpu-mac-filter cpu-load <1-99></code>	■ Set the CPU Load threshold to apply MAC-filtering.	Config
<code>no cpu-mac-filter cpu-load</code>	■ Set the CPU Load threshold to apply MAC-filtering to default.	Config
<code>cpu-mac-filter packet-threshold <1-5000></code>		Config
<code>no cpu-mac-filter packet-threshold</code>	■ Set the Threshold Rate of MAC for MAC-filtering to default.	Config
<code>cpu-mac-filter duration <1-1440></code>	■ Set the blocking duration time to apply MAC-filtering in minutes.	Config
<code>no cpu-mac-filter duration</code>	■ Set the blocking duration time for MAC-filtering to default.	Config
<code>clear cpu-mac-filter <1-4094></code>	■ Clears the Filtering information for vlan Interface in which Cpu-mac-filter is set.	Privileged
<code>show cpu-mac-filter information</code>	■ Shows the settings of Cpu-mac-filter and details of Interface.	Privileged
<code>show cpu-mac-filter table</code>	■ Shows the information on the source mac in which currently mac-filtering is applied.	Privileged

When enabling CPU-MAC-FILTERING in a specific VLAN, it works by the parameter set by the Default value. When changing this value, as described in the above table, the settings can be made in config mode for blocking duration time and packet threshold and cpu load. The settings can be checked by show cpu-mac-filter information, the information on source mac being filtered can be checked by show cpu-mac-filter table.

Traffic-control

Traffic-control Overview

This command is a measure to prevent the ingress of excessive traffic through a specific port. If the ingress traffic is more than the preset value, the traffic of the port is blocked. If the traffic is decreased down to the preset value, the mode will return to the normal mode.

Traffic-control Setting

Basic commands for setting Traffic-control are as follows.

Table 41 Commands for setting traffic-control

Command	Description	Mode
<code>traffic-control pps {all multicast unicast broadcast} {inbound outbound} <10-1400000> <10-1400000> block-mode</code>	Set the traffic amount which is allowed for either 'in' or 'out' direction by the unit of pps. If more than the set amount would flow in the port will be shut down.	Interface
<code>traffic-control pps {all multicast unicast broadcast} {inbound outbound} <10-1400000> <10-1400000> alarm-only</code>	Set the traffic amount which is allowed for either 'in' or 'out' direction by the unit of pps. If more than the set amount would flow in the port will not be shut down. Instead the system generates syslog and snmp-trap.	Interface
<code>traffic-control kbps {inbound outbound} <10-1400000> <10-1400000> block-mode</code>	Set the traffic amount which is allowed for either 'in' or 'out' direction by the unit of kbps. If more than the set amount would flow in the port will be shut down.	Interface
<code>traffic-control kbps {inbound outbound} <10-1400000> <10-1400000> alarm-only</code>	Set the traffic amount which is allowed for either 'in' or 'out' direction by the unit of kbps. If more than the set amount would flow in the port will not be shut down. Instead the system generates syslog and snmp-trap.	Interface
<code>no traffic-control</code>	Remove the traffic limit for the port.	Interface
<code>show port traffic-control</code>	Display the traffic-control information.	Privileged

Chapter 3. **VLAN**

This chapter describes the VLANs of the system.

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

This chapter covers the following subjects:

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

VLAN overview

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

VLANs have the following advantages:

Efficient Traffic Control

With traditional networks, network congestion can be caused by broadcast traffic that is transmitted to all network devices, regardless of whether they require it or not. Only 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 the network analyzer through a hub, he/she can see the network flow. In a VLAN, only the devices in the same VLAN can be seen, and the users can no longer access all the network resources just by connecting 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

The C9500 series 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, the C9500 series assigns 2 ports to each VLAN A and VLAN B, and 2 ports to VLAN C.

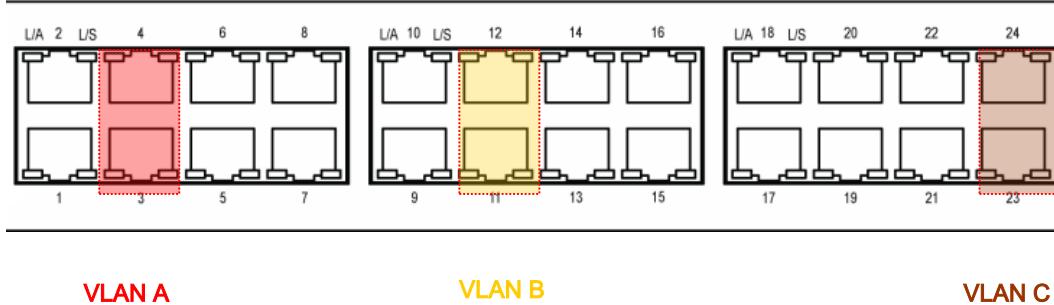


Figure 2 Example of a Port-based VLAN Configuration (the C9500 series)

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 switch 1 are assigned to VLAN A, and two ports of switch 2 are assigned to an access port of VLAN A. Two switches are connected to each other and form a single broadcast domain like the following figure.

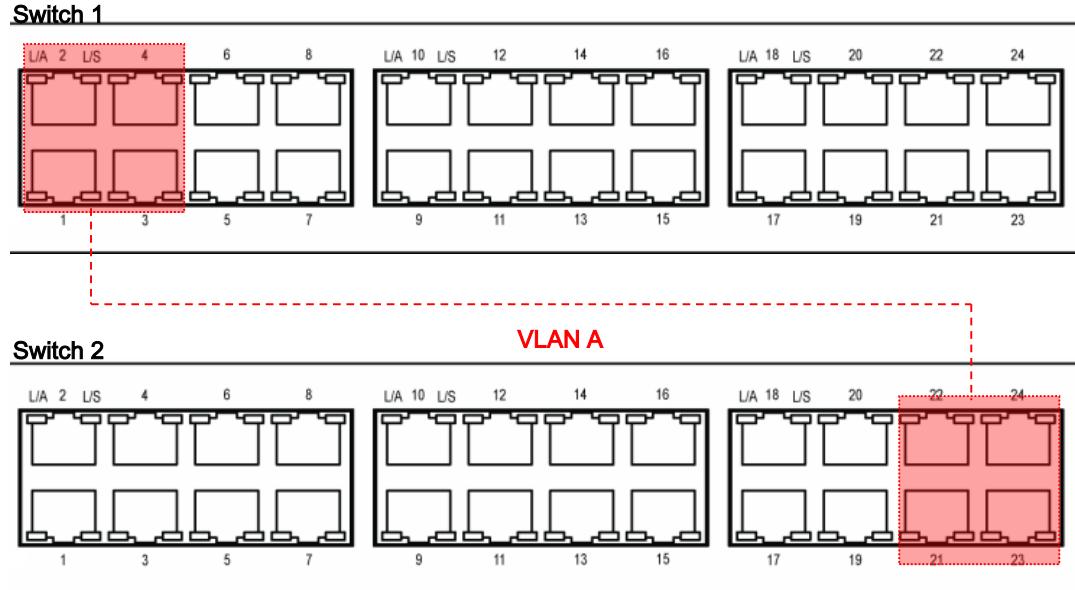


Figure 3 Single Port-based VLANs Connecting 2 Switches

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 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 switch 2 are an access port of VLAN A, and Port 9~14 are assigned as an access port of VLAN B.

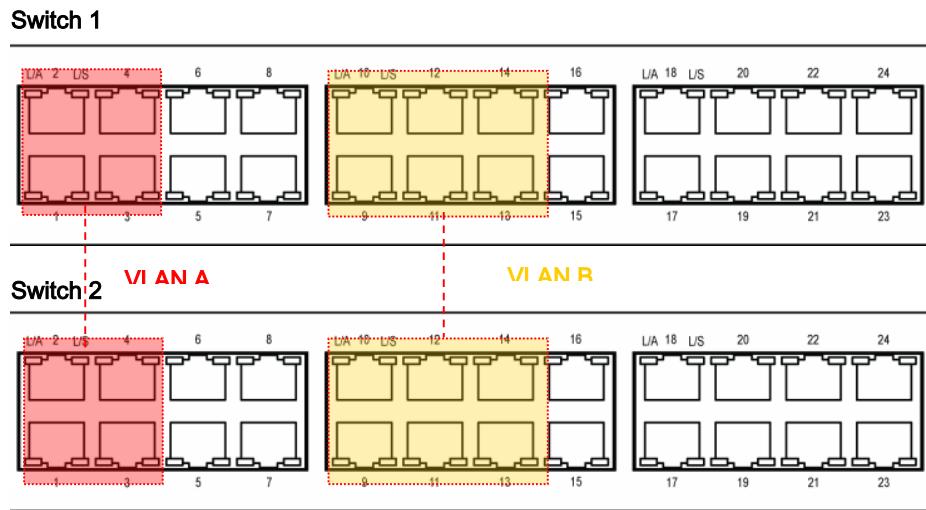


Figure 4 Two Port-based VLANs Connecting 2 Switches

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 switch 1 and switch 2 as connecting port 11 of switch 1 and port 12 of 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

Tagging a VLAN 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 the 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 a 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 a 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:

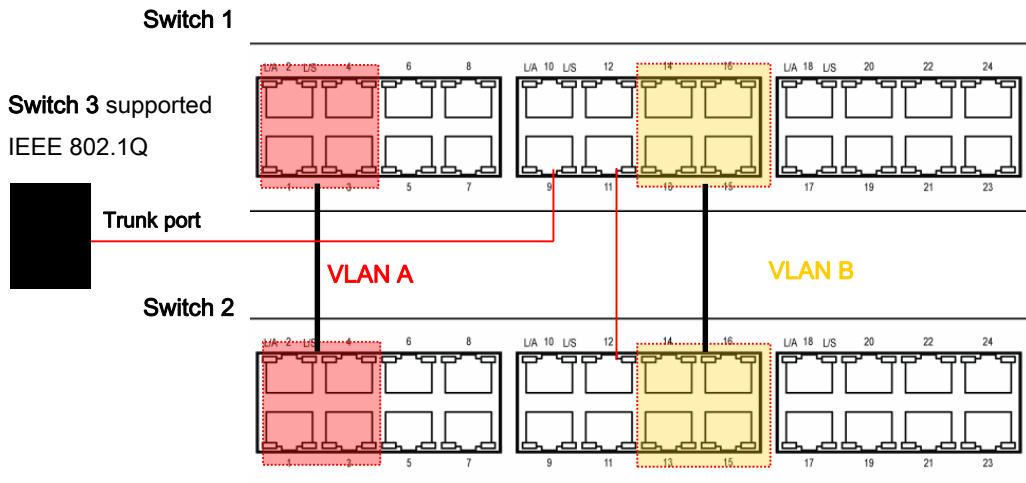


Figure 5 Physical Diagram of Tagged and Untagged Frame

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

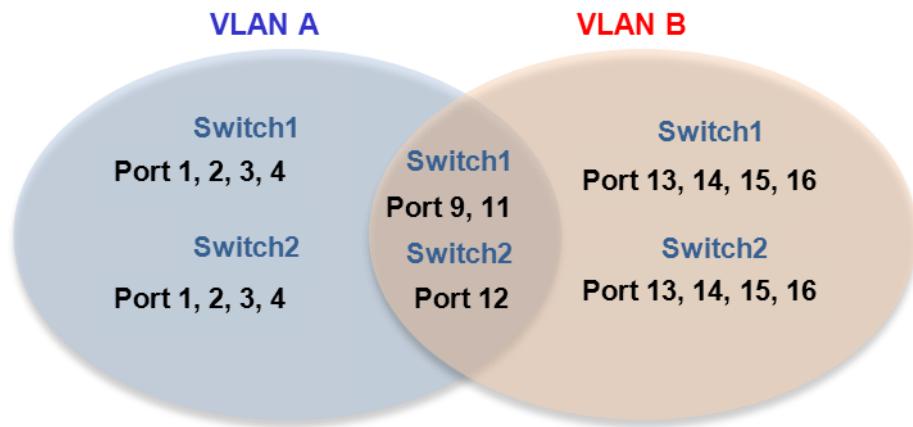


Figure 6 Logical Diagram of Tagged Frame and Untagged frame

- 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. The 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 the VLAN can be connected with the bridges or end station not supporting VLAN through cable.

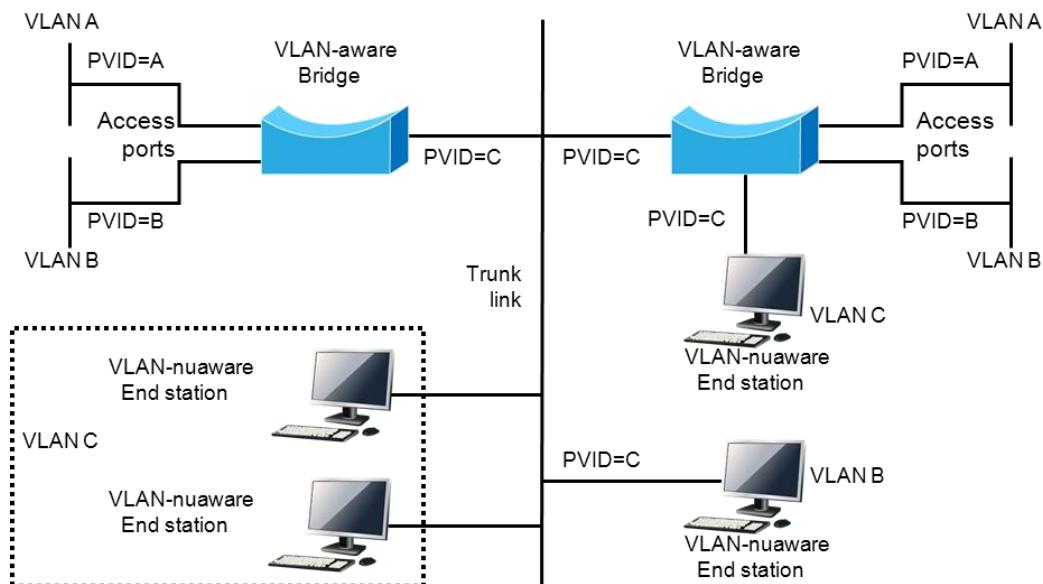


Figure 7 Native VLAN

For example, assume that two end stations not supporting the 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 the C9500 series. 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 42 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 vlan 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 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 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 a tagged VLAN and to assign trunk port. The example creates a tagged VLAN which the *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 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 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 a hybrid VLAN (Tagged, Untagged VLAN). Two ports are set to VLAN 3000 as a 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 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.

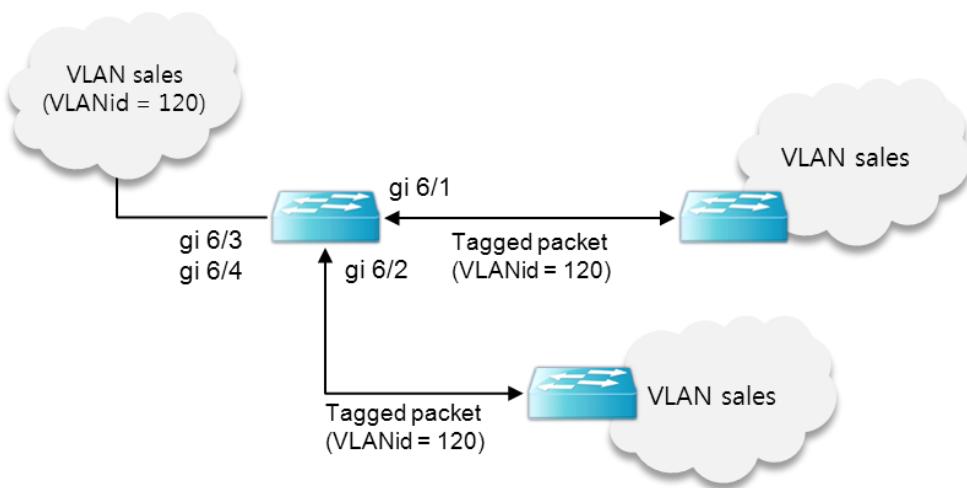


Figure 8 Configuration Example – Tagged and Untagged VLAN

```

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 43 Displaying VLAN Settings

Command	Description	Mode
show vlan	Displays VLAN information in summary: VLANid Member port VLAN belonged to bridge Spanning-tree mode	Privileged
show vlan all	Displays VLAN information as below: VLANid Member port tag, untagged	Privileged
show interface trunk (module <1-6>)	Displays VLAN information as below: Port VLAN Mode Native VLAN, Trunk VLAN	Privileged
show interface summary vlan	Displays VLAN information as below: VLAN id	Privileged

The following example shows how to display the VLAN information:

```
Switch# show vlans
VLAN Name          Status    Ports
----- -----
1     default       active   Gi6/1    Gi6/2    Gi6/3    Gi6/4
                           Gi6/5    Gi6/6    Gi6/7    Gi6/8
                           Tp10/1   Tp10/2   Tp10/3   Tp10/4
                           Tp10/5   Tp10/6   Tp10/7   Tp10/8   64
VLAN0064           active
65    VLAN0065      active
66    VLAN0066      active
67    VLAN0067      active
78    VLAN0078      active

VLAN MTU      BridgeNo BrdgMode
----- -----
1    1500        0        vlan-bridge
64   1500        0        vlan-bridge
65   1500        0        vlan-bridge
66   1500        0        vlan-bridge
67   1500        0        vlan-bridge
78   1500        0        vlan-bridge
Switch#
```

Private Edge VLAN

Private edge VLAN are 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 makes 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 the C9500 series:

- IFNAME

Specify the uplink using the port name (ex. Gi6/1, gi7/1, 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 <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 VLANID at specific interface.	Interface

The ports to be protected are ep1/1 and ep1/2, and uplink is Te7/1. Traffic between the protected ports is not allowed, but only the traffic of Te7/1 is allowed.

```
Switch# configure terminal
Switch(config)# interface ep1/1
Switch(config-if-ep1/1)# private-edge-VLAN te7/1
Switch(config-if-ep1/1)# interface ep1/2
Switch(config-if-ep1/2)# private-edge-VLAN te7/1
```

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.

The C9500 series can assign an IP configuration to the following interfaces.

- VLAN interface
- Loopback interface
- Management interface

Assigning an IP address

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

Table 45 Available IP Addresses

Class	Range	Status
A	0.0.0	Reserved
	1.0.0.0 ~ 126.0.0.0	Available
	127.0.0.0	Reserved
B	128.0.0.0 ~ 191.254.0.0 191.255.0.0	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 addresses, refer to RFC1166, Internet Number. To obtain a network number, just ask your ISP (Internet Service Provider).

The C9500 series supports multiple IP addresses per interface. The C9500 series 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. 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 this instance, 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 while in interface configuration mode:

Table 46 IP Commands for Assigning IP Address

Command	Description
ip address <i>ipaddress/prefixlen</i>	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 the ARP table, use the following commands in privilege mode. You can set Static ARP and Proxy ARP.

Table 47 Commands for ARP Configuration

Commands	Description	Mode
show arp	■ Display the entries of an ARP table.	Privileged
show arp static	■ Display the entries which have been set as static by arp command.	Privileged
clear arp-cache	■ Delete the entries of an ARP table	Privileged
Clear arp-cache interface IFNAME	■ Delete the ARP table entries for specified interface	Privileged
show arp access-list	■ Display the ARP table entries which have been registered by ACL command.	Privileged

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 48 Commands for configuring Static route path

Command	Description
<code>ip route {destination-prefix mask destination-ipaddress/mask} {gateway-ipaddress null0} [distance-value]</code>	Registers a static route. Destination-prefix: Specifies the network number of the destination-prefix destination. Mask: Specifies the mask of the 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 49 Default administrative distances of dynamic routing protocol

item	Basic Setting Value
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 the router address in a static route, the static route is deleted from the IP routing table.

To display the static route information, use the following command in the privileged mode.

Table 50 Showing IP route Information

Command	Description
<code>show ip route static</code>	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-if-vlan5)# ip address 192.10.25.1/24
```

In the following example, Subnet 1 and 2 of 131.108.0 network are separated by the backbone network. Two networks are configured as a logical network.

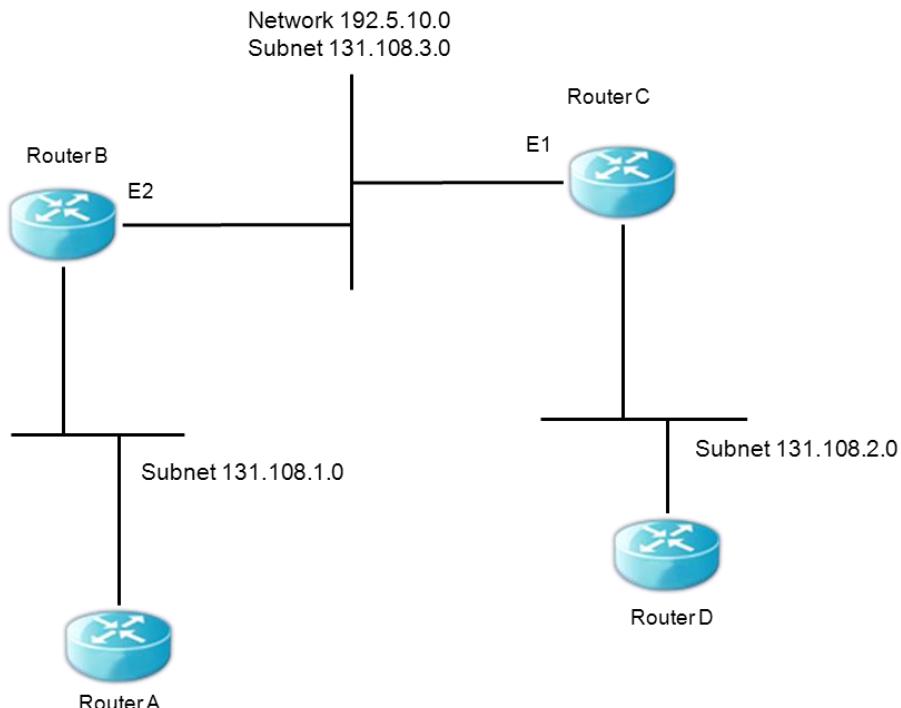


Figure 9 Network Configuration Example – multiple IP address

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 secondary
```

Router C Configuration

```
Switch(config)# interface vlan2
Switch(config-int-vlan2)# ip address 192.5.10.2/24
Switch(config-int-vlan2)# ip address 131.108.3.2/24 secondary
```

The following example is to show the contents of an ARP table

```
Switch#show arp
Protocol Address          Hardware Addr      Type      Interface    Port
```

Internet	20.0.1.1	00:07:70:9e:f0:03	dynamic	Vlan20	Port-
channel1					
Internet	21.0.1.1	00:07:70:9e:f0:03	dynamic	Vlan21	Port-
channel2					
Internet	210.1.1.254	00:07:70:9e:75:f8	dynamic	eth0	
Internet	210.1.0.254	00:07:70:9e:75:f8	dynamic	eth0	

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
Switch# show arp
```

IP Address	MAC Address	Interface	PORT	RefCnt	Flags
142.10.52.196	0010.073c.0514	vlan1	gi2	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.

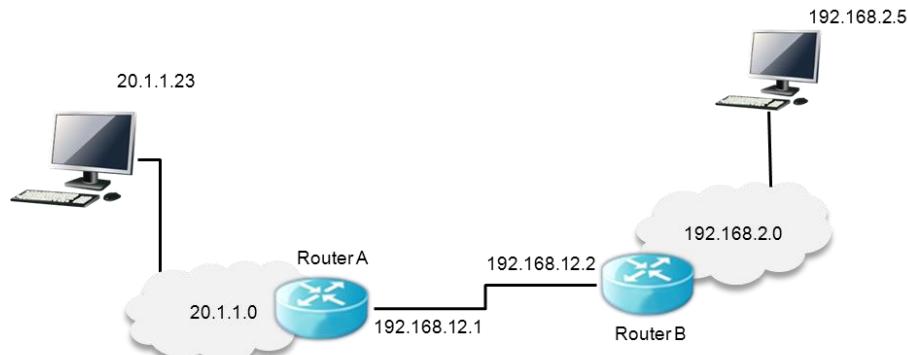


Figure 10 Network Configuration Example – Static route

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
Switch(config)#

```

Chapter 5. *DHCP*

This chapter describes the DHCP configuration of 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.

The C9500 series 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)

The C9500 series Switch 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 (the C9500 series):

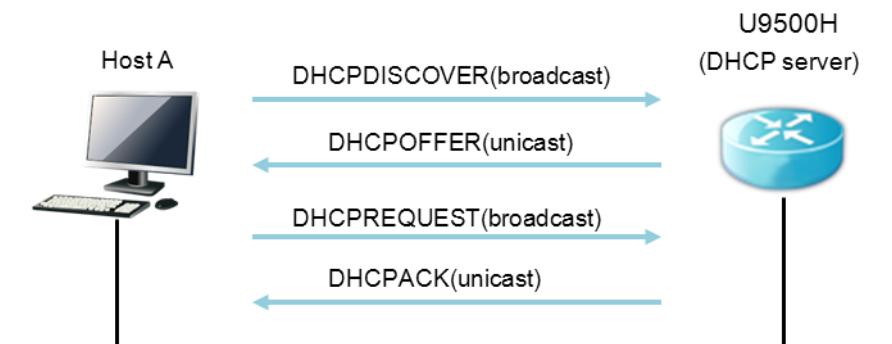


Figure 11 The C9500 series Switch as a DHCP server

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.

The C9500 series Switch as a DHCP relay agent

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

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 the C9500 series as DHCP relay agent, the DHCP client and DHCP server forwards DHCP packet to each other.

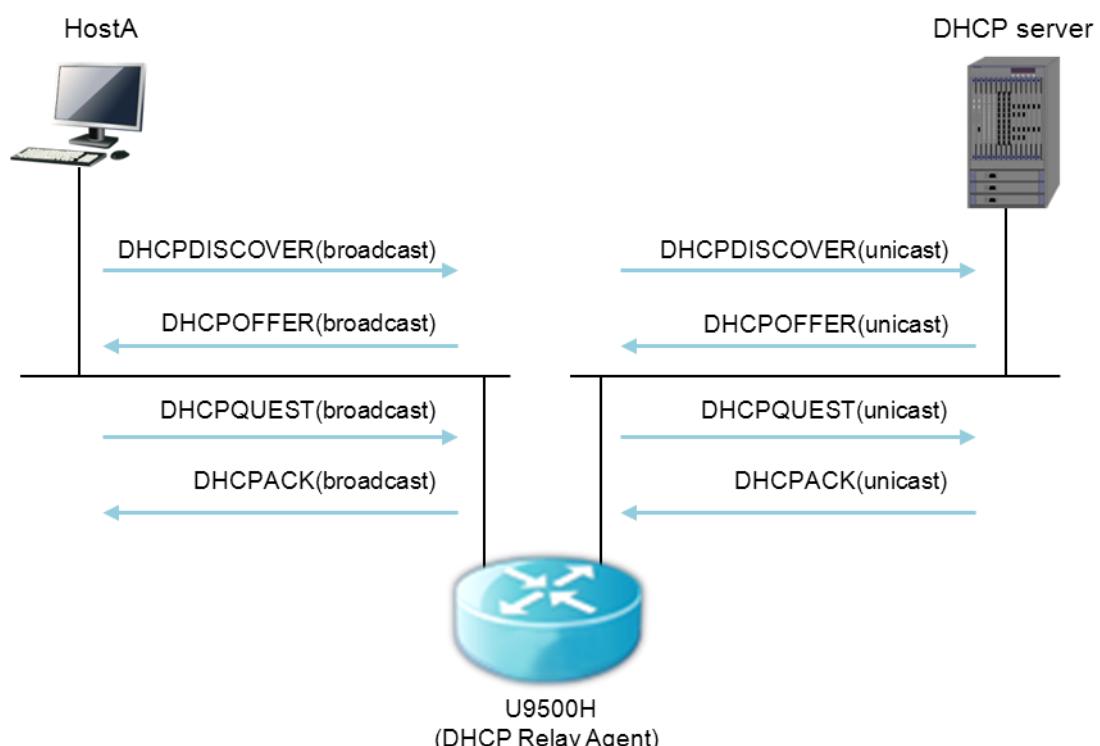


Figure 12 Transmitting DHCP server Message as a DHCP relay agent

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.

Advantages of DHCP Server

The features of the C9500 series 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.

DHCP Pool Configuration

You can configure a DHCPNetwork Pool with a name that is a symbolic string (such as “CommScope”) 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 a 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 51 IP DHCP Pool

Command	Description
ip dhcp pool <i>name</i>	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.

```
Switch# configure terminal
Switch(config)# ip dhcp pool network_pool1
Switch(dhcp-config)# exit
Switch# 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 52 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:

```
Switch# configure terminal
Switch(config)# ip dhcp pool network_pool1
Switch(dhcp-config)# network 100.0.0.0/24
Switch# 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 53 Setting IP Address Range to be assigned in Network Pool

Command	Description
range <i>lowest-address highest-address</i>	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:

```
Switch# configure terminal
Switch(config)# ip dhcp pool network_pool1
Switch(dhcp-config)# range 100.0.0.1 100.0.0.100
Switch# 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 54 Setting the Default Router for Client

Command	Description
default-router <i>address</i>	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:

```
Switch# configure terminal
Switch(config)# ip dhcp pool network_pool1
Switch(dhcp-config)# default-router 100.0.0.1
Switch(dhcp-config)# exit
Switch# 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 55 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.

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

```
Switch# configure terminal
Switch(config)# ip dhcp pool network_pool1
Switch(dhcp-config)# dns-server 200.0.0.1
Switch(dhcp-config)# exit
Switch# show running-config
. . .
!
ip dhcp pool network_pool1
dns-server 200.0.0.1
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 56 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 “CommScope.com” in a DHCP server for the client.

```
Switch# configure terminal
Switch(config)# ip dhcp pool network_pool1
Switch(dhcp-config)# domain-name CommScope.com
Switch(dhcp-config)# exit
Switch# show running-config
. . .
!
ip dhcp pool network_pool1
dns-server 200.0.0.1
domain-name CommScope.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 57 Setting Group for Network Pool

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



Notice

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

The following is an example of binding different network pools into “CommScope_pool”

```
Switch# configure terminal
Switch(config)# ip dhcp pool network_pool1
Switch(dhcp-config)# group CommScope_pool
Switch(dhcp-config)# exit
Switch# show running-config
. . .
!
ip dhcp pool network_pool1
dns-server 200.0.0.1
domain-name CommScope.com
default-router 100.0.0.1
network 100.0.0.0/24
range 100.0.0.1 100.0.0.100
group CommScope_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 58 Setting the Address Lease Time

Command	Description
lease {days hours minutes infinite}	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:

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

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.

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

The following example shows how to enable DHCP server function.

```
Switch# configure terminal
Switch(config)# service dhcp
Switch# sh running-config
!
. . .
service dhcp
. . .
!
```

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 subnet.

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 the C9500 series as DHCP relay agent, DHCP client and DHCP server forwards DHCP packet each other.

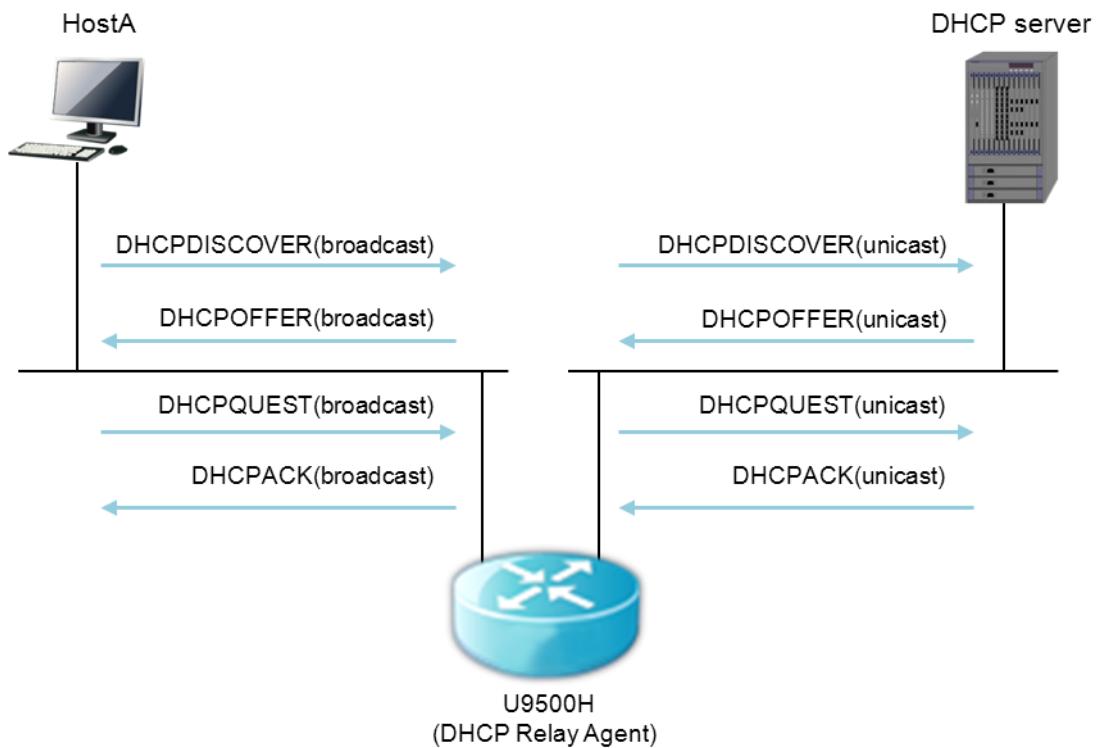


Figure 13 Message transmissions of DHCP server as a DHCP relay agent

1. DHCP client sends broadcast message, *DHCPDISCOVER*, to request an IP address.
2. DHCP relay agent receives the IP request message from DHCP client, and transfer 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 relay agent function is not enabled. To enable the DHCP relay agent, use the following command in global configuration mode:

Table 59 Enabling DHCP Server Function

Command	Description
service dhcp relay	Enables DHCP Relay function of router Use no format of this command to disable the DHCP relay.

The following example shows how to enable a DHCP relay function.

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

DHCP relay : Enabled
DHCP Smart Relay feature : Disabled
DHCP Smart Relay retry count : 3
DHCP server-id based relay : Disabled
Verification of MAC address : Enabled
Insertion of option 82 : Disabled
DHCP Option82 Management-IP : 0.0.0.0
DHCP maximum hop count : 10
Global rate-limit (per MAC) : 0/0/0

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.

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

Table 60 DHCP Server Configuration on DHCP Relay Agent

Command	Description
ip dhcp-server address	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 the C9500 series can have up to 20 helper-addresses.

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

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

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

```
Global rate-limit (per MAC) : 0/0/0
```

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

DHCP relay 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.

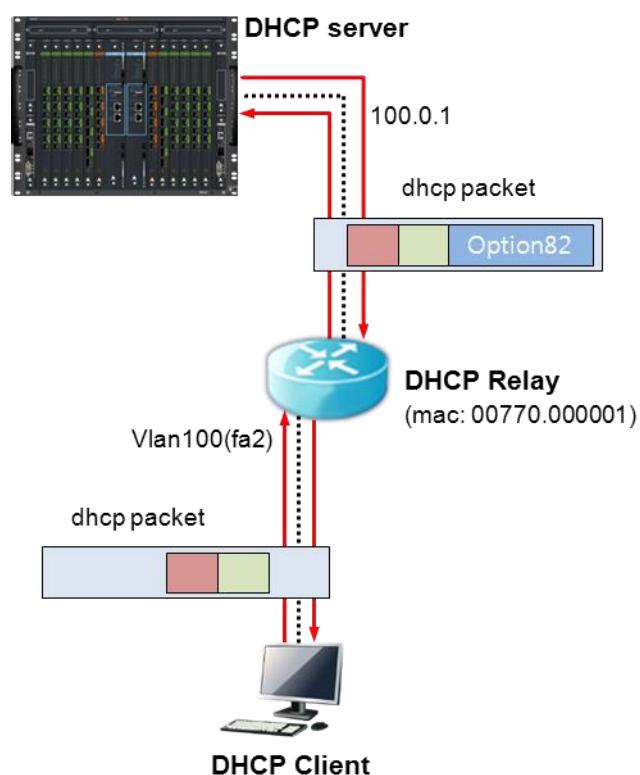


Figure 14 DHCP Relay Option82

Enabling DHCP relay information option

To enable the relay information option function of the C9500 series DHCP Relay Agent, use the following command:

Table 61 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:

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

DHCP relay : Enabled
DHCP Smart Relay feature : Disabled
DHCP Smart Relay retry count : 3
DHCP server-id based relay : Disabled
Verification of MAC address : Enabled
Insertion of option 82 : Enabled
DHCP relay information policy : replace
DHCP Option82 Management-IP : 0.0.0.0
DHCP maximum hop count : 10
Global rate-limit (per MAC) : 0/0/0

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 62 Relay agent information option reforwarding Policy Configuration

Command	Description
ip dhcp relay information policy {append keep replace}	<ul style="list-style-type: none">■ The default is set to replace.■ append: adds relay information to existing relay information■ keep: maintains the existing relay information option: and adds relay information option if no relay agent information option in router.■ replace: Replaces the relay information option in router with relay information option.

In the following example, DHCP Relay Information Option reforwarding is set to keep:

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

DHCP relay : Enabled
DHCP Smart Relay feature : Disabled
DHCP Smart Relay retry count : 3
DHCP server-id based relay : Disabled
Verification of MAC address : Enabled
Insertion of option 82 : Enabled
DHCP relay information policy : keep
DHCP Option82 Management-IP : 0.0.0.0
DHCP maximum hop count : 10
Global rate-limit (per MAC) : 0/0/0

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

DHCP Smart Relay Configuration

The system forwards the 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.

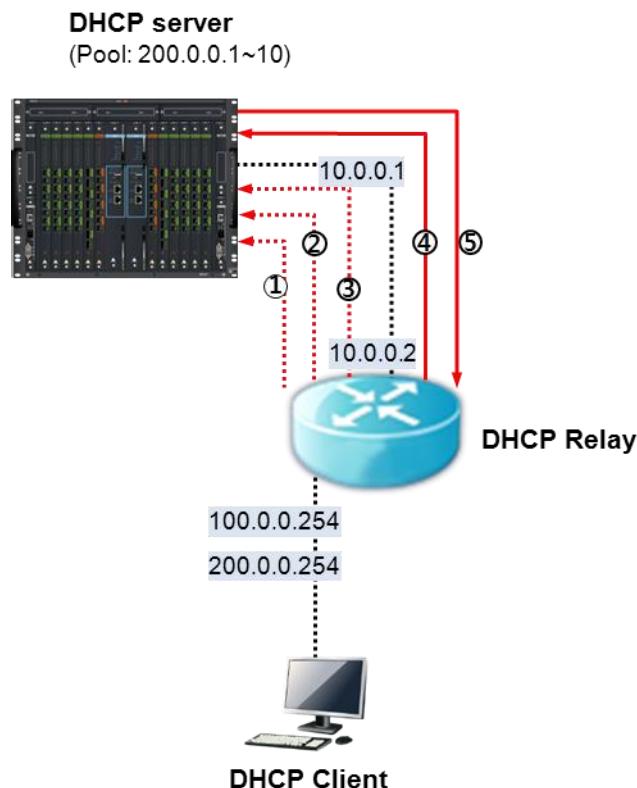


Figure 15 DHCP Smart-Relay running procedure

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

Table 63 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.

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

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

DHCP relay : Enabled
DHCP Smart Relay feature : Enabled
```

```

DHCP Smart Relay retry count : 3
DHCP server-id based relay : Disabled
Verification of MAC address : Enabled
Insertion of option 82 : Enabled
DHCP relay information policy : keep
DHCP Option82 Management-IP : 0.0.0.0
DHCP maximum hop count : 10
Global rate-limit (per MAC) : 0/0/0

DHCP helper-address is configured on following servers:
  192.168.0.254

```

DHCP Relay 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 64 DHCP Relay 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 deactivating the function of “DHCP relay agent verifies MAC-address”:

```

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

DHCP relay : Enabled
DHCP Smart Relay feature : Enabled
DHCP Smart Relay retry count : 3
DHCP server-id based relay : Disabled
Verification of MAC address : Disabled
Insertion of option 82 : Enabled
DHCP relay information policy : keep
DHCP Option82 Management-IP : 0.0.0.0
DHCP maximum hop count : 10
Global rate-limit (per MAC) : 0/0/0

DHCP helper-address is configured on following servers:
  192.168.0.254

```

DHCP relay rate-limit Set-up

In the C9500 series DHCP relay agent can control the number of DHCP Discover or DHCP Request packets by means of setting the Rate-limit, which is set for a second. The following figure shows how the C9500 series permits and drops packets as time goes when the Rate-limit is set to 30.



Figure 16 DHCP Relay Rate-limit in work

To activate DHCP Relay Rate-limit function use the commands in Global mode. DHCP Relay Rate-limit function is available per MAC address.

Command	Description
ip dhcp relay rate-limit <0-100>	Set the number of DHCP packets - Discover and Request altogether - that are allowed to pass per a second whereas all the DHCP packets are coming from an identical DHCP client. Default setting is 'Not activated' Use 'no' prefix in front of the command to deactivate the function.
ip dhcp relay rate-limit discover <0-100>	Set the number of DHCP Discover packets that are allowed to pass per a second whereas all the DHCP packets are coming from an identical DHCP client.
ip dhcp relay rate-limit request <0-100>	Set the number of DHCP Request packets that are allowed to pass per a second whereas all the DHCP packets are coming from an identical DHCP client.

The below example shows how to set DHCP Relay Rate-limit per MAC.

```
Switch# configure terminal
Switch(config)# ip dhcp relay rate-limit 30
Switch(config)# exit
Switch#
Switch# show ip dhcp relay

DHCP relay : Enabled
DHCP Smart Relay feature : Enabled
DHCP Smart Relay retry count : 3
DHCP server-id based relay : Disabled
Verification of MAC address : Disabled
Insertion of option 82 : Enabled
DHCP relay information policy : keep
DHCP Option82 Management-IP : 0.0.0.0
DHCP maximum hop count : 10
Global rate-limit (per MAC) : 30/0/0

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

Regardless of DHCP Client if you want to activate DHCP Relay Rate-limit per interface, then you may use the commands in below table in the interface mode.

Command	Description
ip dhcp relay rate-limit <0-100>	Set the number of DHCP Discover or Request packets that are allowed to pass per a second whereas all the DHCP packets are coming to this interface. Default setting is ‘Not activated’ Use ‘no’ prefix in front of the command to deactivate the function.
ip dhcp relay rate-limit discover <0-100>	Set the number of DHCP Discover packets that are allowed to pass per a second whereas all the DHCP packets are coming to this interface.
ip dhcp relay rate-limit request <0-100>	Set the number of DHCP Request packets that are allowed to pass per a second whereas all the DHCP packets are coming to this interface.

The below example shows how to set DHCP Relay Rate-limit within an Interface.

```
Switch# configure terminal
Switch(config)# interface GigabitEthernet 6/1
Switch(config-if-Giga6/1)#ip dhcp relay rate-limit 50
Switch(config-if-Giga6/1)#end
Switch#
Switch#show ip dhcp relay port rate-limit

Port name    inCount      drop      permit      configured
-----  -----  -----  -----  -----
gi6.1        0          0          0          50/0/0
```



Notice

When you set the Rate-limit for both of MAC and Interface, the received packets will be processed according to ‘Per Interface Rate-limit setting’.

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.

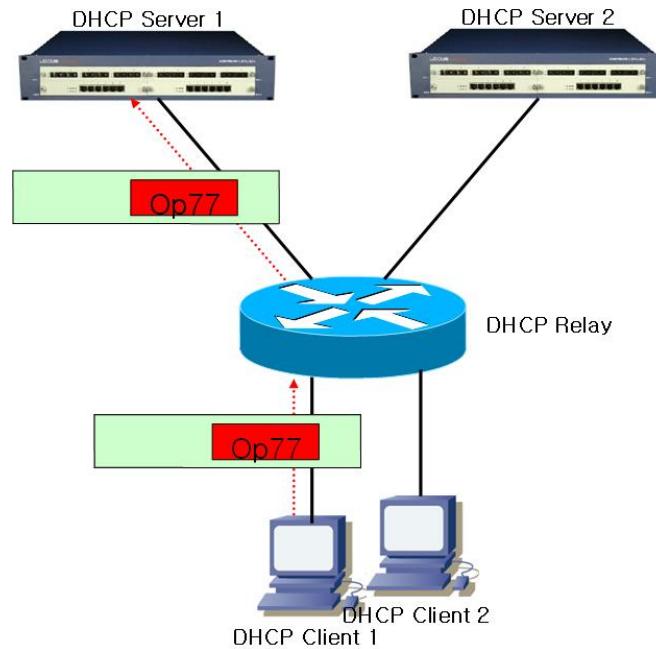


Figure 1. DHCP Class based on DHCP packet Relay

DHCP Class Configuration

To set DHCP class in the C9500 series DHCP relay agent, use the following command.

Table 65 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,



Notice

For a hexadecimal format, you must use even number of digits.

e.g.

ip dhcp option 60 hex 1 (x)

ip dhcp option 60 hex 01 (o)

The following example shows how to set "test".

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

DHCP Relay-Pool Configuration

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

Table 66 DHCP Relay-Pool Configuration

Command	Description
ip dhcp relay-pool WORD	Creates a DHCP relay-pool and enters DHCP relay-pool which is recognized as “(dhcp-pool)”. WORD: name of relay-pool delete relay-pool, use no command.
relay source A.B.C.D/M	Sets the subnetwork of relay-pool. disable the function, use no command.
class class-name	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. can assign more than one class. disable the function, use no command.
relay target A.B.C.D/M	Sets a server which will forward a DHCP DISCOVER/ REQUEST message. disable the function, use no command.

If you set “test” DHCP class and DHCP relay-pool “test-pool”, DHCP relay agent forwarding message included “CommScope” 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.

Activation of DHCP Snooping Function

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

Table 67 DHCP Snooping Function Activation

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

The following is an example of enabling DHCP Snooping function:

```
Switch# configure terminal
```

```

Switch(config)# ip dhcp snooping
Switch(config)# exit
Switch# show ip dhcp snooping
Switch DHCP Snooping is enabled
Invalid entry keep time: 14400 mins
DHCP Packet rate-limit per client: 0 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 snooped.

Table 68 DHCP Snooping VLAN Configuration

Command	Description
ip dhcp snooping VLAN VLAN_ID	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.

```

Switch# configure terminal
Switch(config)#
Switch(config)#
Switch(config)# ip dhcp snooping vlan 10
Switch(config)# exit
Switch# show ip dhcp snooping
Switch DHCP Snooping is enabled
Invalid entry keep time: 14400 mins
DHCP Packet rate-limit per client: 0 pps
Verification of hwaddr field is enabled
Insertion of option 82 is disabled
DHCP snooping is configured on following VLANs:
vlan10

```

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 the C9500 series Snooping, use the following command:

Table 69 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:

```
Switch# configure terminal
Switch(config)# ip dhcp snooping information option
Switch(config)# exit
Switch# show ip dhcp snooping
Switch DHCP Snooping is enabled
Invalid entry keep time: 14400 mins
DHCP Packet rate-limit per client: 0 pps
Verification of hwaddr field is enabled
Insertion of option 82 is enabled [replace]
DHCP snooping is configured on following VLANs:
  vlan10
```

DHCP snooping information option reforwarding policy Configuration

By default, DHCP Snooping information policy of the C9500 series drops packets with information option sent by DHCP client.

To change default policy of the C9500 series, use the following command in global mode:

Table 70 DHCP Snooping information option reforwarding policy Configuration

Command	Description
ip dhcp snooping information policy {append keep replace}	The default is set to replace. append : add new DHCP Snooping information to existing DHCP Snooping information. keep : maintain the existing DHCP Snooping information. replace : substitute the existing DHCP Snooping information with new DHCP Snooping information.

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

```
Switch# configure terminal
Switch(config)# ip dhcp snooping information policy keep
Switch(config)# exit
Switch#
Switch# show ip dhcp snooping
Switch DHCP Snooping is enabled
Invalid entry keep time: 14400 mins
DHCP Packet rate-limit per client: 0 pps
Verification of hwaddr field is enabled
Insertion of option 82 is enabled [keep]
DHCP snooping is configured on following VLANs:
  vlan10
```

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 71 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 'gi6/1' on Trust Port:

```
Switch(config)# interface GigabitEthernet 6/1
Switch(config-if-Giga6/1)# ip dhcp snooping trust
Switch(config-if-Giga6/1)# end
Switch# show ip dhcp snooping interface
Interface      Trust State   Max Entry
-----  -----  -----
Giga6/1        Trusted    20000
Giga6/2        Untrusted  20000
Giga6/3        Untrusted  20000
Giga6/4        Untrusted  20000
Giga6/5        Untrusted  20000
Giga6/6        Untrusted  20000
Giga6/7        Untrusted  20000
Giga6/8        Untrusted  20000
Switch#
```

DHCP Snooping max-entry Configuration

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

Table 72 DHCP snooping max-entry Configuration

Command	Description
ip dhcp snooping max-entry <10-10000>	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. default, each port has 10000 Max-entries.

The following example shows how to set DHCP Snooping Max-Entry of gi 6/2 with 100:

```
Switch# configure terminal
Switch(config)# interface GigabitEthernet 6/2
Switch(config-if- Giga6/2)# ip dhcp snooping max-entry 100
Switch(config-if- Giga6/2)# end
Switch# show ip dhcp snooping interface
Interface      Trust State   Max Entry
-----  -----  -----
Giga6/1        Trusted    10000
Giga6/2        Untrusted  100
Giga6/3        Untrusted  10000
Giga6/4        Untrusted  10000
Giga6/5        Untrusted  10000
Giga6/6        Untrusted  10000
Giga6/7        Untrusted  10000
Giga6/8        Untrusted  10000
Switch#
```

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 73 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 5 minutes:

```
Switch# configure terminal
Switch(config)# ip dhcp snooping entry-time
    <5-65535> Minutes
Switch(config)# ip dhcp snooping entry-time 5
Switch(config)# exit
Switch# show ip dhcp snooping
Switch DHCP Snooping is enabled
Invalid entry keep time: 5 mins
DHCP Packet rate-limit per client: 0 pps
Verification of hwaddr field is enabled
Insertion of option 82 is enabled [keep]
DHCP snooping is configured on following VLANs:
    vlan10
```

DHCP Snooping Rate-Limit Configuration

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

Table 74 DHCP Snooping Rate-Limit Configuration

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

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

```
Switch# configure terminal
Switch(config)# ip dhcp snooping rate-limit
    <1-100> DHCP Packet rate-limit in pps
Switch(config)# ip dhcp snooping rate-limit 100
Switch(config)# end
Switch#
Switch# show ip dhcp snooping
Switch DHCP Snooping is enabled
Invalid entry keep time: 14400 mins
DHCP Packet rate-limit per client: 100 pps
Verification of hwaddr field is enabled
Insertion of option 82 is enabled [keep]
DHCP snooping is configured on following VLANs:
    vlan10
```

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 75 DHCP Snooping Verify MAC-Address Configuration

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

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

```
Switch# configure terminal
Switch(config)# no ip dhcp snooping verify mac-address
Switch(config)# exit
Switch# show ip dhcp snooping
Switch DHCP Snooping is enabled
Invalid entry keep time: 5 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:
vlan10
```

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 mode:

Table 76 DHCP server Pool Information Inquiry

Command	Description
show ip dhcp pool	Shows the DHCP address pool information of the DHCP server.
show ip dhcp pool [pool_name]	Shows the DHCP address pool information of the DHCP server which has the name, pool_name.

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 mode:

Table 77 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 78 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 79 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 80 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 Server Debug command

Table 81 DHCP Server Debug command

Command	Description
debug ip dhcp server on	Enable the debugging function in DHCP Server

DHCP relay Monitoring and Control

Table 82 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 83 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 statistics; information.
show debugging ip dhcp snooping	Shows DHCP Snooping debugging.
debug ip dhcp snooping all	Enables DHCP Snooping debugging function.

DHCP Configuration Examples

This section provides examples as follows:

- DHCP network 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 CommScope.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.

```
Switch(config) # configure terminal
Switch(config) # ip dhcp pool marketing
Switch(dhcp-config) # domain-name CommScope.com
Switch(dhcp-config) # lease 1 0 0
Switch(dhcp-config) # network 192.168.1.0/24
Switch(dhcp-config) # default-router 192.168.1.1
Switch(dhcp-config) # range 192.168.1.10 192.168.1.100
Switch(dhcp-config) # 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 192.168.2.10~192.168.2.40. 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 server is set as 1.2.3.4. Each client is guaranteed up to 12 hours of IP address lease.

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



Notice

To the client who has been manually bound will be assigned same IP address all the time.

DHCP Server Monitoring and Control

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

```
Switch# show ip dhcp pool
Pool marketing :
  network: 192.168.1.0/24
  address range(s):
    add: 192.168.1.10 to 192.168.1.100
    add: 192.168.1.150 to 192.168.1.230
    lease <days:hours:minutes> <1:0:0>
    domain: CommScope.com
    no dns-servers
    default-router(s): 192.168.1.1

  Pool sales1 :
    network: 192.168.2.0/24
    address range(s):
      add: 192.168.2.10 to 192.168.2.240
      lease <days:hours:minutes> <0:12:0>
      no domain is defined
      dns-server(s): 1.2.3.4, 1.2.3.5
      default-router(s): 192.168.2.1

  Pool sales2 :
    network: 192.168.3.0/24
    address range(s):
      add: 192.168.3.10 to 192.168.3.50
      add: 192.168.3.100 to 192.168.3.230
      lease <days:hours:minutes> <0:12:0>
      no domain is defined
      dns-server(s): 1.2.3.4, 1.2.3.5
      default-router(s): 192.168.3.1
Switch#
```



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 has assigned to the client:

```
Switch# show ip dhcp binding
IP address      Hardware address      Lease expiration      Type
192.168.2.10   00:01:02:94:77:d7   Infinite           Manual
192.168.3.10   02:c7:f8:00:04:22   Infinite           Manual
total 2 bindings found
```

The following example shows the IP address that the DHCP server assigned to the client in detail:

```
Switch(Config)# show ip dhcp binding detail
-----
-----
TYPE          : Manual
IP addr       : 192.168.2.10
HW addr       : 00:01:02:94:77:d7
Client ID     : -
Host Name     : -
Lease         : Infinite
-----
-----
```

```

TYPE : Manual
IP addr : 192.168.3.10
HW addr : 02:c7:f8:00:04:22
Client ID :
Host Name :
Lease : Infinite
-----
---
total 2 bindings
found

```

The following example shows how to display the statistics of DHCP server:

```

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

Message Sent
BOOTREPLY 0
DHCP OFFER 190
DHCP ACK 172
DHCP NAK 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.

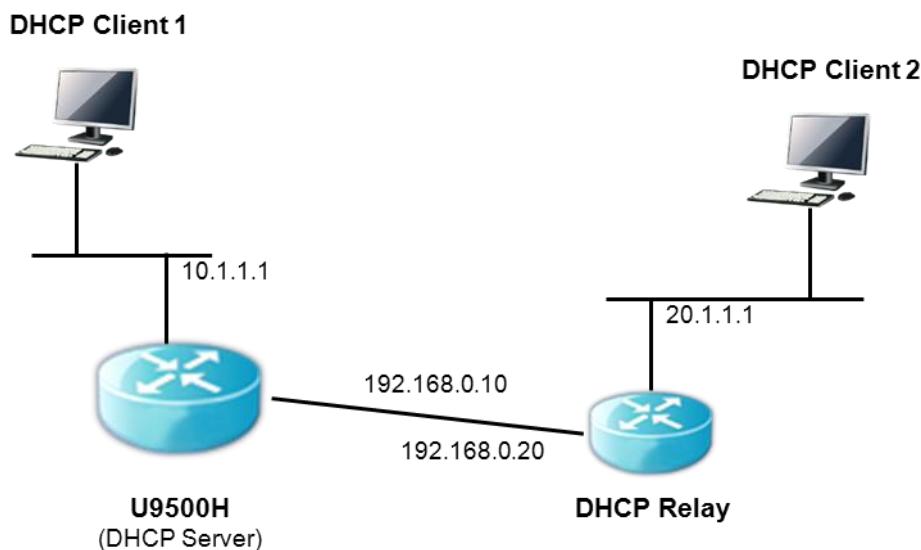


Figure 17 Network – DHCP Relay Agent Configuration

```
Switch(config)# configure terminal
Switch(config)# ip dhcp-server 10.1.1.2
Switch(config)# service dhcp relay
Switch (config)# end
Switch# show ip dhcp helper-address
Server's IP address : 10.1.1.2
Switch #
Switch # show ip dhcp relay statistics

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

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

**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.

Chapter 6. *RIP*

This chapter introduces how to set up RIP (Rounting 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 Distance
- Enabling Split Horizon

Enabling RIP

To enable RIP, do the following steps.

Table 84 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 mode

Allowing Unicast updates for RIP

As RIP is a broadcast protocol, in order to make RIP routing reach to non-broadcast network, use the following command in the router configuration mode.

Table 85 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

By this command, **passive-interface**, you can disable the transfer of Update routing information for a specific interface. To set passive interface, use the command in router configuration mode.

Table 86 Passive interface

Command or Action	Purpose
passive-interface IFNAME Example: Switch(config-router)# passive-interface gi7/1	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 87 Applying Offsets to Routing metrics

Command or Action	Purpose
offset-list access-list-name {in/out} metric IFNAME Example: Switch (router-config)# offset-list aa in 5 gi7/1	To apply offset on routing metric

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 (180 seconds)
- Garbage collection timer (120 seconds)

To adjust time value, use the following command in router configuration mode:

Table 88 Adjusting Timers

Command or Action	Purpose
timer basic update invalid holddown Example: Switch(config-router)# timer basic 30 120 120	Adjusts routing protocoltimer

Specifying a RIP Version

To make packets of a same RIP version to be available, use the following command in router configuration mode.

Table 89 Specifying a RIP Version 1

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 90 Specifying a RIP Version 2

Command or Action	Purpose
ip rip send version VERSION Example: Switch(config-if-Giga7/1)# ip rip send version 1 Switch(config-if-Giga7/1)# ip rip send version 2 Switch(config-if-Giga7/1)# ip rip send version 1 2	Sets interface to receive only RIP packets that are of the specified 'VERSION' Note Both versions of 1 and 2 are supported when they are selected.

To control the version of the packets coming into an interface, use the following command in interface configuration mode.

Table 91 Specifying a RIP Version

Command or Action	Purpose
ip rip receive version VERSION Example: Switch(config-if-Giga7/1)# ip rip receive version 1 Switch(config-if-Giga7/1)# ip rip receive version 2 Switch(config-if-Giga7/1)# 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 92 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 93 Enabling Split Horizon

Command or Action	Purpose
ip rip split-horizon [poisoned] Example: Switch(config-if-Giga7/1)# 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.

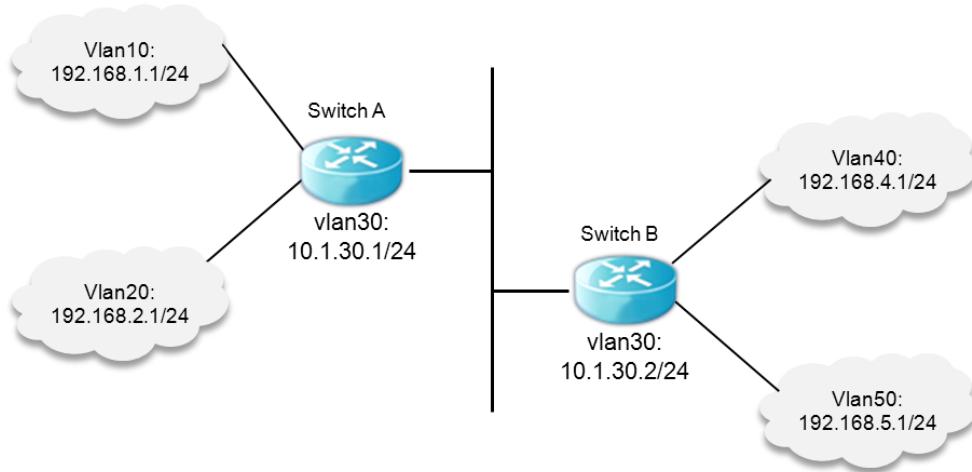


Figure 18 RIP Network Configuration Example and Diagram

Switch A	Switch B
vlan10 192.168.1.1/24	vlan30 10.1.30.2/24
vlan20 192.168.2.1/24	vlan40 192.168.4.1/24
vlan30 10.1.30.1/24	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 Set-UP

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 vlan30 of Router A, Router A receives all the paths but Router B cannot get any update of the paths that Router A sends to vlan30.

```

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 7. *OSPF*

This chapter introduces OSPF routing protocol used in the C9500 series. 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 94 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 used at the same time 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 95 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.

1. Broadcast networks (Ethernet, Token Ring, FDDI)
2. Nonbroadcast multi-access(NBMA) networks (Switched Multimegabit Data Service(SMDS), Frame Relay, X.25)
3. 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 96 OSPF network type CLI

Command	Description
Router (config-if) # ip ospf network {broadcast non-broadcast {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 97 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 98 Non broadcast network CLI

Command	Description
Router (config-router) # neighbor ip-address [priority number] [poll-interval seconds]	Connects router of Nonbroadcast network.

To identify neighbors from point-to-multipoint nonbroadcast network, use **neighbor** command in router configuration mode.

To set the interface with point-to-multipoint to the system not applied broadcast, use the following commands with order.

Table 99 Non broadcast network Configuration

Step	Command	Description
Step 1	Router (config-if) # ip ospf network point-to-multipoint non-broadcast	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 100 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 routhier 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.

OSPF not-so-stubby area (NSSA) can be found at RFC 3101 for further explanation.

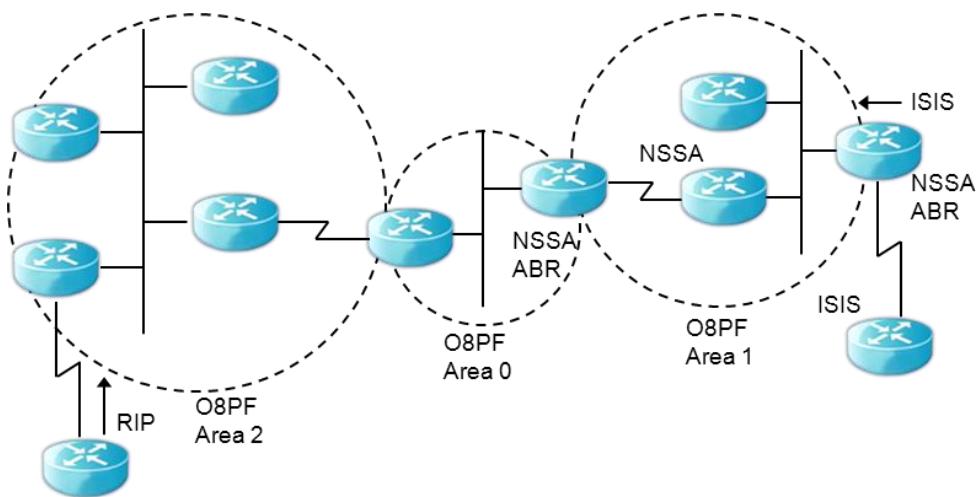


Figure 20 OSPF Network

Because NSSA is extention of stub area, Route redistributed from RIP does not flow in 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 101 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 102 OSPF area route summarization CLI

Command	Description
Router (config-router) # area area-id range ip-address mask [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 103 External Route summarization CLI

Command	Description
Router (config-router) # summary-address {ip-address/prefix} [not-advertise] [tag tag]	Sets an address including redistributed routes sent to one route.

Virtual Links

In 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 104 OSPF virtual link CLI

Command	Description
Router (config-router) # area area-id virtual-link router-id [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 Route

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 105 OSPF default route CLI

Command	Description
Router (config-router) # default-information originate [always] [metric metric-value] [metric-type type-value] [route-map map-name]	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 106 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 107 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 108 OSPF distance CLI

Command	Description
Router (config-router) # distance ospf {[inter-area dist1] [inter-area dist2] [external dist3]}	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 109 OSPF passive interface CLI

Command	Description
Router (config-router) # passive-interface interface-name	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 110 OSPF SPF timer CLI

Command	Description
Router (config-router) # timers throttle spf spf-start spf-hold spf-max-wait	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 111 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 112 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 113 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 114 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	
Router # show ip ospf [process-id] database [database-summary]	Shows OSPF database

<pre>Router # show ip ospf [process-id] database [router] [self-originate]</pre> <pre>Router # show ip ospf [process-id] database [router] [adv-router [ip-address]]</pre> <pre>Router # show ip ospf [process-id] database [router] [/link-state-id]</pre> <pre>Router # show ip ospf [process-id] database [network] [/link-state-id]</pre> <pre>Router # show ip ospf [process-id] database [summary] [/link-state-id]</pre> <pre>Router # show ip ospf [process-id] database [asbr-summary] [/link-state-id]</pre> <pre>Router # show ip ospf [process-id] database [external] [/link-state-id]</pre> <pre>Router # show ip ospf [process-id] database [nssa-external] [/link-state-id]</pre> <pre>Router # show ip ospf [process-id] database [opaque-link] [/link-state-id]</pre> <pre>Router # show ip ospf [process-id] database [opaque-area] [/link-state-id]</pre> <pre>Router # show ip ospf [process-id] database [opaque-as] [/link-state-id]</pre>	
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 115 Maintaining OSPF CLI

Command	Description

Chapter 8. *IS-IS*

This chapter introduces IS-IS (Intermediate System to Intermediate System) routing protocol.

IS-IS Overview

Intermediate System to Intermediate System (IS-IS) is a routing protocol designed to move information efficiently within a computer network, a group of physically connected computers or similar devices. It accomplishes this by determining the best route for datagrams through a packet-switched network. The protocol was defined in ISO/IEC 10589:2002 as an international standard within the Open Systems Interconnection (OSI) reference design.

IS-IS is a link-state Interior Gateway Protocol (IGP). Link-state protocols are characterized by the propagation of the information required to build a complete network connectivity map on each participating device. That map is then used to calculate the shortest path to destinations.

The IS-IS protocol was developed in the late 1980s by Digital Equipment Corporation (DEC) and was standardized by the International Standards Organization (ISO) in ISO/IEC 10589. The current version of this standard is ISO/IEC 10589:2002.

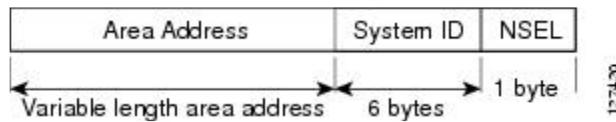
IS Address Assignment

An IS is identified by an address known as a Network Entity Title (NET). The NET is the address of a Network Service Access Point (NSAP), which identifies an instance of the IS-IS routing protocol running on an IS.

The NET may be 8 to 20 octets in length and consists of three parts:

- Area address—This field is 1 to 13 octets in length and is composed of high-order octets of the address.
- System ID—This field is 6 octets long and immediately follows the area address. When the IS operates at Level 1, the system ID must be unique among all the Level-1 devices in the same area. When the IS operates at Level 2, the system ID must be unique among all devices in the domain.
- NSEL—The N-selector field is 1 octet in length and immediately follows the system ID. It must be set to 00.

The figure below shows the format for the NET.



IS-IS PDU Types

ISs exchange routing information with their peers using protocol data units (PDUs). The following types of PDUs are used:

IIHs

Intermediate System-to-Intermediate System Hello PDUs (IIHs) are exchanged between IS neighbors on circuits on which the IS-IS protocol is enabled. IIHs include the system ID of the sender, the assigned area address(es), and the identity of neighbors on that circuit that are known to the sending IS. Additional optional information may also be included.

There are three types of IIHs:

Point-to-Point IIHs—These are sent on point-to-point circuits.

Level-1 LAN IIHs—These are sent on multiaccess circuits when the sending IS operates as a Level-1 device on that circuit.

Level-2 LAN IIHs—These are sent on multiaccess circuits when the sending IS operates as a Level-2 device on that circuit.

LSPs

An IS generates Link-State PDUs (LSPs) to advertise its neighbors and the destination that are directly connected to the IS. An LSP is uniquely identified by the following:

- System ID of the IS that generated the LSP
- Pseudonode ID—This value is always 0 except when the LSP is a pseudonode LSP (see “Operation of IS-IS on Multiaccess Circuits” section).
- LSP number (0 to 255)
- 32-bit sequence number

Whenever a new version of an LSP is generated, the sequence number is incremented.

Level-1 LSPs are generated by ISs that support Level 1. The Level-1 LSPs are flooded throughout the Level-1 area. The set of Level-1 LSPs generated by all Level-1 ISs in an area is the Level-1 LSP Database (LSPDB). All Level-1 ISs in an area will have an identical Level-1 LSPDB and will therefore have an identical network connectivity map for the area.

Level-2 LSPs are generated by ISs that support Level 2. Level-2 LSPs are flooded throughout the Level-2 subdomain. The set of Level-2 LSPs generated by all Level-2 ISs in the domain is the Level-2 LSP Database (LSPDB). All Level-2 ISs will have an identical Level-2 LSPDB and will therefore have an identical connectivity map for the Level-2 subdomain.

SNPs

Sequence Number PDUs (SNPs) contain a summary description of one or more LSPs. There are two types of SNPs for both Level 1 and Level 2:

Complete Sequence Number PDUs (CSNPs) are used to send a summary of the LSPDB that an IS has for a given level.

Partial Sequence Number PDUs (PSNPs) are used to send a summary of a subset of the LSPs for a given level that an IS either has in its database or needs to obtain.

LSPDB Synchronization

Proper operation of IS-IS requires a reliable and efficient process to synchronize the LSPDBs on each IS. In IS-IS this process is called the update process. This section provides a brief overview of the operation of the update process. The update process operates independently at each supported level.

LSPs may be locally generated, in which case they always are new LSPs. LSPs may also be received from a neighbor on a circuit, in which case they may be generated by some other IS or may be a copy of an LSP generated by the local IS. Received LSPs may be older, the same age, or newer than the current contents of the local LSPDB.

Handling of Newer LSPs

A newer LSP is added to the local LSPDB. If an older copy of the same LSP currently exists in the LSPDB, it is replaced. The newer LSP is marked to be sent on all circuits on which the IS currently has an adjacency in the UP state at the level associated with the newer LSP—excluding the circuit on which the newer LSP was received.

On point-to-point circuits, the newer LSP will be flooded periodically until the neighbor acknowledges its receipt by sending a PSNP or by sending an LSP that is the same or newer than the LSP being flooded.

On multiaccess circuits, the IS will flood the newer LSP once. The IS examines the set of CSNPs that are sent periodically by the DIS for the multiaccess circuit. If the local LSPDB contains one or more LSPs that are newer than what is described in the CSNP set (this includes LSPs that are absent from the CSNP set) those LSPs are reflooded over the multiaccess circuit. If the local LSPDB contains one or more LSPs that are older than what is described in the CSNP set (this includes LSPs described in the CSNP set that are absent from the local LSPDB), a PSNP is sent on the multiaccess circuit with descriptions of the LSPs that require updating. The DIS for the multiaccess circuit responds by sending the requested LSPs.

Handling of Older LSPs

An IS may receive an LSP that is older than the copy in the local LSPDB. An IS may receive an SNP (complete or partial) that describes an LSP that is older than the copy in the local LSPDB. In both cases the IS marks the LSP in the local database to be flooded on the circuit on which the older LSP or SNP that contained the older LSP was received.

At this point, the actions taken are identical to the actions that are described in the “Handling of Newer LSPs” section after a new LSP has been added to the local database.

Handling LSPs That Are the Same

Because of the distributed nature of the update process, it is possible than an IS may receive copies of an LSP that is the same as the current contents of the local LSPDB.

On a point-to-point circuit, receipt of such an LSP is ignored. Periodic transmission of a CSNP set by the DIS for that circuit will serve as an implicit acknowledgement to the sender that the LSP has been received.

In a multiaccess circuit, receipt of such an LSP is ignored. Periodic transmission of a CSNP set by the DIS for that circuit will serve as an implicit acknowledgement to the sender that the LSP has been received.

The figure below shows how the LSPs are used to create a network map. Imagine the network topology as a jigsaw puzzle. Each LSP (representing an IS) is considered one of the jigsaw pieces.

Shortest Path Calculation

When the contents of the LSPDB change, each IS independently reruns a shortest path calculation. The algorithm is based on the well-known Dijkstra algorithm for finding the shortest paths along a directed graph where the ISs are the vertices of the graph and the links between the ISs are edges with a nonnegative weight. A two-way connectivity check is performed before considering a link between two ISs as part of the graph. This prevents the use of stale information in the LSPDB, for example, when one IS is no longer operating in the network but did not purge the set of LSPs that it generated before ceasing operation.

The output of the SPF is a set of tuples (destination, next hop). The destinations are protocol-specific; for example, they would be prefixes when the supported protocol is IP. Multiple equal-cost paths are supported, in which case multiple next hops would be associated with the same destination.

Independent SPFs are performed for each level supported by the IS. In cases in which the same destination is reachable by both Level-1 and Level-2 paths, the Level-1 path is preferred.

A Level-2 IS that indicates that it has one or more Level-2 neighbors in other areas may be used by Level-1 devices in the same area as the path of last resort, also called the default route. The Level-2 IS indicates its attachment to other areas by setting an attached bit (ATT) in its Level-1 LSP 0.

Route Redistribution

Devices are allowed to redistribute external prefixes, or routes, that are learned from any other routing protocol, static configuration, or connected interfaces. The redistributed routes are allowed in either a Level 1 device or a Level 2 device. Level 2 routes injected as Level 1 routes is called route leaking.

IS-IS Configuration

Enabling IS-IS as an IP Routing Protocol on the Device

IS-IS must be enabled to use IS-IS routing protocol. Complete the following procedures. After enabling IS-IS, use the following commands to manage protocol according to the requirements and needs.

Command	Description
router isis area-tag Example: Switch(config)# router isis TEST	Assigns a tag to an IS-IS process. Enters router configuration mode. Configure tags to identify multiple IS-IS processes by giving a meaningful name for each routing process. If the tag is not specified, a null tag (0) is assumed and the process is referenced with a null tag. The tag name must be unique among all IP router processes for the device.
net network-entity-title Example: Switch(config-router)# net 49.0001.0000.0000.000b.00	Configures the NET on the device. The NET identifies the device for IS-IS.

IS-IS interface parameters

To configure IS-IS, perform the tasks described in the following sections. The tasks in the first section are required; the tasks in the remaining sections are optional:

Command	Description
Switch(config-if-vlanid)# ip router isis process-tag	Configures an IS-IS routing process for IP Service on an interface and attaches an area designator to the routing process
Switch(config-if-vlanid)# isis metric <1-63> {level-1 level-2}	Configures the metric (or cost) for the specified interface.
Switch(config-if-vlanid)# isis hello-interval {<1-65535> minimal} {level-1 level-2}	Specifies the length of time (in seconds) between hello packets
Switch(config-if-vlanid)# isis csnp-interval <1-65535> {level-1 level-2}	Configures the IS-IS CSNP interval for the specified interface.
Switch(config-if-vlanid)# isis retransmit-interval <0-65535>	Configures the number of seconds between retransmission of IS-IS LSPs for point-to-point links.
Switch(config-if-vlanid)# isis lsp-interval milliseconds	Configures the IS-IS LSP retransmission throttle interval.
Switch(config-if-vlanid)# isis hello-multiplier multiplier-value {level-1 level-2}	Sets the hello multiplier.
Switch(config-if-vlanid)# isis priority priority-value {level-1 level-2}	Configures the priority to use for designated router election.
Switch(config-if-vlanid)# isis circuit-type {level-1 level-1-2 level-2-only}	Configures the type of adjacency desired for neighbors on the specified interface (the interface circuit type).
Switch(config-if-vlanid)# isis password password {level-1 level-2}	Configures the authentication password for a specified interface.

IS-IS Network type

IS-IS supports two generic network types:

- Point-to-point: A point-to-point circuit has exactly two ISs on the circuit. An IS forms a single adjacency to the other IS on the point-to-point circuit. The adjacency type describes what level(s) are supported on that circuit.
- Multiaccess: Multiaccess circuits support multiple ISs; for example, two or more operating on the circuit. The ability to address multiple systems utilizing a multicast or broadcast address is assumed.

Command	Description
Syntax: isis network {broadcast point-to-point}	Sets IS-IS network type of IS-IS interface.

Specifying the System Type

You can configure the router to act as a Level 1 (intra-area) router, as both a Level 1 router and a Level 2 (interarea) router, or as an interarea router only.

Command	Description
Switch(config-router)# is-type {level-1 level-1-2 level-2-only}	Configures the system type (area or backbone router).

Tuning LSP Interval and Lifetime

By default, the router sends a periodic LSP refresh every 15 minutes. LSPs remain in a database for 20 minutes by default. If they are not refreshed by that time, they are deleted. You can change the LSP refresh interval or the LSP lifetime. The LSP interval should be less than the LSP lifetime or else LSPs will time out before they are refreshed. The software will adjust the LSP refresh interval if necessary to prevent the LSPs from timing out.

Command	Description
Switch(config-router)# lsp-refresh-interval seconds	Sets the LSP refresh interval.
Switch(config-router)# max-lsp-lifetime seconds	Sets the maximum time that link-state packets (LSPs) can remain in a router's database without being refreshed.

Throttling of IS-IS LSP Generation, SPF Calculation, and PRC Works

IS-IS throttling of LSP generation, SPF calculations, and PRC occurs by default. You can customize the throttling of these events with the **lsp-gen-interval**, **spf-interval**, and **prc-interval** commands, respectively. The arguments in each command behave similarly. For each command:

- The first argument indicates the maximum number of seconds between LSP generations or calculations.
- The second argument indicates the initial wait time (in milliseconds) before running the first LSP generation or calculation.
- The third argument indicates the minimum amount of time to wait (in milliseconds) between the first and second LSP generation or calculation. (In addition to this wait time, there might be some other system overhead between LSP generations or calculations.)

Command	Description
Switch(config-router)# lsp-gen-interval {level-1 level-2 seconds}	Sets IS-IS LSP generation throttling timers. • The default lsp-max-wait interval is 5 seconds.

	<ul style="list-style-type: none"> The default lsp-initial-wait interval is 50 milliseconds. The default lsp-second-wait interval is 5000 milliseconds.
Switch(config-router)# spf-interval {level-1 level-2} spf-max-wait spf-initial-wait spf-second-wait	<ul style="list-style-type: none"> Sets IS-IS SPF throttling timers. The default spf-max-wait interval is 10 seconds. The default spf-initial-wait interval is 5000 milliseconds. The default spf-second-wait interval is 5000 milliseconds.
Switch(config-router)# prc-interval-exp <0-2147483647>	<ul style="list-style-type: none"> Sets IS-IS partial route computation throttling timers. The default prc-max-wait interval is 10 seconds. The default prc-initial-wait interval is 2000 milliseconds. The default prc-second-wait interval is 5000 milliseconds.

Generating a Default Route

You can force a default route into an IS-IS routing domain. Whenever you specifically configure redistribution of routes into an IS-IS routing domain.

Command	Description
Switch(config-router)# default-information originate	Forces a default route into the IS-IS routing domain.

Summarizing Address Ranges

You can create aggregate addresses that are represented in the routing table by a summary address. This process is called route summarization. One summary address can include multiple groups of addresses for a given level. Routes learned from other routing protocols also can be summarized. The metric used to advertise the summary is the smallest metric of all the more-specific routes

Command	Description
Switch(config-router)# summary-address <i>ip-address/prefix</i> {level-1 level-1-2 level-2 metric}	Creates a summary of addresses for a given level.

Passive-interface

A passive interface in IS-IS is one which does not send or receive IS-IS routing traffic. The network for the interface is still included in LSPs generated by the router.

Command	Description
Switch(config-router)# passive-interface <i>IFNAME</i>	Suppress/unsuppress IS-IS packets from being sent or received over the specified interface.

ISIS 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.

Each route source has a default administrative distance. The default administrative distance for IS-IS is 115.

Command	Description
Switch(config-router)# distance <1-255>	To change the administrative distance for IPv4 IS-IS routes

Administrative Tag

An administrator associates an Administrative Tag value with some interesting property. When IS-IS advertises reachability for some IP prefix that has that property, it adds the Administrative Tag to the IP reachability information TLV for that prefix, and the tag "sticks" to the prefix as it is flooded throughout the routing domain.

Command	Description
Switch(config-if -vlandid)# isis tag tag-value	Sets the Tag value on ISIS LSP

Monitoring IS-IS

To monitor the IS-IS tables and databases, use the following commands in EXEC mode

Command	Description
show ip protocols Example: Switch# show ip protocols	Displays the parameters and current state of the active routing protocol process. You can use this command to learn what protocols are active, what interfaces they are active on, what networks they are routing for, and other parameters that relate to the routing protocols.
show isis area-tag database {level-1 level-2 I1 I2 detail} Example: Switch# show isis database detail	Displays additional information about the IS-IS database. Displays the link-state database for Level-1 and Level-2, the contents for each LSP, and the link-state protocol PDU identifier.
show isis database verbose Example: Switch# show isis database verbose	Displays additional information about the IS-IS database such as the sequence number, checksum, and holdtime for LSPs.
show isis area-tag topology Example: Switch# show isis topology	Displays a list of all connected routers in all areas.
show isis area-tag neighbors detail Example: Switch# show isis neighbors detail	Displays IS-IS adjacency information. The show isis neighbor detail command output verifies that the right adjacencies have established. A matrix of adjacencies should be prepared before you configure your routers, showing what neighbors should be expected in the adjacencies table, to facilitate verification.

show isis interface brief IFNAME Example: Switch# show isis interface brief	Display status information about Intermediate System-to-Intermediate System (IS-IS)-enabled interfaces.
--	---

Chapter 9. *BGP*

This chapter introduces BGP among available IP Unicast routing protocols of the C9500 series.

BGP Configuration

BGP is a protocol that receives/sends routing information among Management Domains (Autonomous System: AS), and manages routing between domains unlike RIP and OSPF. The C9500 series support BGP-4.

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 <1-4294967295>
```

The last number in the AS number, which is Autonomous System number given by network operator to distinguish BGP networks.

2. Specify 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.

- Filtering
- BGP Attribute Configuration
- Routing policy Modification
- Other functions

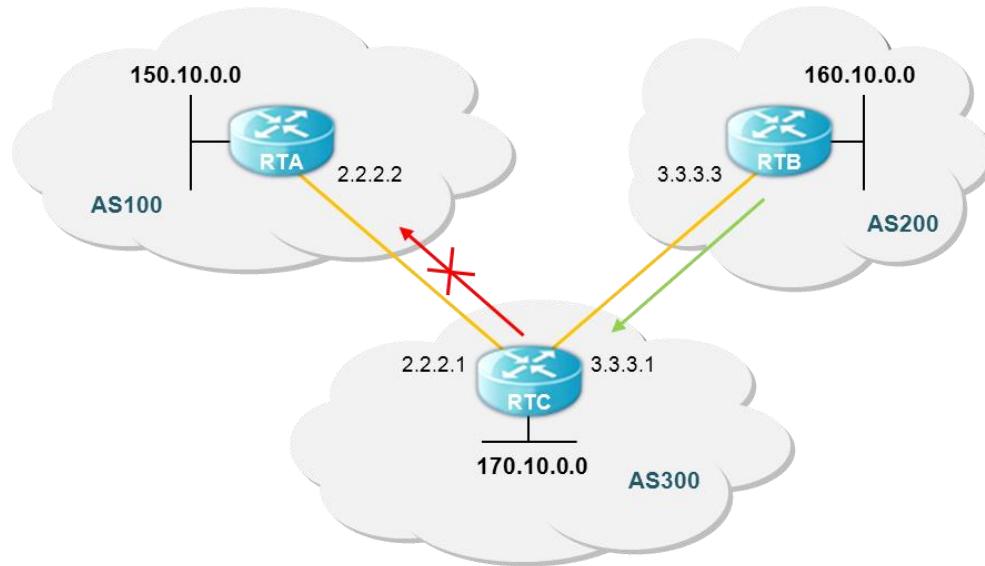
BGP Filtering

BGP updated 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 a router receives or advertises, it filters BGP based on routing updates going/coming to the specific neighbor. The specific Access-list is applied to the Input/Output update to the specific neighbor with the following command.

```
neighbor {ip-address|peer-group-name} distribute-list access-list-number {in|out}
```



RTB generates network 160.10.0.0 and transmits this information to RTC. If RTC does not transmit it to AS 100, apply Access-list and connection to RTA to filter the information update.

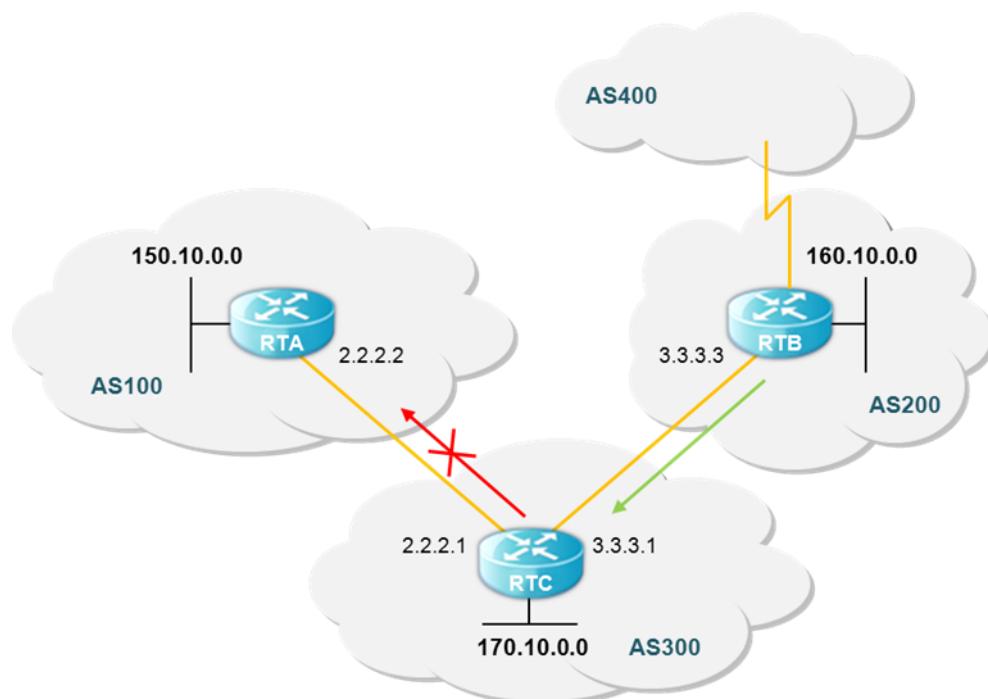
The following shows the construction of the operation.

```
/*-- 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}
```

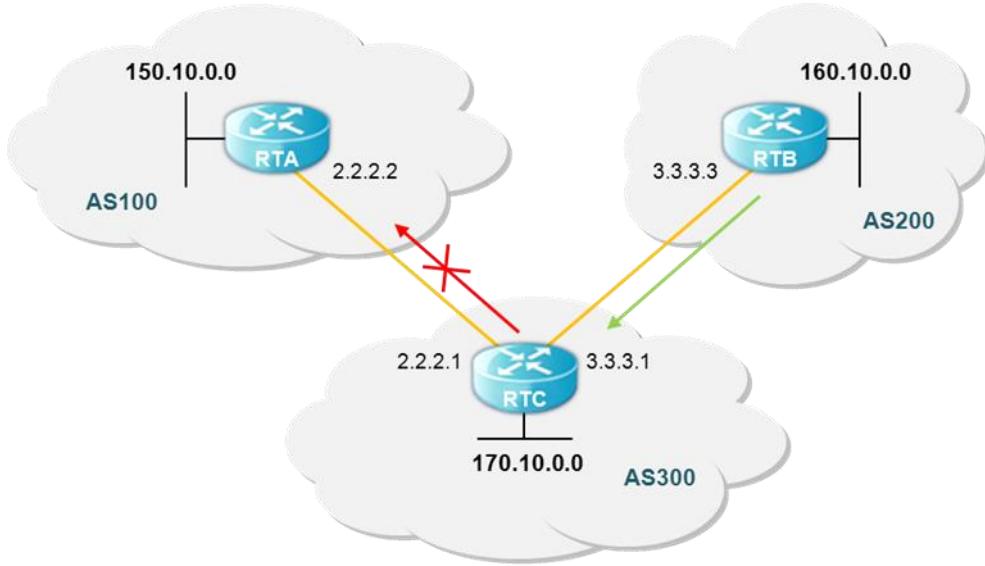


The following shows the configuration that RTC updates 160.10.0.0 to RTA with the Path Filtering.

```
/*-- 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



As in the figure above, RTC 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 community group which are used Match command for Route Map 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 and 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
!
```

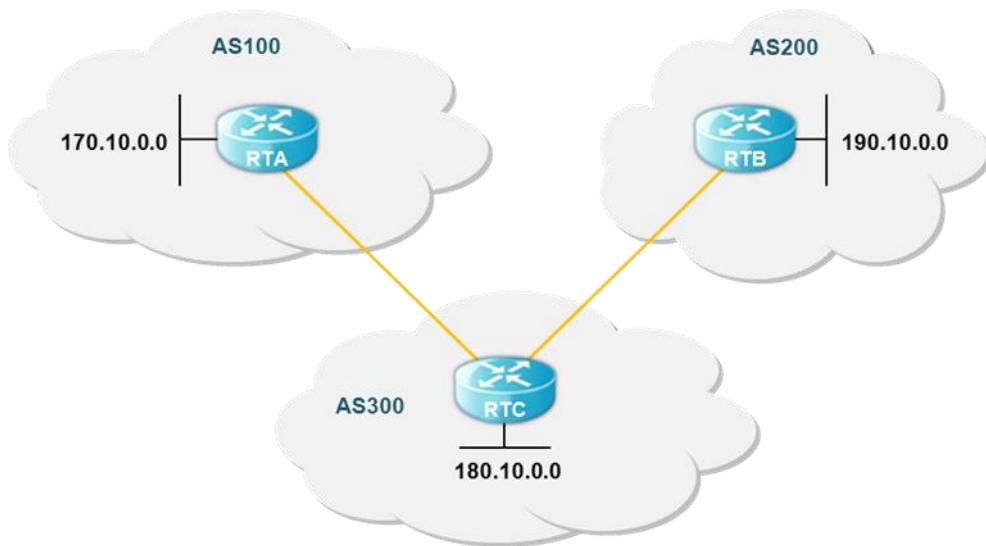
The route with the community attribute 100 is matched with List 1 and weight is set as 20. The route with the community attribute 200 is matched with List 2 and Weight is set as 10. The keyword “exact” shows that there should not be other values if community should have community 200. The last community 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



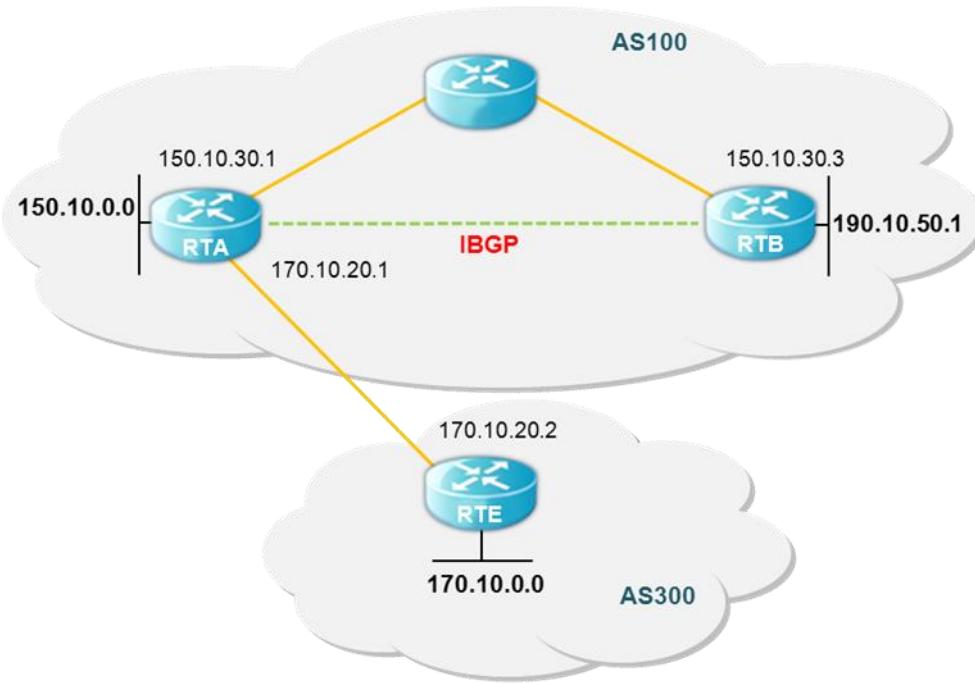
When one route passes one AS, the AS number is added to the update of route.

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 received through BGP and displayed as “e” in the BGP table.
- **INCOMPLETE:** NLRI is unknown or received through various ways. This is used when the static route is redistributed to BGP and displayed “?” in the BGP table.



```

/*-- 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:

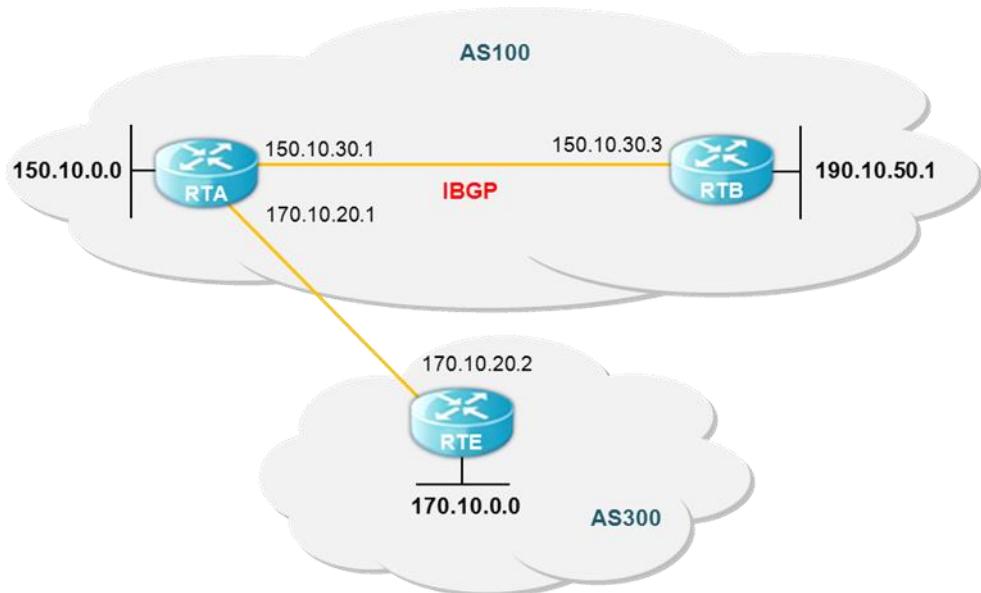
- RTA gets to 170.10.0.0 through 300i.
(The next AS pass is 300 and the route origin is IGP.)

- RTA gets to 190.10.50.0 through 100i.
(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.

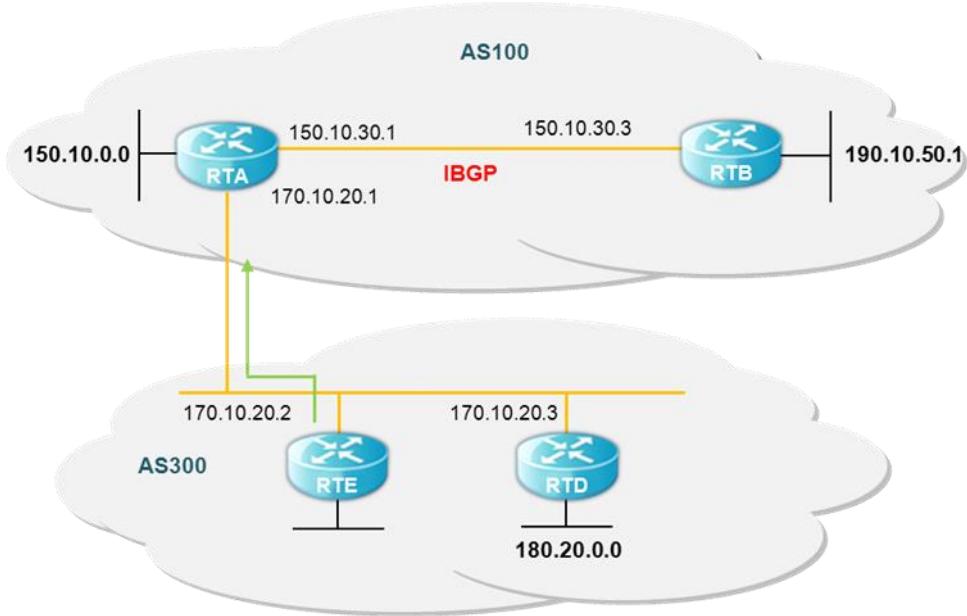


```
/*-- RTA --*/
!
router bgp 100
network 150.10.0.0
neighbor 170.10.20.2 remote-as 300
neighbor 150.10.30.3 remote-as 100
!
/*-- RTB --*/
!
router bgp 100
neighbor 150.10.30.1 remote-as 100
!
/*-- RTC --*/
!
router bgp 300
network 170.10.0.0
neighbor 170.10.20.1 remote-as 100
!
```

- 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.

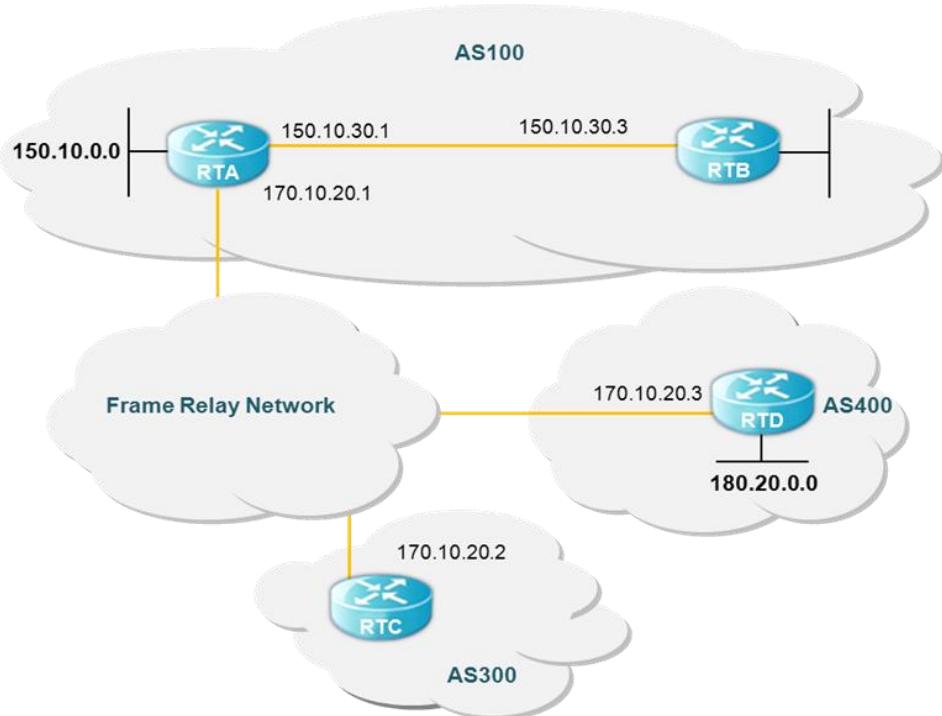
The following shows you should be careful in the multi access network and NBMA network.

BGP Nexthop (Multiple access networks)



RTE connects RTA and EBGP. RTE gets 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, RTE, 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.

BGP Nexthop (NBMA) - the common media among RTA, RTC, and RTD, causes more complicated problems.



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
!
```

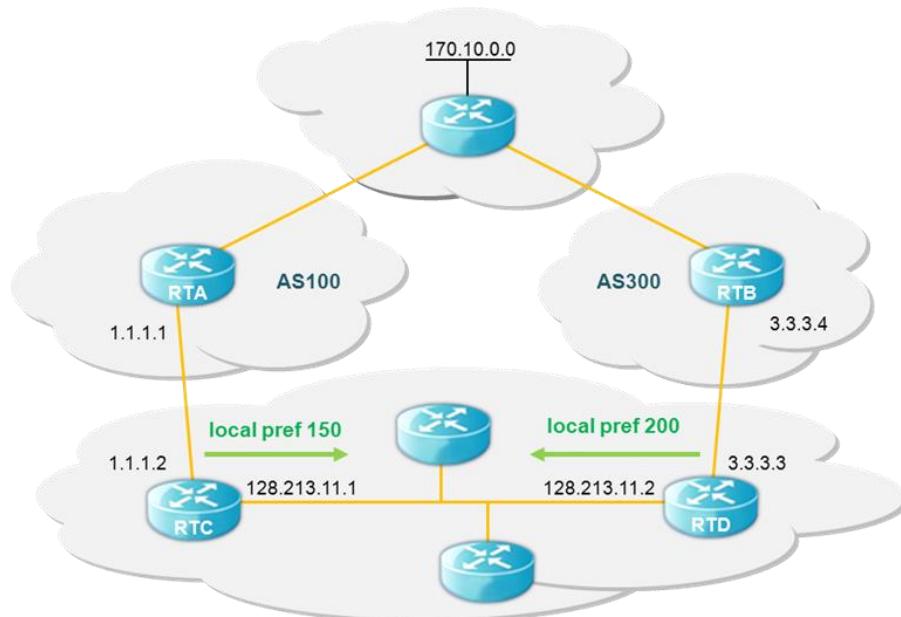
RTC transmits 180.20.0.0 to nextHop, 170.10.20.2.

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.

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 300 update, 150 for AS 150.



```
/*-- 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 asa 200. RTC and RTD recognized that the network 170.10.0.0 information from AS300 has the higher local preference than one from AS100. So, all traffic of AS256 assigned as 170.10.0.0 is transmitted to RTD.

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.

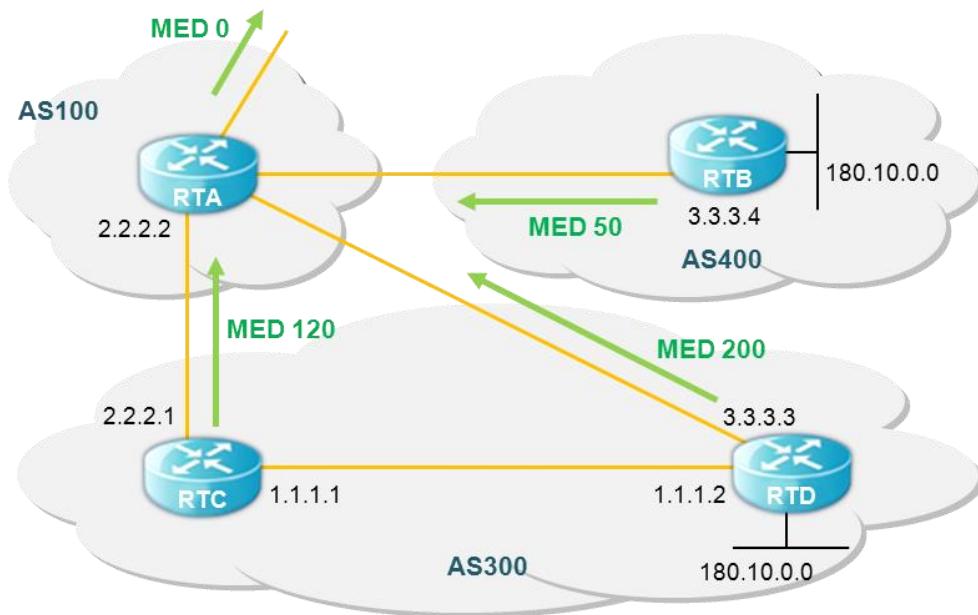
```
/*-- RTD --*/
!
router bgp 256
neighbor 3.3.3.4 remote-as 300
neighbor 3.3.3.4 route-map setlocalin in
neighbor 128.213.11.1 remote-as 256
!
ip as-path access-list 7 permit ^300$
!
route-map setlocalin permit 10
match as-path 7
set local-preference 200
!
route-map setlocalin permit 20
set local-preference 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.



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 metric 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 3.3.3.4 remote-as 400
!
/*-- RTB --*/
!
router bgp 400
neighbor 3.3.3.4 remote-as 100
neighbor 3.3.3.4 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</pre>


---



```

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
```

or

```
route-map setcommunity
match as-path 1
set community 200 additive
```

If additive keyword is not set, the value 200 replaces the current community value, and if additive keyword is set, the value 200 is added. After setting the community attribute, this system transmits this to the neighbor as default. But Cisco system should use the following command.

```
neighbor {ip-address|peer-group-name} send-community
```

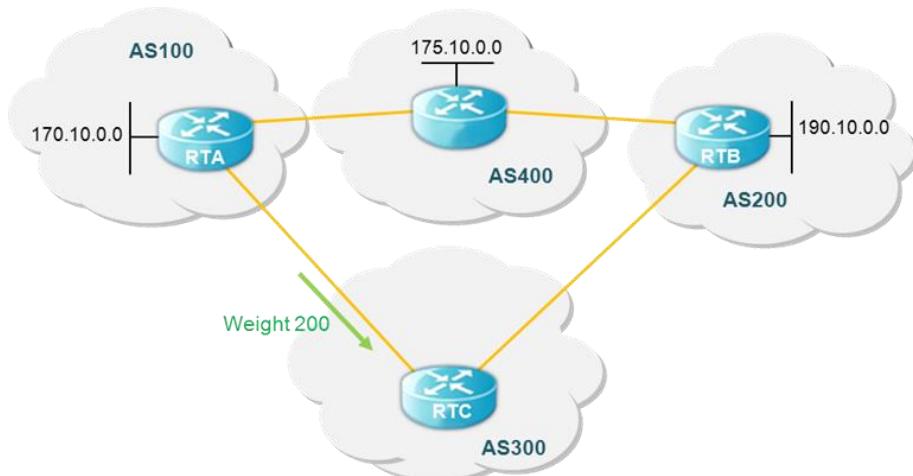
```
/*-- RTA --*/
!
router bgp 100
neighbor 3.3.3.3 remote-as 300
neighbor 3.3.3.3 send-community
neighbor 3.3.3.3 route-map setcommunity out
!
```

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.



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 netxthop. 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.

- Additional setting by operator is not needed
- Additional memory for routing information modification is not needed

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 recommandable 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]
```

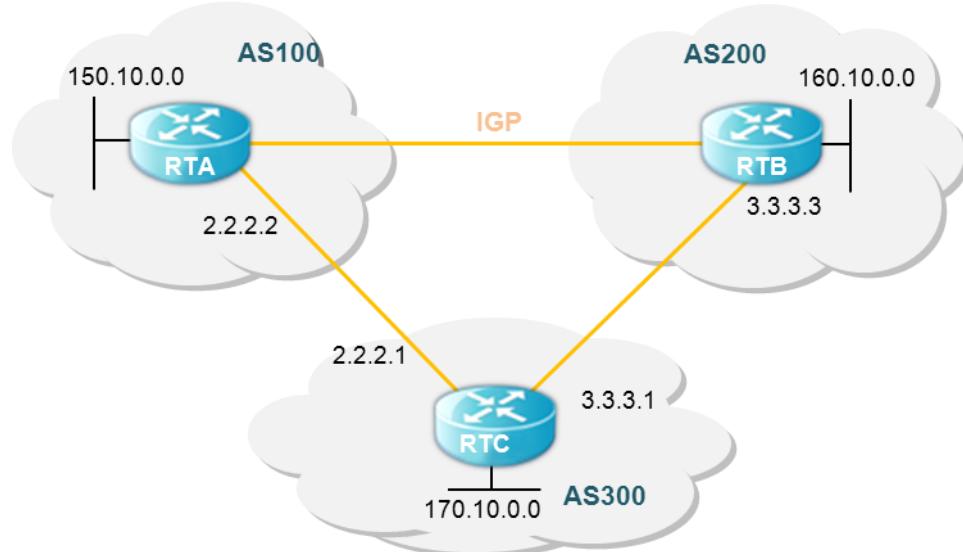
BGP Peer Groups

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



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 eiBGP Multipath feature)
- AS-PATH (after the addition of the eiBGP Multipath feature)

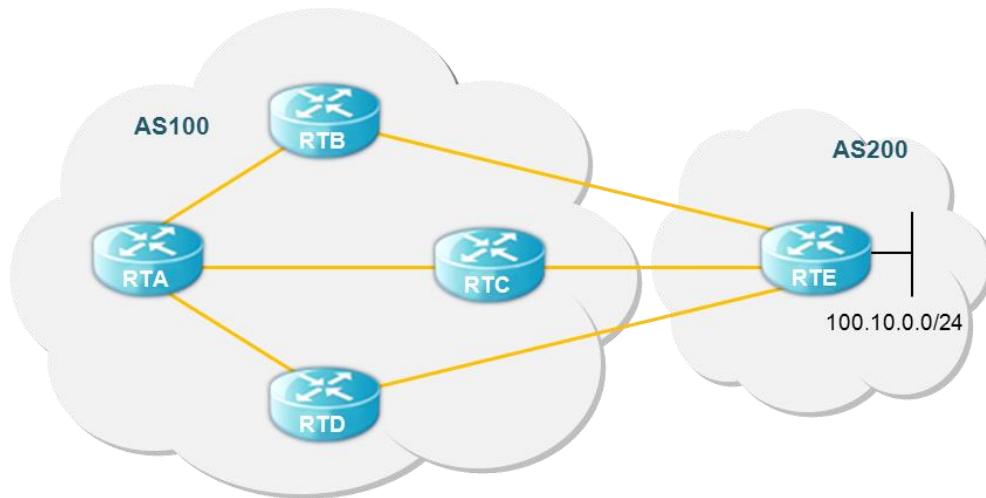
Some characteristics of BGP multipath have the additional requirements for the candidates of multipath.

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 Password encryption

You can use the authentication function with respect to TCP connection by specifying a password for the 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 exceeds 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 116 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-life-time.

Chapter 10. *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

Enable IGMP Snooping on a VLAN

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

Table 117 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)
    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 other querier interval is 262 seconds
    IGMP max query response time is 25 seconds
    Group Membership interval is 275 seconds
    IGMP Last member query count is 2
    IGMP Last member query interval is 1000 milliseconds
    IGMP Startup query count is 2
    IGMP Startup query interval is 31 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
    IGMP Snooping last-member-query is enabled
.....
Router#
```

Configure IGMP Snooping Functionality

IGMP Snooping Report-Suppression

If you enable ‘IGMP Snooping’ on a VLAN Interface, ‘IGMP Report-suppression’ is basically set to ‘Enable’ and only one IGMP Report is sent to Multicast Router for each IGMP Membership. If IGMP Report-suppression is set to Disable, all IGMP Report that are received will be forwarded to the Multicast Router.

This feature applies only to IGMPv1 and IGMPv2, and the following commands are to be executed in interface configuration mode.

Table 118 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)
    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 other querier interval is 262 seconds
    IGMP max query response time is 25 seconds
    Group Membership interval is 275 seconds
    IGMP Last member query count is 2
    IGMP Last member query interval is 1000 milliseconds
    IGMP Startup query count is 2
    IGMP Startup query interval is 31 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
    IGMP Snooping last-member-query is enabled
.....
Router#

```

IGMP Snooping 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.

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)
    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 other querier interval is 262 seconds
IGMP max query response time is 25 seconds
Group Membership interval is 275 seconds
IGMP Last member query count is 2
IGMP Last member query interval is 1000 milliseconds
IGMP Startup query count is 2
IGMP Startup query interval is 31 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
IGMP Snooping last-member-query is enabled
.....
```

```
Router#
```

IGMP Snooping 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 multcaster 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 119 IGMP Snooping 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 gi7/2
Router(config-if-Vlan22)# end
Router# show ip igmp snooping mrouter
VLAN      Interface:
22        Giga7/2
```

```
Router#
```

IGMP Snooping Querier

If you enable IGMP Snooping on a VLAN Interface, then the VLAN Interface will behave as IGMP NON-Querier. To make the VLAN Interface behave as IGMP Querier, you will need to enable the PIM-SM. However by using of IGMP Snooping Querier functionality you can have the VLAN Interface operate as and IGMP Querier without activation of the PIM-SM. When using the IGMP Snooping Querier feature, you should set manually the mrouter port in order to avoid the IGMP Query which might be transferred to upper layer equipment.

To set the IGMP Snooping Query feature the following command are to be executed in interface configuration mode.

Table 120 IGMP Snooping Querier

Command	Description
ip igmp snooping querier	Set snooping querier for the VLAN.
no ip igmp snooping querier	Remove the set snooping querier for the VLAN.

```

Router# configure terminal
Router(config)# interface vlan22
Router(config-if-Vlan22)# ip igmp snooping mrouter interface gi7/2
Router(config-if-Vlan22)# ip igmp snooping querier
Router(config-if-Vlan22)# end
Router# show ip igmp interface
.....
Interface Vlan22 (Index 2022)
    IGMP Enabled, Active, Non-Querier, Version 2 (default)
    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 other querier interval is 262 seconds
    IGMP max query response time is 25 seconds
    Group Membership interval is 275 seconds
    IGMP Last member query count is 2
    IGMP Last member query interval is 1000 milliseconds
    IGMP Startup query count is 2
    IGMP Startup query interval is 31 seconds
    IGMP Snooping is enabled on this interface
    IGMP Snooping fast-leave is not enabled
IGMP Snooping querier is enabled
    IGMP Snooping report suppression is disabled
    IGMP Snooping last-member-query is enabled
.....
Router#

```

IGMP Snooping Last-Member-Query

If you enable IGMP Snooping on a VLAN Interface, Last-Member-Query is set to enable by default. And, IGMP Snooping will transfer Group Specific Query only if the Last Member Leave. If Last-Member-Query is set to disable then Group Specific Query is sent whenever all of the Member leave.

To enable this feature, the following commands are to be executed in interface configuration mode.

Table 121 IGMP Snooping Last-Member-Query

Command	Description
ip igmp snooping last-member-query	Set snooping last-member-query for the VLAN.
no ip igmp snooping last-member-query	Remove the set snooping last-member-query for the VLAN

```

Router# configure terminal
Router(config)# interface vlan22
Router(config-if-Vlan22)# ip igmp snooping last-member-query
Router(config-if-Vlan22)# end
Router# show ip igmp interface
.....
Interface Vlan22 (Index 2022)
    IGMP Enabled, Active, Non-Querier, Version 2 (default)
    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 other querier interval is 262 seconds
IGMP max query response time is 25 seconds
Group Membership interval is 275 seconds
IGMP Last member query count is 2
IGMP Last member query interval is 1000 milliseconds
IGMP Startup query count is 2
IGMP Startup query interval is 31 seconds
IGMP Snooping is enabled on this interface
IGMP Snooping fast-leave is not enabled
IGMP Snooping querier is enabled
IGMP Snooping report suppression is disabled
IGMP Snooping last-member-query is disabled
.....
Router#

```

IGMP Snooping Access-Group

To set IGMP Access-Group, use the following command in the interface configuration mode.

Table 122 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 gi6/1
Router(config-if-Giga6/1)# ip igmp snooping access-group 10
Router(config-if-Giga6/1)# 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 123 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 gi6/1
Router(config-if-Giga6/1)# ip igmp snooping access-group 10 vlan 22
Router(config-if-Giga6/1)# end

```

```
Router#
```

IGMP Snooping 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 124 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 gi6/1  
Router(config-if-Giga6/1)# ip igmp snooping limit 10  
Router(config-if-Giga6/1)# 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 125 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 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 gi6/1  
Router(config-if-Giga6/1)# ip igmp snooping limit 10 vlan 22  
Router(config-if-Giga6/1)# end  
Router#
```

Display System and Network Statistics

Table 126 IGMP Snooping-related Monitoring Command

Command	Description
show ip igmp snooping mrouter <IFNAME>	Displays Mrouter Port of IGMP snooping
show ip igmp snooping table {group interface reporters }	Displays Reporter information of IGMP snooping
show ip igmp snooping info	Displays interface information of IGMP snooping

Chapter 11. *IP 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.

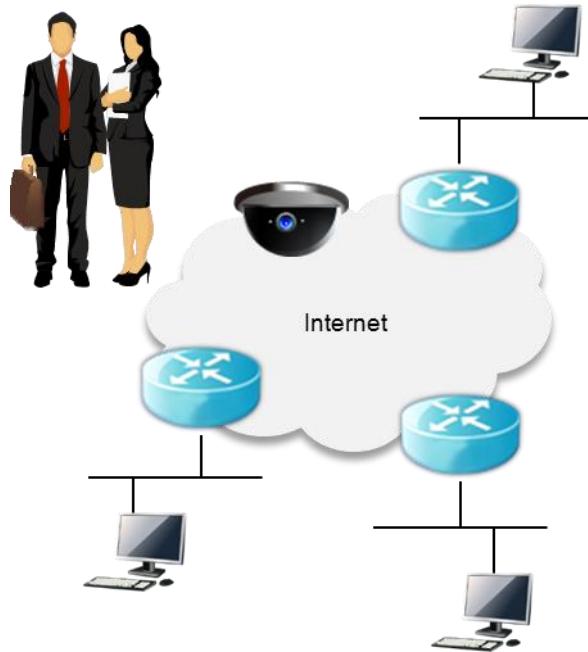


Figure 19 Multicasting to Transmit Traffic to Many Destinations

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 127 below summarizes the requirements for each protocol unicast and flooding algorithm.

Table 127 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 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 cannot 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 cannot 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 v2 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.

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 128 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 129 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 GigabitEthernet 7/1  
Router(config-if-Giga7/1)# ip pim sparse-mode  
Router(config-if-Giga7/1)# end  
Router# show ip pim sparse-mode interface  
Address          Interface   VIFindex Ver/      Nbr      Query   DR      DR  
                  Mode        Count     Intvl    Prior  
2.1.1.1          Giga7/1    0         v2/S     0       30      1       2.1.1.1  
Router#  
Router# show ip igmp interface  
Interface Giga7/1 (Index 1211)  
  IGMP Active, Querier, Version 2 (default)  
  IGMP interface has 0 group-record states  
  IGMP activity: 0 joins, 0 leaves  
  IGMP query interval is 125 seconds  
  IGMP other querier interval 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.

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 6/1
Router(config-if-Giga6/1)# router-guard ip multicast
Router(config-if-Giga6/1)# interface GigabitEthernet 7/1
Router(config-if-Giga7/1)# router-guard ip multicast vlan 22
Router(config-if-Giga7/1)# end
Router# show router-guard ip multicast
```

Globally enabled on interface gi6.1

Drop statistics

```
    IGMP Queries      : 0
    PIM Messages     : 0
    DVMRP Messages   : 0
    Invalid Messages : 0
```

Enabled on interface gi7.1, vlan22

Drop statistics

```
    IGMP Queries      : 0
    PIM Messages     : 0
    DVMRP Messages   : 0
    Invalid Messages : 0
```

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 130 Global Multicast Group-Limit

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

ip multicast group-range access-list	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.

Table 131 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 132 Multicast Route-Limit

Command	Description
ip multicast route-limit <1-2147483647> [<1-2147483647>]	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 recv 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 recv/Reg NACK recv/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 recv

```
Client msg counts: WRONGVIF/WHOLEPKT/Imm Stat/Timed Stat sent
Reg pkt counts: Reg ACK recv/Reg NACK recv/Reg pkt sent
Router#
```

Configure 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 133 IGMP VersionTable

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 GigabitEthernet 7/1
Router(config-if-Giga7/1)# ip igmp version 3
Router(config-if-Giga7/1)# end
Router# show ip igmp interface
IGMP Enabled, Active, Querier, Configured for version 3
    IGMP interface has 0 group-record states
    IGMP activity: 0 joins, 0 leaves
    IGMP query interval is 125 seconds
    IGMP other querier interval is 262 seconds
    IGMP max query response time is 25 seconds
    Group Membership interval is 275 seconds
    IGMP Last member query count is 2
    IGMP Last member query interval is 1000 milliseconds
    IGMP Startup query count is 2
    IGMP Startup query interval is 31 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 Snooping last-member-query 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 134 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 7/1	
Router(config-if-Giga7/1)# ip igmp access-group 1	
Router(config-if-Giga7/1)# end	

IGMP Query-Interval

The multicast router sends an IGMP query message periodically for managing multicast membership.

To change IGMP query message interval, use the following command in interface configuration mode:

An IGMP Querier is elected among multicast routers in each Network to transmit IGMP Query message. A router whose IP address is the smallest value will be elected. The elected IGMP Querier is responsible to send IGMP Query messages periodically to all host on the Network.

The IGMP Querier sent IGMP Query messages every 125 seconds by default in order to keep transmission overhead low. To change the interval between this message transmission, the below command is executed in interface configuration mode.

Table 135 IGMP Query-Interval

Command	Description
ip igmp query-interval <1-18000>	Sets igmp query-interval (Default: 125 seconds)
no ip igmp query-interval	Sets IGMP query interval as default.

```
Router# configure terminal
Router(config)# interface GigabitEthernet 7/1
Router(config-if-Giga7/1)# ip igmp query-interval 60
Router(config-if-Giga7/1)# end
Router# show ip igmp interface
Interface Giga7/1 (Index 1211)
    IGMP Enabled, Active, Querier, Version 2 (default)
    IGMP interface has 0 group-record states
    IGMP activity: 0 joins, 0 leaves
IGMP query interval is 60 seconds
    IGMP other querier interval is 262 seconds
    IGMP max query response time is 25 seconds
    Group Membership interval is 275 seconds
    IGMP Last member query count is 2
    IGMP Last member query interval is 1000 milliseconds
    IGMP Startup query count is 2
    IGMP Startup query interval is 31 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

When an IGMP Querier receives an IGMP Leave message from a Host which means the Host secedes from the Multicast Group, the IGMP Querier generates IGMP Group-Specific Query in order to check out there is any other Host in the same Multicast Group.

If there is no response from any Host to the Group-Specific Query, then the IGMP Querier removes the Multicast Membership.

IGMP last-member-query-count specifies 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 136 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 7/1
Router(config-if-Giga7/1)# ip igmp last-member-query-count 3
Router(config-if-Giga7/1)# 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 137 IGMP Last-Member-Query-Interval

Command	Description
ip igmp last-member-query-interval <1000-25500>	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 7/1
Router(config-if-Giga7/1)# ip igmp last-member-query-interval 2000
Router(config-if-Giga7/1)# end
Router# show ip igmp interface
Interface Giga7/1 (Index 1211)
    IGMP Enabled, Active, Querier, Version 2 (default)
    IGMP interface has 0 group-record states
    IGMP activity: 0 joins, 0 leaves
    IGMP query interval is 125 seconds
    IGMP other querier interval is 262 seconds
    IGMP max query response time is 25 seconds
    Group Membership interval is 275 seconds
IGMP Last member query count is 3
IGMP Last member query interval is 2000 milliseconds
    IGMP Startup query count is 2
    IGMP Startup query interval is 31 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 138 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 GigabitEthernet 7/1
Router(config-if-Giga7/1)# ip igmp immediate-leave group-list 2
Router(config-if-Giga7/1)# 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 139 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 GigabitEthernet 7/1
Router(config-if-Giga7/1)# ip igmp limit 100
Router(config-if-Giga7/1)# end
```

IGMP Global Limit

IGMP Querier manages the Hosts which join a Multicast Membership Group per the interface. Multicast Router can limit the total number of Multicast Membership Group which are managed by the IGMP Querier.

To set the IGMP Global Group Limit the following command in global configuration mode is executed.
Table 140 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
<pre>Router# configure terminal Router(config)# ip igmp limit 100 Router(config)# end</pre>	

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 141 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 GigabitEthernet 7/1
Router(config-if-Giga7/1)# ip igmp minimum-version 2
Router(config-if-Giga7/1)# 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 142 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 GigabitEthernet 7/1
Router(config-if-Giga7/1)# ip igmp querier-timeout 300
Router(config-if-Giga7/1)# end
Router# show ip igmp interface
Interface Giga7/1 (Index 1211)
    IGMP Enabled, Active, Querier, Version 2 (default)
    IGMP interface has 0 group-record states
    IGMP activity: 0 joins, 0 leaves
    IGMP query interval is 125 seconds
IGMP other querier interval is 300 seconds
    IGMP max query response time is 25 seconds
    Group Membership interval is 275 seconds
    IGMP Last member query count is 2
    IGMP Last member query interval is 1000 milliseconds
    IGMP Startup query count is 2
    IGMP Startup query interval is 31 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 Snooping last-member-query 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 143 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 GigabitEthernet 7/1
Router(config-if-Giga7/1)# ip igmp query-max-response-time 10
Router(config-if-Giga7/1)# end
Router# show ip igmp interface
Interface Giga7/1 (Index 1211)
    IGMP Enabled, Active, Querier, Version 2 (default)
    IGMP interface has 0 group-record states
    IGMP activity: 0 joins, 0 leaves
    IGMP query interval is 125 seconds
    IGMP other querier interval is 262 seconds
IGMP max query response time is 10 seconds
    Group Membership interval is 275 seconds
    IGMP Last member query count is 2
    IGMP Last member query interval is 1000 milliseconds
    IGMP Startup query count is 2
    IGMP Startup query interval is 31 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 Snooping last-member-query 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 144 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 GigabitEthernet 7/1
Router(config-if-Giga7/1)# ip igmp rate 100
Router(config-if-Giga7/1)# end
Router# show ip igmp rate-limit statistics
```

IGMP Message Ratelimit (pps) for IP Multicast					
Ifname	Incoming rate	Rate-limit	Permit	Drop	Rx-Total
Gi7.1	0	100	0	0	0

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 145 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 7/1
Router(config-if-Giga7/1)# ip igmp robustness-variable 5
Router(config-if-Giga7/1)# end
Router#
```

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 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 146 IGMP Static-Group

Command	Description
class-map type multicast-flows name	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 147 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 A.B.C.D to A.B.C.D source A.B.C.D	Assigns multiple IGMPv3 groups and a source(S, Gn).
no group A.B.C.D	Deletes the assigned IGMPv2 group (*, G).
no group A.B.C.D source A.B.C.D	Deletes the assigned IGMPv3 and source (S, G).
no group A.B.C.D to A.B.C.D	Deletes the assigned multiple IGMPv2 groups (*, Gn).
no group A.B.C.D to A.B.C.D source A.B.C.D	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 148 IGMP Rate

Command	Description
ip igmp static-group A.B.C.D	Sets the IGMPv2 static-group not using the IGMP class-map.
ip igmp static-group A.B.C.D interface IFNAME	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 A.B.C.D source A.B.C.D	Sets an IGMPv3 static-group not using the IGMP class-map.
ip igmp static-group A.B.C.D source A.B.C.D interface IFNAME	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 name	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 A.B.C.D	Disables the IGMPv2 static-group.

no ip igmp static-group A.B.C.D interface /IFNAME	Disables the IGMPv2 static-group that is set in the VLAN interface with enabled IGMP Snooping.
no ip igmp static-group A.B.C.D source A.B.C.D	Disables the IGMPv3 static-group.
no ip igmp static-group A.B.C.D source A.B.C.D interface /IFNAME	Disables the IGMPv3 static-group that is set in the VLAN interface with enabled IGMP Snooping.
no ip igmp static-group class-map name	Disables the static-group of IGMP Class-Map.

```

Router# configure terminal
Router(config)# interface GigabitEthernet 7/1
Router(config-if-Giga7/1)# ip igmp static-group igmp_static
Router(config-if-Giga7/1)# end
Router# show ip igmp group
IGMP Connected Group Membership
Group Address      Interface          Uptime    Expires   Last Reporter
225.1.1.1          Giga7/1           00:01:42  static    0.0.0.0
225.1.1.2          Giga7/1           00:01:42  static    0.0.0.0
225.1.1.3          Giga7/1           00:01:42  static    0.0.0.0
225.1.1.4          Giga7/1           00:01:42  static    0.0.0.0
225.1.1.5          Giga7/1           00:01:42  static    0.0.0.0
225.1.1.6          Giga7/1           00:01:42  static    0.0.0.0
225.1.1.7          Giga7/1           00:01:42  static    0.0.0.0
225.1.1.8          Giga7/1           00:01:42  static    0.0.0.0
225.1.1.9          Giga7/1           00:01:42  static    0.0.0.0
225.1.1.10         Giga7/1           00:01:42  static    0.0.0.0
225.1.2.1          Giga7/1           00:01:42  static    0.0.0.0
Router# show ip igmp static-group class-map interface gi7/1

Giga7/1
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 149 IGMP SSM-MAP1

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 150 IGMP SSM-MAP2

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#

```

Configure PIM-SM Functionality

To configure the Protocol Independent Multicast (PIM) feature, do the following tasks.

PIM Hello-Interval

PIM sends out Hello message in periodic manner. To set the interval between message transmission use the below commands in interface configuration mode.

command	Description
ip pim hello-interval < 1-65535>	Set the interval between Hello message transmission. (Default : 30s)

no ip pim hello-interval	Return the interval to the default value.
---------------------------------	---

```
Router# configure terminal
Router(config)# interface GigabitEthernet 6/1
Router(config-if-Giga6/1)# ip pim hello-interval 60
Router(config-if-Giga6/1)# end
Router# show ip pim sparse-mode interface
Address           Interface   VIFindex Ver/   Nbr      Query DR     DR
                           Mode       Count  Intvl Prior
3.1.3.222        Giga6/1    0        v2/S   0       60     1    3.1.3.222
Router#
```

PIM Hello-Holdtime

PIM sends out Hello message in periodic manner and any Neighbor who receives the PIM Hello message should maintain the message sender as its neighbor for the 'Holdtime' period specified in the received Hello message. To set Holdtime use the below commands in interface configuration mode.

Command	Description
ip pim hello-holdtime < 1-65535>	Set the holdtime in Hello message. (Default : 105s)
no ip pim hello-interval	Return the holdtime to default value in Hello message.

```
Router# configure terminal
Router(config)# interface GigabitEthernet 6/1
Router(config-if-Giga6/1)# ip pim hello-holdtime 120
Router(config-if-Giga6/1)# end
```

PIM DR-Priority

PIM sends out Hello message in periodic manner and any Neighbor who receives the PIM Hello message should select DR of the corresponding interface according to the specified DR-Priority in the received Hello message.

When selecting DR, the following rule will be applied:

- After comparing the DR Priority specified in both the interface and the Neighbor message, the host whose DR Priority is higher will be the DR Router.
- When the DR Priority specified in both the interface and the Neighbor message is same, the host whose IP address is the highest will be the DR Router.
- In case the received PIM Hello message do not include DR Priority, it is deemed that the Neighbor has the highest priority so the Neighbor will be the DR Router.
- When there are multiple Neighbors which do not include DR Priority, the Neighbor whose IP address is the highest will be the DR Router.

To modify the DR Priority in PIM Hello message, use the following commands in interface configuration mode.

command	Description
ip pim dr-priority <0-4294967294 >	Set DR Priority in PIM Hello message. (Default : 1)
no ip pim dr-priority	Return DR Priority to default value.

```

Router# configure terminal
Router(config)# interface GigabitEthernet 6/1
Router(config-if-Giga6/1)# ip pim dr-priority 10
Router(config-if-Giga6/1)# end
Router# show ip pim sparse-mode interface
Address          Interface  VIFIndex Ver/ Nbr      Query   DR      DR
                  Mode        Count    Intvl Prior
3.1.3.222        Giga6/1    0         v2/S    0       60      10     3.1.3.222
Router#

```

PIM Propagation-Delay

In Multi-Access Network environment, if any one particular PIM Neighbor no longer wants to receive Multicast Traffic, the PIM Neighbor will send 'PIM Prune' message to the Upstream Router. Then the Upstream Router will stay on hold during the specified time so as to determine whether there is any other PIM Router which may want to receive the same Multicast Traffic.

If there is any PIM Router which wants to receive the delayed Multicast Traffic, the PIM Router will need to send PIM Join message within the reserved time period to the Upstream Router so that the Upstream Router will continue to forward the Multicast Traffic.

For the Multicast Traffic Forwarding in Multi-Access Network environment, PIM Router sends out the propagation delay time that is necessary for delaying PIM Prune process. This is included in PIM Hello messages.

Command	Description
ip pim propagation-delay <1000-5000>	Set propagation delay in PIM Hello message. (Default: 1000ms)
no ip pim propagation-delay	Release the set propagation delay in PIM Hello message.

```

Router# configure terminal
Router(config)# interface GigabitEthernet 6/1
Router(config-if-Giga6/1)# ip pim propagation-delay 5000
Router(config-if-Giga6/1)# end
Router# show ip pim sparse-mode interface detail
Giga6/1 (vif 0):
    Address 3.1.3.222, DR 3.1.3.222
    Hello period 30 seconds, Next Hello in 23 seconds
    Triggered Hello period 5 seconds
    Propagation delay is 1000 milli-seconds
Configured Propagation-delay 5000 milli-seconds
    Generation ID : 795759275
    Neighbors:

```

Router#

PIM Exclude-Genid

PIM sends out Hello message in periodic manner and the PIM Hello message may include Generation ID in the message. In case a PIM Router received PIM Hello messages which have different Generation IDs from an identical Neighbor, it is deemed that the Neighbor has been Started or Restarted. Consequently PIM Neighbor Discovery is conducted to update RP information or PIM RPF.

If you want not to include Generation ID in the PIM Hello message, use the below command in interface configuration mode.

Command	Description
ip pim exclude-genid	Configure not to include Generation ID in the PIM Hello message.

no ip pim exclude-genid	Remove the configuration of exclude-genid.
--------------------------------	--

```
Router# configure terminal
Router(config)# interface GigabitEthernet 6/1
Router(config-if-Giga6/1)# ip pim exclude-genid
Router(config-if-Giga6/1)# end
Router#
```

PIM Neighbor-Filter

PIM sends out Hello message in periodic manner and the Neighbor which receives the PIM Hello messages will choose the DR in its network.

When you need to block any particular PIM Neighbor, use the below command in interface configuration mode.

Command	Description
ip pim neighbor-filter access-list	Set to block the PIM neighbor.
no ip pim neighbor-filter access-list	Release the blocked the PIM neighbor..

```
Router# configure terminal
Router(config)# access-list 3 permit 3.1.3.1
Router(config)# interface GigabitEthernet 6/1
Router(config-if-Giga6/1)# ip pim neighbor-filter 3
Router(config-if-Giga6/1)# end
```

PIM BSR-Border

Bootstrap Router (BSR) generates periodically the Bootstrap message which has the information regarding the dispatched RP over the network. If you configure BSR Border on a specific interface, then different PIM domain can be configured as the transmission of the Bootstrap messages is limited.

To configure BSR Border on a specific interface, use the below commands in interface configuration mode.

Command	Description
ip pim bsr-border	Block the transmission of BSR message for the interface.
no ip pim bsr-border	Release the blocked transmission of BSR message for the interface.

```
Router# configure terminal
Router(config)# interface GigabitEthernet 6/1
Router(config-if-Giga6/1)# ip pim bsr-border
Router(config-if-Giga6/1)# end
```

PIM JP-Timer

Multicast Router sends out PIM Join/Prune messages to the Upstream Multicast Router which is on the Routing Path of SPT or RPT so as to maintain Multicast Traffic Forwarding.

The default value of interval for transmitting PIM Join/Prune messages is 60 seconds. To modify the interval, use the below commands in global configuration mode.

Command	Description
ip pim jp-timer <1-65535>	Set the interval for transmitting PIM Join/Prune messages. (Default : 60 sec)
no ip pim jp-timer	Return the set the interval to default value.

```
Router# configure terminal
Router(config)# ip pim jp-timer 120
Router(config)# exit
```

PIM Access-Group

Multicast Router maintains Multicast Traffic Forwarding receiving PIM Join message periodically. For the case that any PIM Join message for unwanted Multicast Group would be received, you may restrict the join message.

To restrict the PIM join message to unwanted Multicast Group, use the below commands in interface configuration mode.

Command	Description
ip multicast boundary access-list	Limit the PIM join message to the Multicast Group specified as Access-List.
no ip multicast boundary access-list	Release the limitation set for the PIM join message.

```
Router# configure terminal
Router(config)# access-list 3 deny 224.1.1.0 0.0.0.255
Router(config)# interface GigabitEthernet 6/1
Router(config-if-Giga6/1)# ip multicast boundary 3
Router(config-if-Giga6/1)# end
```

PIM Accept-Register

The Multicast Router which acts as RP manages Multicast Source Entry by receiving PIM Register messages from the 1st-Hop Multicast Router in PIM Domain.

To limit the particular source from which the received PIM Register messages are coming, use the below commands in global configuration mode.

Command	Description
ip pim accept-register list access-list	Limit the particular source of the received PIM Register messages.
no ip pim register-filter-group	Release the limitation on the particular source.

```
Router# configure terminal
Router(config)# access-list 30 permit 100.1.1.0 0.0.0.255
Router(config)# access-list 30 deny any
Router(config)# ip pim accept-register list 30
Router(config)# exit
```

PIM SPT-Threshold

When a Multicast Router keeps the IGMP Membership for the IGMP Host, this Multicast Router is called as Last-Hop Router. The Last-Hop Router can configure the SPT(Shortest-Path-Tree) so that it can receive the Multicast Traffic which come from RP Tree in the fastest path.

To configure PIM SPT-Threshold, use the below commands in global configuration mode.

Command	Description
ip pim spt-threshold [group-list access-list]	Configure PIM SPT-Threshold Default is 'Enable'.
no ip pim spt-threshold [group-list access-list]	Release the configured PIM SPT Threshold.

```
Router# configure terminal
Router(config)# no ip pim spt-threshold
Router(config)# exit
```

PIM Cisco-Register-C checksum

The First-Hop Router which has received the Multicast Packet from Multicast Packet Originator sends the packet that is included in PIM Register message to RP by way of unicast routing. The RP which receives this PIM Register message forwards the Multicast Packet to all the Multicast Routing Entry.

According to RFC standards the Checksum of PIM-SM Register message is calculated with the Header part meanwhile Cisco uses the entire message for the Checksum. Therefore, in order to be compatible with CISCO Router Checksum calculation shall be with the whole of the message.

To set the Cisco Register-C checksum use the below command in global configuration mode.

Command	Description
ip pim cisco-register-checksum	Configure to be compatible with CISCO for all Group.
ip pim cisco-register-checksum group-list access-list	Configure to be compatible with CISCO for the Group specified in Access-list.
no ip pim cisco-register-checksum	Release the configuration for all Group.
no ip pim cisco-register-checksum group-list access-list	Release the configuration for the specified Group.

```
Router# configure terminal
Router(config)# ip pim cisco-register-checksum
Router(config)# exit
```

```
Router# configure terminal
Router(config)# access-list 11 permit 224.1.1.0 0.0.0.255
Router(config)# ip pim cisco-register-checksum group-list 11
Router(config)# exit
```

PIM BSR-Candidate

In order for a Multicast Router to act as the BSR Candidate, it should be included in PIM Domain. To configure the Multicast Router to be the BSR Candidate, use the below commands in global configuration mode.

Command	Description
ip pim bsr-candidate ifname [hash-mask-length] [priority]	Configure the Multicast Router to be the BSR Candidate
no ip pim bsr-candidate [ifname]	Release the configuration for the BSR candidate.

```

Router# configure terminal
Router(config)# ip pim bsr-candidate lo0
Router(config)# exit
Router# show ip pim sparse-mode bsr-router
PIMv2 Bootstrap information
This system is the Bootstrap Router (BSR)
    BSR address: 172.16.1.222
    Uptime:      00:02:32, BSR Priority: 64, Hash mask length: 10
    Next bootstrap message in 00:00:24
    Role: Candidate BSR
    State: Elected BSR
Router#

```

```

Router# configure terminal
Router(config)# ip pim bsr-candidate lo0 24 128
Router(config)# exit
Router# show ip pim sparse-mode bsr-router
PIMv2 Bootstrap information
This system is the Bootstrap Router (BSR)
    BSR address: 172.16.1.222
    Uptime:      00:05:01, BSR Priority: 128, Hash mask length: 24
    Next bootstrap message in 00:00:59
    Role: Candidate BSR
    State: Elected BSR
Router#

```

PIM RP-Candidate

In order for a Multicast Router to act as the RP Candidate, it should be included in PIM Domain. RP Candidate can provide service to the whole IP multicast address range or a part of them. Candidate RP sends periodically Candidate RP Advertisement message to Bootstrap Router (BSR).

To configure the Multicast Router to be the RP Candidate, use the below commands in global configuration mode.

Command	Description
ip pim rp-candidate <i>ifname</i>	Configure the Candidate RP to operate with Default value.
ip pim rp-candidate <i>ifname priority <0-255></i>	Configure the Candidate RP of specified priority to operate.
ip pim rp-candidate <i>ifname priority <0-255> interval <1-16383></i>	Configure the Candidate RP that has specified priority and sends out Advertisement message periodically to operate.
ip pim rp-candidate <i>ifname priority <0-255> interval <1-16383> group-list <i>access-list</i></i>	Configure the Candidate RP that has specified priority and sends out Advertisement message periodically to the specified Group to operate.
no ip pim rp-candidate [<i>ifname</i>]	Release the configuration set on the Candidate RP.

```

Router# configure terminal
Router(config)# ip pim bsr-candidate lo0
Router(config)# ip pim rp-candidate lo0
Router(config)# exit
Router# show ip pim sparse-mode bsr-router
This system is the Bootstrap Router (BSR)
    BSR address: 172.16.1.222
    Uptime:      00:03:56, BSR Priority: 64, Hash mask length: 10
    Next bootstrap message in 00:00:07
    Role: Candidate BSR
    State: Elected BSR
Router#

```

```

Candidate RP: 172.16.1.222(Loopback0)
Advertisement interval 60 seconds
Next C-RP advertisement in 00:00:36
Router#
Router# show ip pim sparse-mode rp mapping
PIM Group-to-RP Mappings
This system is the Bootstrap Router (v2)
Group(s): 224.0.0.0/4
RP: 172.16.1.222
Info source: 172.16.1.222, via bootstrap, priority 192
Uptime: 00:00:08, expires: 00:02:24
Router#

```

PIM RP-Address

You can use this feature when you configure a Multicast router to be the RP in static fashion in the Network environment where RP Candidate or BSR Candidate are not available.

Static RP information will have a lower priority than the RP Candidate which has been updated by dynamic learning from Bootstrap message. If you want to increase the priority of the set Static RP than the learned RP Candidate, you will need to configure RP-Address Override.

To set Static RP information on the Multicast Router, use the below command in global configuration mode.

Command	Description
ip pim rp-address A.B.C.D [access-list] [override]	Set Static RP on the Multicast Router.
no ip pim rp-address A.B.C.D [access-list]	Release the set Static RP information.

```

Router# configure terminal
Router(config)# ip pim rp-address 172.16.0.1
Router(config)# exit
Router# show ip pim sparse-mode rp mapping
PIM Group-to-RP Mappings
Group(s): 224.0.0.0/4, Static
RP: 172.16.0.1
Uptime: 00:00:37
Router#

```

PIM Register-Source

When transmitting PIM Register from 1st-Hop Router to RP, you can assign the IP source of the PIM Register Packet. To set the PIM Register-Source, use the below command in global configuration mode.

Command	Description
ip pim register-source [ifname A.B.C.D]	Set PIM Register-Source.
no ip pim rp-address A.B.C.D [access-list]	Release the set PIM Register-Source.

```

Router# configure terminal
Router(config)# ip pim register-source lo0
Router(config)# exit
Router#

```

PIM SSM

If you set PIM SSM, all the groups which are included in the configured SSM will not have RPT function but SPT.

To configure the Group Range of SSM, use the below commands in global configuration mode.

Table 151 PIM SSM

Command	Description
ip pim ssm default	Assign Default Group range(232/8) for PIM SSM.
ip pim ssm range access-list	Assign the Group range specified in Access-List for PIM SSM.
no ip pim ssm	Release the PIM SSM Group range.

```
Router# configure terminal
Router(config)# ip pim ssm default
Router(config)# access-list 10 permit 224.1.1.0 0.0.0.255
Router(config)# ip pim ssm range 10
Router(config)# exit
```

Display System and Network Statistics

Table 152 Monitoring Commands of IP Multicast Routing

Command	Description
show ip igmp groups	Display the multicast groups.
show ip igmp interface	Display the multicast related information of the interface.
show ip igmp rate-limit statistics	Display the statistics on multicast packet of the interface which is set with rate-limit.
show ip igmp ssm-map	Display the configuration status of ssm-map.
show ip igmp static-group class-map	Display the configuration status of class-map which is for specifying static group.
show ip igmp statistics {receive send} {interface }	Display the igmp statistics.
show ip mcache	Display the content of multicast routing cache.
show ip mroute	Display the content of multicast routing table.
show ip mvif	Display the information of multicast interface.
show ip pim sparse-mode anycast-rp	Display the information of PIM anycast RP.
show ip pim bsr-router	Display the information of BSR router.
show ip pim sparse-mode interface	Display the information of the interface which PIM has configured.
show ip pim sparse-mode local-members	Display the PIM local membership information.
show ip pim sparse-mode mroute	Display the content of multicast routing table which PIM manages.
show ip pim neighbor	Display the PIM neighbors.
show ip pim rp	Display the information about RP.
show ip pim rp-hash	Display the information about RP-HASH.
show ip rpf	Display the information about RPF.
show ip rpf event	Display the received RPF event information.

Chapter 12. ***Statistics Monitoring***

This chapter describes the monitoring function for the system and statistics of the C9500 series OLT systems:

- System Status Monitoring
- Interface Statistics
- Logging setting
- RMON (Remote Monitoring)
- Setting threshold value

The Statistics that the C9500 series 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 the C9500 series. With show and its sub-commands, it provides status information, which will be displayed on your terminal screen.

Table 153 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 SCM 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 154 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 155 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 156 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 157 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

The C9500 series system provides the statistics for individual ports of the system. To view the statistics, use the following commands.

```
show interface [ifname]
```

The C9500 series 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 7/1
```

```
Giga7/1 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
VRP 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 158 Commands for Port Statistics Check

Command	Description	Mode
show port counter [detail]	For the items below, it displays the accumulated statistics of all the interfaces.	Privileged

	I-Kbps/ O-Kbps InOctets/ OutOctets InPkts/ OutPkts	
show port statistics {all <i>IFNAME</i> }	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 [<i>IFNAME</i>]	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 [<i>IFNAME</i>]	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 <i>IFNAME</i>	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
Te6/1	0	0	0	0
Te6/2	0	0	0	0
Te6/3	0	0	0	0
Te6/4	0	0	0	0
Te6/5	0	0	0	0
Te6/6	0	0	0	0
Te6/7	2,560	0	20	0
Te6/8	2,560	0	20	0
Port	OutOctets	OutUcastPkts	OutMcastPkts	OutBcastPkts
Gi7/1	0	0	0	0
Gi7/2	0	0	0	0
Gi7/3	0	0	0	0
Gi7/4	0	0	0	0
Gi7/5	37,466	0	305	0
Gi7/6	37,220	0	303	0
Gi7/7	36,974	0	301	0
Gi7/8	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 gi7/5
```

Last clearing of counters 00:14:24

Port	TX		RX	
	bits/s	pkts/s	bits/s	pkts/s
Gi7/5				
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 159 Commands for Port Statistics Configuration

Command	Description	Mode
<code>load-interval <i>interval</i></code>	Sets the interval value - the system updates the average statistics of the interface for the period of the interval.	Interface
<code>no load-interval</code>	Returns the interval value to default one.	Interface
<code>input-load-monitor <i>interval</i> <i>low-threshold</i> <i>high-threshold</i></code>	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
<code>no input-load-monitor</code>	Clears the monitoring setting.	Interface
<code>show port input-load-monitor</code>	Shows the current monitoring setting.	Interface

You can use the following commands to initialize the accumulated statistic values.

Table 160 Command for Initialization of Port Statistic

Command	Description	Mode
<code>clear counters</code>	Initializes the accumulated statistic values of all the interfaces.	Privileged
<code>clear counters <i>IFNAME</i></code>	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 the C9500 series allows network administrators to improve system efficiency and reduce the network load.

The following sections explain more about RMON and the features that the C9500 series 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.

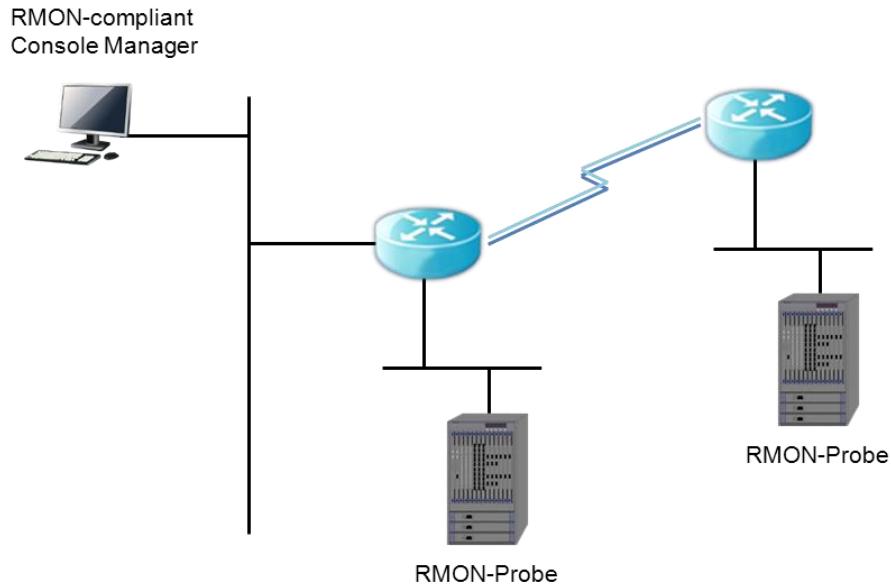


Figure 20 RMON Manager & RMON Probe

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.

The C9500 series supports only statistics, history, alarm, and event groups among the nine RMON groups, as defined in Table 161. All the RMON functions are set as disabled by default.

Table 161 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. <u>Displays of the usage by time and comparing the data with other segment data.</u>
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 162 Commands for RMON Alarm and Event Configuration

Command	Description	Mode
rmon alarm <i>index variable interval seconds {absolute delta} rising-threshold value event num falling-threshold value event num [owner string]</i>	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 <i>Interval:</i> Sampling time period (Unit: second). <i>Absolute:</i> Indicates the sampled alarm value to be set and monitored as absolute value. <i>Delta:</i> Indicates the sampled alarm value to be monitored in terms of the difference between current and previous values. <i>Rising-threshold, falling-threshold value:</i> The configured value which is used as the reference while the system generates alarm. <i>event:</i> Indicates the specified event to be invoked when the sampled alarm value reaches either rising-threshold or falling -threshold. <i>owner:</i> Registers the owner of the alarm.	Config
rmon event <i>index</i>	Adds an event to RMON event table	Config

[log] [trap <i>community</i>] [description <i>string</i>] [owner <i>string</i>]	<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.	
no rmon alarm <i>alarm-index</i>	Clears the setting of RMON alarm.	Config
no rmon event <i>event-index</i>	Clears the setting of RMON event.	Config
show rmon alarms	Prints out RMON alarm information.	Privileged
show rmon events	Prints out RMON event information.	Privileged

The following example demonstrates how to set the rmon alarm with respect to GigabitEthernet 7/2. It shows the system will do sampling in the Octets value of GigabitEthernet 7/2 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 7/2
Switch(config-if-Giga7/2)# 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 Giga7/2 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 163 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 7/2.

```

Switch# configure terminal
Switch(config)# interface GigabitEthernet 7/2
Switch(config-if-Giga7/2)# rmon collection stats 1
Switch(config-if-Giga7/2)# rmon collection history 1 buckets 30 interval 10
Switch(config-if-Giga7/2)# 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

The C9500 series 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

The C9500 series 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.

The C9500 series has 0-7 severity levels as shown in the following table:

Table 164 The C9500 series 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

The system log messages of the C9500 series 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 164.
- 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 lns
May  6 11:54:01 [5] IFM-NOTICE: Rate limit ra creation
May  7 02:10:24 [5] %REMOTE-CONNECT: login from console as lns
May  7 02:10:40 [5] IFM-NOTICE: Flow xx classified
May  7 02:10:48 [5] IFM-NOTICE: Flow xx match rate 10
May  7 05:17:56 [5] %REMOTE-CONNECT: login from console as lns
May  7 05:23:10  [5] IFM-NOTICE: Service pa add interface fa1
```

Default Logging Value

Table 165 System Log Default value

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 166 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)#
```

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 to 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)#
```

Chapter 13. ***STP (Spanning Tree Protocol) & SLD (Self-loop Detection)***

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

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 Bridgeld.

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. The C9500 series 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 167 Switch Priority Value and Extended System ID

Switch Priority Value											
Bit16		Bit15			Bit14			Bit13			
32768		16384			8192			4096			
Extended System ID(Set Equal to the VLAN ID)											
Bit12	Bit11	Bit10	Bit9	Bit8	Bit7	Bit6	Bit5	Bit4	Bit3	Bit2	Bit1
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 168 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).

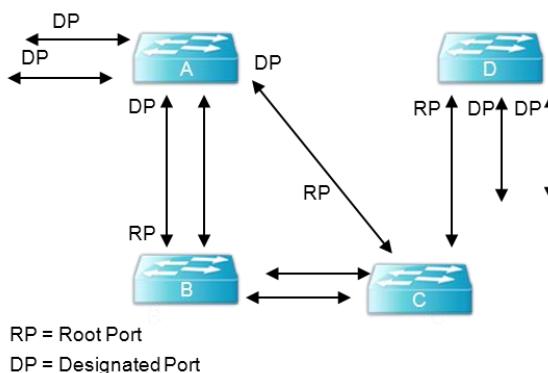


Figure 21 Spanning-Tree Topology

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.

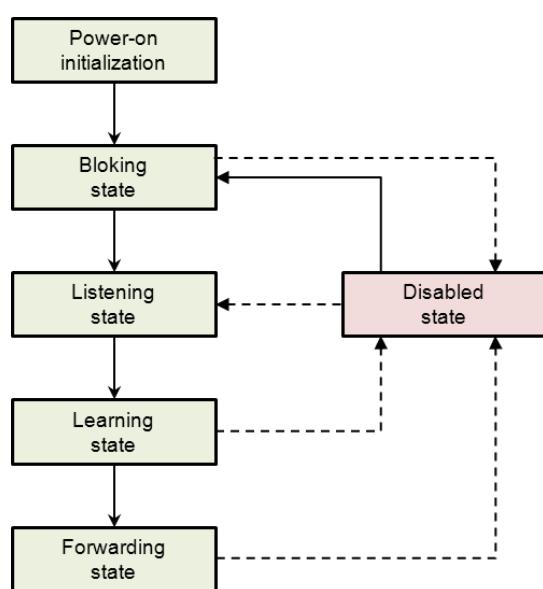


Figure 22 Spanning-Tree Interface States

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:</p> <ul style="list-style-type: none"> Drops the frames received through the port Drops the frames switched from other interfaces Does not perform address learning Receives BPDUs
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:</p> <ul style="list-style-type: none"> Drops the frames received through the port Drops the frames switched from other interfaces Does not perform address learning Receives BPDUs
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:</p> <ul style="list-style-type: none"> Drops the frames received through the port Drops the frames switched from other interfaces Performs address learning Receives BPDUs
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:</p> <ul style="list-style-type: none"> Forwards the frames received through the port Forwards the frames switched from other interfaces Performs address learning Receives BPDUs
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:</p> <ul style="list-style-type: none"> Drops the frames received through the port Drops the frames switched from other interfaces Does not perform address learning Does not receive BPDUs

Understanding RSTP

RSTP 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 169 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.

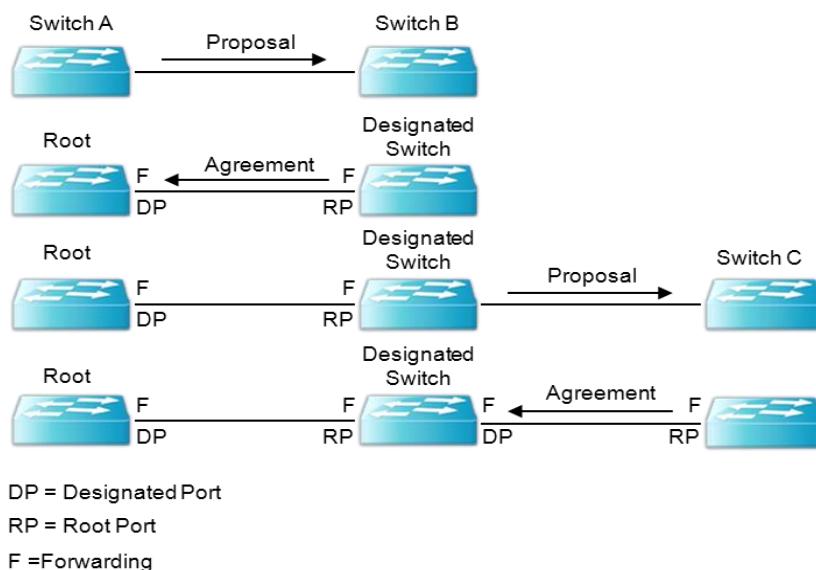


Figure 23 Proposal and Agreement Handshaking for Rapid Convergence

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 170 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.

Understanding 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 system 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. Furthermore if MSTP runs, BPDU transmission quantity also reduces progressively. 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.

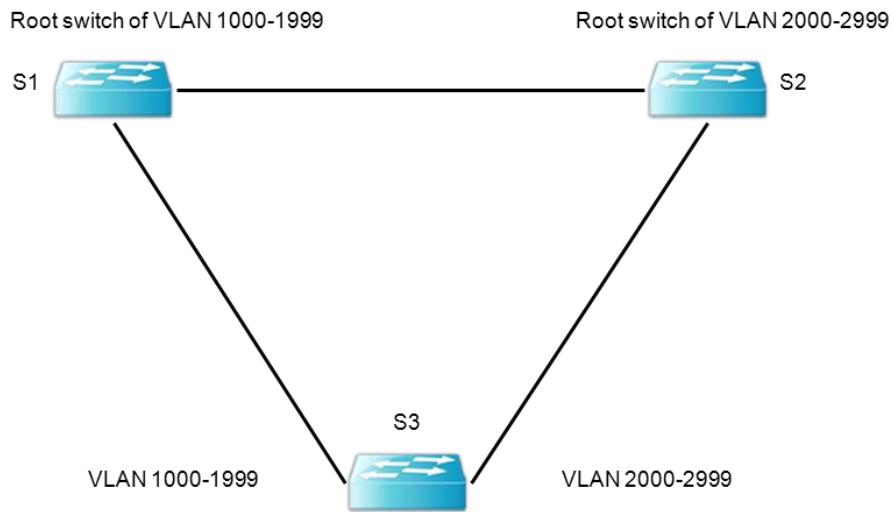


Figure 30 load balance over VLANs

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 switches having the same MST setting value is called one MST region. It defines the switches 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:

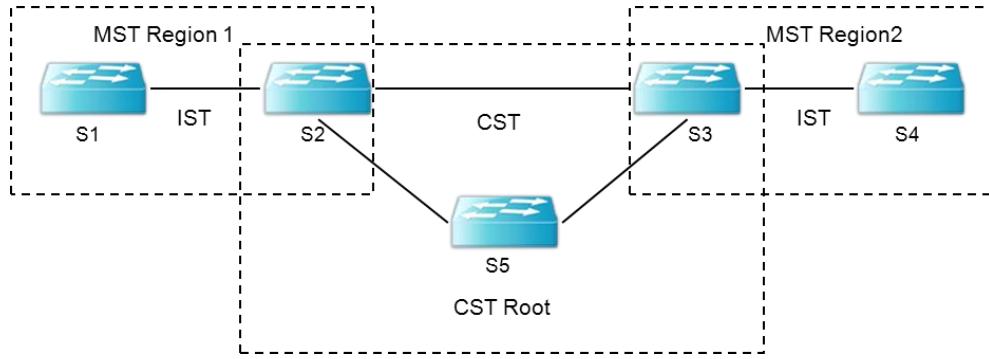


Figure 24 CST, IST, CIST

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 master. CST run not only each different MST region but also between the switches running with 802.1D or between 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:

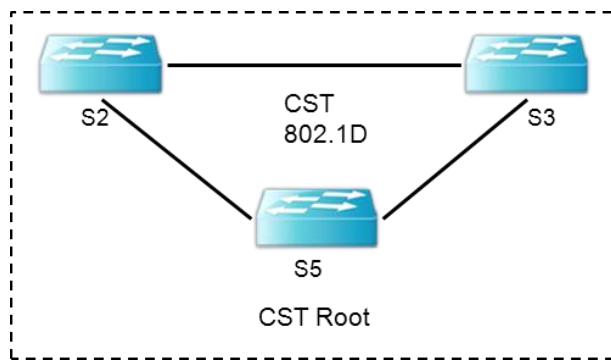


Figure 25 The network perceived at CST

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 171 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 a Bridge with up to 256 numbers. A VLAN can belong to only one Bridge. In the case of trunk VLAN, it can belong to only the 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.



Caution

If STP is not active and a network loop has been developed, it could degrade the network performance severely because of excessive traffic and unlimited packet duplication.

To enable STP, do the following steps on the Privileged mode.

	Command	pose
Step1	configure terminal	Enter to Global configuration.
Step2	spanning-tree enable	Enables STP on Default Bridge.
Step3	exit	Back to Privileged 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 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  
-----  
Giga6/2 Disb BLK 4 128.610 P2p  
  
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.



Notice

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 mode:

Step	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.

To enable STP in bridges other than the default bridge, use **bridge shutdown <1-256> bridge-forward** command in global configuration

mode. To remove the bridge use **no bridge <1-256>** command.

```
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 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 172 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 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 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
----- -----
Giga6/3 Disb BLK 4 128.138 P2p

Switch # configure terminal
Switch(config)#int GigabitEthernet 6/3
Switch(config-if-Giga6/3)#spanning-tree port-priority 0
Switch(config-if-Giga6/3)#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 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
----- -----
Giga6/3 Disb BLK 4 0.138 P2p

Switch#configure terminal
Switch(config)#interface GigabitEthernet 6/3
Switch(config-if-Giga6/3)#no spanning-tree port-priority
Switch(config-if-Giga6/3)#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 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
----- -----
Giga6/3 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.



Notice

Port group cannot decide the path cost by interface speed but each member port can have a different speed. Set path cost for the port group manually.

To configure the path cost of interface, follow the procedure set out below:

Table 173 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 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 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
Giga6/3	Disb	BLK	4	128.138	P2p

Switch#configure terminal

```
Switch(config)#interface GigabitEthernet 6/3
Switch(config-if-Giga6/3)#spanning-tree path-cost 10
Switch(config-if-Giga6/3)#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 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  

-----  

Giga6/3      Disb  BLK 10          128.138   P2p  

-----  

Switch#configure terminal  

-----  

Switch(config)#interface GigabitEthernet 6/3  

Switch(config-if-Giga6/3)#no spanning-tree path-cost  

Switch(config-if-Giga6/3)#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  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  

-----  

Giga6/3      Disb  BLK 4           128.138   P2p  

-----  

Switch#
-----
```

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 174 Configuring the Switch Priority of a VLAN

Step	Command	Purpose
Step1	configure terminal	To enter Global configuration mode
Step2	spanning-tree priority <i>priority</i>	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	exit	To return to Privileged mode.
Step4	show spanning	To check the setting
Step5	copy running-config startup-config	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**.

Use **bridge <1-256>** command rather than **spanning-tree** except for Default Bridge.

```
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
----- -----
Giga6/3 Disb BLK 4 128.138 P2p

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
----- -----
Giga6/3 Disb BLK 4 128.138 P2p

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
----- -----
Giga6/3 Disb BLK 4 128.138 P2p

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 175 Configuring the Hello Time

Step	Command	Purpose
Step1	configure terminal	To enter global configuration mode
Step2	spanning-tree hello-time seconds	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 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 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
----- -----
Giga6/3 Disb BLK 4 128.138 P2p

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 Foward 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
----- -----
Giga6/3 Disb BLK 4 128.138 P2p

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 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
----- -----
Giga6/3 Disb BLK 4 128.138 P2p
Switch#

```

Configuring the Forwarding-Delay Time for a VLAN

To configure the forwarding-delay time for a VLAN, perform the following the procedures:

Table 176 Configuring the Forwarding-Delay Time for a VLAN

Step	Command	Purpose
Step1	configure terminal	To enter Global configuration mode
Step2	spanning-tree forward-time seconds	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	(optional) Save the new configuration.

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
----- -----
Giga6/3 Disb BLK 4 128.138 P2p

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
-----
Giga6/3 Disb BLK 4 128.138 P2p

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 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
-----
Giga6/3 Disb BLK 4 128.138 P2p

Switch#

```

Configuring the Maximum-Aging Time for a VLAN

To configure the maximum-aging time, perform the following the procedure:

Table 177 Configuring the Maximum-Aging Time for a VLAN

Step	Command	Purpose
Step1	configure terminal	Enters global configuration mode
Step2	spanning-tree max-age seconds	Sets maximum-aging time seconds range is between 6 and 40. The default is 20.
Step3	exit	Returns to Privileged 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 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
----- -----
Giga6/3 Disb BLK 4 128.138 P2p

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 Foward Delay 15 sec

Bridge ID Priority 32768
Address 00077074ff01
Hello Time 2 sec Max Age 15 sec Foward Delay 15 sec
Aging Time 300

Interface Role Sts Cost Prio.Nbr Type
----- -----
Giga6/3 Disb BLK 4 128.138 P2p

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
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
----- -----
Giga6/3 Disb BLK 4 128.138 P2p

Switch#
```

Changing the Max-hops for switch

MSTP mode use hop count like TTL of IP instead of using max age and forward delay.

Step	Command	Purpose
Step1	configure terminal	Enters to global configuration mode.
Step2	Spanning-tree max-hops count	Changes max-hop.
Step3	exit	Backs to Privileged 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
-----
Giga6/3           Mstr    FWD 20000    128.138  P2p
Giga6/4           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
-----
Giga6/3           Mstr    FWD 20000    128.138  P2p
Giga6/4           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 178 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 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 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
Giga6/3	Disb	BLK	4	128.138	P2p

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 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
Giga6/3	Disb	DIS	4	128.138	P2p

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 Foward Delay 15 sec
```

Bridge ID	Priority	Address
32768	32768	00077074ff01

	Hello Time	2 sec	Max Age	20 sec	Forward Delay	15 sec
	Aging Time	300				
Interface	Role	Sts	Cost		Prio.Nbr	Type
Giga6/3	Disb	BLK	20000		128.138	P2p

Configuring portfast for switch

You can configure all the port in the C9500 series to have bpdu-filter and bpdu-guard features. The option ‘bpdu-filter’ is for blocking the incoming bpdu to the port meanwhile ‘bpdu-guard’ is for turning the port to block state when bpdu come into the port.

The following example shows how to set portfast for switch:

	Command	Purpose
Step1	configure terminal	Enter the Global configuration mode.
Step2	spanning-tree portfast {bpdu-filter bpdu-guard }	Sets the portfast to every port.
Step3	exit	Enter the Privileged 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 gi6/3
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
Giga6/3: Port 138 - Id 808a - Role Rootport - State Forwarding
Giga6/3: Designated Path Cost 0
Giga6/3: Configured Path Cost 4 - Add type Explicit ref count 1
Giga6/3: Designated Port Id 8001 - Priority 128 -
Giga6/3: Root 80000007709e12fd
Giga6/3: Designated Bridge 80000007709e12fd
Giga6/3: Message Age 0 - Max Age 20
Giga6/3: Hello Time 2 - Forward Delay 15
Giga6/3: Forward Timer 0 - Msg Age Timer 4 - Hello Timer 0 - topo change timer 0
Giga6/3: forward-transitions 1
Giga6/3: Version Rapid Spanning Tree Protocol - Received RSTP - Send RSTP
Giga6/3: No portfast configured - Current portfast off
Giga6/3: portfast bpdu-guard default - Current portfast bpdu-guard off
Giga6/3: portfast bpdu-filter default - Current portfast bpdu-filter off
Giga6/3: no root guard configured - Current root guard off
Giga6/3: Configured Link Type point-to-point - Current point-to-point
```

```

Switch(config)#spanning-tree portfast bpdu-filter
Switch(config)#do show spa inter gi6/3
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
Giga6/3: Port 138 - Id 808a - Role Rootport - State Forwarding
Giga6/3: Designated Path Cost 0
Giga6/3: Configured Path Cost 4 - Add type Explicit ref count 1
Giga6/3: Designated Port Id 8001 - Priority 128 -
Giga6/3: Root 80000007709e12fd
Giga6/3: Designated Bridge 80000007709e12fd
Giga6/3: Message Age 0 - Max Age 20
Giga6/3: Hello Time 2 - Forward Delay 15
Giga6/3: Forward Timer 0 - Msg Age Timer 4 - Hello Timer 0 - topo change timer 0
Giga6/3: forward-transitions 1
Giga6/3: Version Rapid Spanning Tree Protocol - Received RSTP - Send RSTP
Giga6/3: No portfast configured - Current portfast off
Giga6/3: portfast bpdu-guard default - Current portfast bpdu-guard off
Giga6/3: portfast bpdu-filter default - Current portfast bpdu-filter on
Giga6/3: no root guard configured - Current root guard off
Giga6/3: Configured Link Type point-to-point - Current point-to-point

```



Notice

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)

Step	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 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
-----
Giga6/3        Mstr    FWD 20000    128.138  P2p
Giga6/4        Altn    BLK 20000    128.139  P2p

C9500_112(config)#no spanning-tree transmit-holdcount
C9500_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
-----
Giga6/3        Mstr    FWD 20000    128.138  P2p
Giga6/4        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 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 mode.
Step4	show running-config	Shows current running configuration.
Step5	copy running-config startup-	Saves current running configuration to startup-

	config	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.



Notice

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 mode:

Table 179 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 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 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
----- -----
Giga6/3 Disb BLK 4 128.138 P2p

Switch#configure terminal
Switch(config)#interface GigabitEthernet 6/3
Switch(config-if-Giga6/3)#spanning-tree edgeport
Switch(config-if-Giga6/3)#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
-----  -----  -----  -----  -----
Giga6/3            Disb BLK 4       128.138      P2p edge port

Switch#configure terminal
Switch(config)#interface GigabitEthernet 6/3
Switch(config-if-Giga6/3)#no spanning-tree edgeport
Switch(config-if-Giga6/3)#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
-----  -----  -----  -----  -----
Giga6/3            Disb BLK 4       128.138      P2p

Switch#

```

Specifying the Link Type to Ensure Rapid Transitions

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

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.



Notice

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 mode:

Table 180 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 mode.
Step5	show running-config	Views the settings.
Step6	copy running-config startup-	Stores the (option) settings in the configuration file.

	config	
--	---------------	--

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

Configuring force-version for port

For the sake of STP compatibility the port can keep the version of RSTP or MSTP so that it can operate according to the set version.

To set force-version on port, do the following steps on Privileged mode:

	Command	Pose
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 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

Giga6/3: Port 138 - Id 808a - Role Rootport - State Forwarding

Giga6/3: Designated Path Cost 0

Giga6/3: Configured Path Cost 4 - Add type Explicit ref count 1

Giga6/3: Designated Port Id 8001 - Priority 128 -

Giga6/3: Root 80000007709e12fd

Giga6/3: Designated Bridge 80000007709e12fd

Giga6/3: Message Age 0 - Max Age 20

Giga6/3: Hello Time 2 - Forward Delay 15

Giga6/3: Forward Timer 0 - Msg Age Timer 5 - Hello Timer 0 - topo change timer 0

Giga6/3: forward-transitions 1

Giga6/3: Version Rapid Spanning Tree Protocol - Received RSTP - Send RSTP

Giga6/3: No portfast configured - Current portfast off

Giga6/3: portfast bpdu-guard default - Current portfast bpdu-guard off

Giga6/3: portfast bpdu-filter default - Current portfast bpdu-filter off

Giga6/3: no root guard configured - Current root guard off

Giga6/3: Configured Link Type point-to-point - Current point-to-point

Switch(config)#inter gi6/3

```

Switch(config-if-Giga6/3)#spanning-tree force-version 0
Switch(config-if-Giga6/3)#do show spa inter gi6/3
    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
        Giga6/3: Port 138 - Id 808a - Role Designated - State Discarding
        Giga6/3: Designated Path Cost 4
        Giga6/3: Configured Path Cost 4 - Add type Explicit ref count 1
        Giga6/3: Designated Port Id 808a - Priority 128 -
        Giga6/3: Root 80000007709e12fd
        Giga6/3: Designated Bridge 8000000770dead99
        Giga6/3: Message Age 1 - Max Age 20
        Giga6/3: Hello Time 2 - Forward Delay 15
        Giga6/3: Forward Timer 14 - Msg Age Timer 0 - Hello Timer 0 - topo change timer 34
        Giga6/3: forward-transitions 1
        Giga6/3: Version Spanning Tree Protocol - Received None - Send STP
        Giga6/3: No portfast configured - Current portfast off
        Giga6/3: portfast bpdu-guard default - Current portfast bpdu-guard off
        Giga6/3: portfast bpdu-filter default - Current portfast bpdu-filter off
        Giga6/3: no root guard configured - Current root guard off
        Giga6/3: Configured Link Type point-to-point - Current point-to-point

```

Configuring root guard for port

This is used to prevent the switch that is connected to the port from being the root switch. In case Root guard is configured, even if superior BPDU is transferred, they are to be ignored. This feature is only for MSTP.

To set root guard on port, do the following steps on Privileged 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 mode.
Step4	show running-config	Shows current running configuration.
Step5	copy running-config startup-config	Saves current running configuration to startup-configuration.

```

Giga6/3 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 gi6/3
Switch(config-if-Giga6/3)#spanning-tree guard root
Switch(config-if-Giga6/3)#do show spa mst inter gi6/3
Giga6/3 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 is the same as setting of a switch except entering interface mode.

Configuring portfast for port

You can set portfasper port. This is the same as setting of a switch except entering interface mode.

Configuring transmit-holdcount for port

You can set transmit-holdcount per port. This is the same as setting of a switch except entering interface mode.

Configuring restricted-role for port

This is used to prevent the specified port from being the root port in MSTP mode.

To set restricted-role for port, do the following steps on Privileged mode:

	Command	Purpose
Step1	configure terminal	Enters global configuration mode.
Step2	Interface <i>interface-id</i>	Enters interface configuration mode.
Step3	spanning-tree restricted-role	Sets restricted-role on port.
Step4	exit	Back to Privileged mode.
Step5	show running-config	Shows current running configuration.
Step6	copy running-config startup-config	Saves current running configuration to startup-configuration.

```

C9500_112(config)#inter gi6/3
C9500_112(config-if-Giga6/3)#spanning-tree restricted-role
C9500_112(config-if-Giga6/3)#do show spa

```

```

Default Bridge up - Spanning Tree Enabled rstp-vlan-bridge
Root ID Priority 32768
          Address 0007709e12fd
          Cost 4
          Port 139 (Giga6/4)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32768
          Address 000770dead99
          Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
          Aging Time 300

Interface      Role Sts Cost Prio.Nbr Type
-----  

Giga6/3      Aln  BLK 4    128.138   P2p
Giga6/4        Root FWD 4    128.139   P2p

C9500_112(config-if-Giga6/3)#no spanning-tree restricted-role
C9500_112(config-if-Giga6/3)#do show spa

Root ID Priority 32768
          Address 0007709e12fd
          Cost 20000
          Port 138 (Giga6/3)
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32768
          Address 000770dead99
          Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
          Aging Time 300

Interface      Role Sts Cost Prio.Nbr Type
-----  

Giga6/3      Root FWD 4    128.138   P2p
Giga6/4        Aln  BLK 4    128.139   P2p

```

Configuring restricted-tcn for port

You can configure the specified port not to receive tcn BPDU.

To set restricted-role for port, do the following steps on Privileged mode.

	Command	Purpose
Step1	configure terminal	Enters global configuration mode.
Step2	Interface <i>interface-id</i>	Enters interface configuration mode.
Step3	spanning-tree restricted-tcn	Sets restricted-tcn on port.
Step4	exit	Back to Privileged mode.
Step5	show running-config	Shows current running configuration.

Step6	copy running-config startup-config	Saves current running configuration to startup-configuration.
--------------	---	---

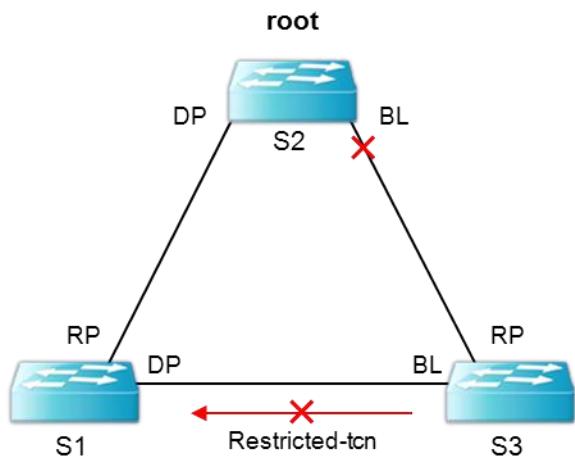


Figure 26 restricted-tcn

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 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 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 6/3
Switch(config-if-Giga6/3)#spanning-tree instance 1
Switch(config-if-Giga6/3)#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 mode:

	Command	Purpose
Step1	configure terminal	Enters Global configuration mode.
Step2	Spanning-tree instance <i>instance-id</i> priority <i>priority</i>	Sets priority on Instance.
Step3	exit	Back to Privileged mode.
Step4	show running-config	Shows current running configuration.
Step5	copy running-config startup-config	(Optional)Saves current running configuration to startup-configuration.

To return to default value, use **no spanning-tree instance *instance-id* priority** 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
-----
Giga6/3       Disb     BLK 20000    128.138  P2p

```

```

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
-----
Giga6/3       Disb     BLK 20000    128.138  P2p
Switch#

```

To set the priority to a port, follow the steps below in Privileged mode.

	Command	Purpose
Step1	configure terminal	Enter Global configuration mode.
Step2	interface <i>interface-id</i>	Enter interface configuration mode by specifying the intended interface.
Step3	Spanning-tree instance <i>instance-id</i> priority <i>priority</i>	Assign priority to the port.
Step4	exit	Get back to Privileged mode.
Step5	show running-config	Check out the configuration is made.
Step6	copy running-config startup-config	(Optional) Modified configuration is to be save as a file.

To return to default value, use **no spanning-tree instance *instance-id* priority** 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
-----
Giga6/3       Disb    BLK 20000     128.138  P2p
```

```
Switch#configure terminal
Switch(config)#interface GigabitEthernet 6/3
Switch(config-if-Giga6/3)#spanning-tree instance 1 priority 0
Switch(config-if-Giga6/3)#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
-----
Giga6/3       Disb    BLK 20000     0.138   P2p
```

```
Switch#configure terminal
Switch(config)#interface GigabitEthernet 6/3
Switch(config-if-Giga6/3)#no spanning-tree instance 1 priority
Switch(config-if-Giga6/3)#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
Giga6/3 Switch#	Disb	BLK 20000	128.138	P2p

To set the path cost value of port, do the following steps on Privileged 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</i> path-cost <i>path-cost</i>	Sets path cost on port.
Step4	exit	Back to Privileged 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
-----------	------	----------	----------	------

Giga6/3	Disb	BLK 20000	128.138	P2p
---------	------	-----------	---------	-----

Switch#configure terminal

Switch(config)#interface GigabitEthernet 6/3

Switch(config-if-Giga6/3)#**spanning-tree instance 1 path-cost 1**

Switch(config-if-Giga6/3)#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
-----------	------	----------	----------	------

Giga6/3	Disb	BLK 1	128.138	P2p
---------	------	-------	---------	-----

Switch#configure terminal

Switch(config)#interface GigabitEthernet 6/3

```

Switch(config-if-Giga6/3)#no spanning-tree instance 1 path-cost
Switch(config-if-Giga6/3)#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
-----
Giga6/3       Disb    BLK 20000    128.138  P2p
Switch#

```



Notice

To set MSTP on the port, you must create instance first.

Setting region and revision number for MST

Any switch that belongs to a same MST should keep same MST configuration. ‘Region’ and ‘revision number’ are the items included in MST configuration.

To set revision number and Region, do the following steps on Privileged mode.

	Command	Purpose
Step1	configure terminal	Enters global configuration mode.
Step2	spanning-tree mst configuration	Enters mst configuration mode.
Step3	Region NAME	Sets region name.
Step4	Revision number	Sets revision number.
Step5	exit	Back to Privileged 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 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
-----
Giga6/3 Disb BLK 4 128.138 P2p
```

```
Switch#show spanning-tree interface gi6/3
% 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
% Giga6/3: Port 138 - Id 8263 - Role Disabled - State Discarding
% Giga6/3: Designated Path Cost 0
% Giga6/3: Configured Path Cost 4 - Add type Explicit ref count 1
% Giga6/3: Designated Port Id 0 - Priority 128 -
% Giga6/3: Root 000000077074ff01
% Giga6/3: Designated Bridge 000000077074ff01
% Giga6/3: Message Age 0 - Max Age 0
% Giga6/3: Hello Time 0 - Forward Delay 0
% Giga6/3: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change timer 0
```

```
% Giga6/3: forward-transitions 0
% Giga6/3: Version Rapid Spanning Tree Protocol - Received None - Sext STP
% Giga6/3: No portfast configured - Current portfast off
% Giga6/3: portfast bpdu-guard default - Current portfast bpdu-guard off
% Giga6/3: portfast bpdu-filter default - Current portfast bpdu-filter off
% Giga6/3: no root guard configured - Current root guard off
% Giga6/3: Configured Link Type point-to-point - Current P2p
%
%
```

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 flag not 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 (Giga6/3)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 P2p
BPDU: sent 0
```

Switch#



Notice

show spanning-tree interface IFNAME command does not run in MSTP.

Configuring Bridge MAC Forwarding

To make a Layer 2 Ethernet network operate, L2 frames can be sent to the intended destination interface, which requires comparing the MAC address of the frame with the MAC address table. For this, the MAC address table should be built up in advance. The process that collects all the MAC address and assigns them into the MAC address table is called MAC learning. There are two ways to achieve MAC learning – Dynamic MAC learning and Static MAC learning.

To do MAC learning, do the following commands on config mode:

mand	pose
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.

Use **bridge <1-256> mac-address-table static MAC (forward|discard) IFNAME** command except for Default Bridge.

The following example shows how to set MAC learning statically:

```
Switch#configure terminal
Switch(config)#mac-address-table static 1111.1111.1111 forward gi6/3
Switch(config)#exit
Switch#show mac-address-table

      vlan    mac address      type      fwd          ports
-----+-----+-----+-----+
      1  1111.1111.1111  static   1 Gi6/3
Switch(config)#no mac-address-table static 1111.1111.1111 forward gi6/3
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:

mand	pose
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 multicast MAC address entry in the relevant Bridge.

Use clear mac-address-table (dynamic|multicast|static) (address MACADDR | interface IFNAME | vlan VID) bridge <1-256> command except for Default 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 Gi6/3

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.

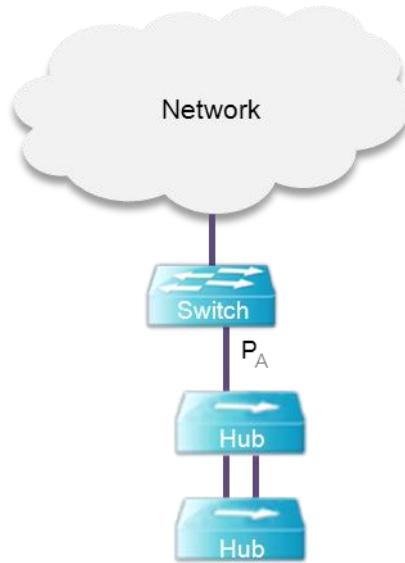


Figure 27 Environment Where a Self-loop is Formed

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).

Default SLD Configuration

The table below shows the default setting of SLD.

Table 181 Default SLD Configuration

Feature	Default Setting
System SLD enable	Disable
Interface SLD enable	Disable
Loop detection action	Port shutdown
Port check	Disable
Hello time	2 seconds

Configuring Self-loop Detection

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

- Configuring SLD PDU Policy-MAP
- Enabling Self-loop Detection on System
- Enabling Self-loop Detection on Interface
- Changing The Service Status of Port
- Disabling Self-loop Detection
- Disabling SLD Port Check (option)
- Changing SLD Interval (option)
- Changing SLD Action (option)

Enabling Self-loop Detection on System

To activate the SLD function of the switch, follow the steps below in Privileged mode.

	Command	Purpose
Step1	<i>Configure terminal</i>	Enter Global configuration mode.
Step2	sld enable	Activate SLD function of the system.
Step3	end	Return to Privileged mode.
Step4	show running-config	Check out the configuration is made.
Step5	copy running-config startup-config	(Optional) Save the modified configuration to a file.

Enabling Self-loop Detection on Interface

You can active the SLD function per each port. The default option for SLD function is ‘Not active’. To activate the SLD function per port of the switch, follow the steps below in Privileged mode.

	Command	Purpose
Step1	<i>Configure terminal</i>	Enter Global configuration mode.
Step2	interface interface-name	Enter Interface configuration mode.
Step3	sld enable	Activate SLD function.
Step4	end	Return to Privileged mode.
Step5	show running-config	Check out the configuration is made.
Step6	copy running-config startup-config	(Optional) Save the modified configuration to a file.

The below example shows how to activate SLD function for gi6/1 port.

```
Switch# configure terminal
Switch(config)# interface gi6/1
Switch(config-if-Giga6/1)# sld enable
Switch(config-if-Giga6/1)# service-policy input SLD_PDU
Switch(config-if-Giga6/1)# end
Switch# show sld
Interface  Enable  Flag   Sts    Link  Count  Last change
Gi6/1      yes     PL     ok     up    0      00:00:02
Gi6/2      no      PL     n/a    down  0      n/a
Gi6/3      no      PL     n/a    down  0      n/a
Gi6/4      no      PL     n/a    down  0      n/a
.....
Switch#
```

Changing the Service Status of Port

You can enable the locked port which has been set to be disabled by SLD function. For this use the below command in Privileged mode.

	Command	Purpose
Step1	clear sld interface-type portID	Have the port to be enabled.
Step2	show ip interface brief	Display the port status.

Disabling Self-loop Detection

To deactivate the SLD detection function, follow the steps below in Privileged mode.

Table 182 Disabling Self-loop Detection

	Command	Purpose
Step1	<i>Configure terminal</i>	Enter Global configuration mode.
Step2	interface interface-name	Enter Interface configuration mode.
Step3	no sld enable	Deactive the SLD detection function. The port that were shut down by SLD will be released.
Step4	end	Return to Privileged mode.
Step5	show running-config	Check out the configuration is made.
Step6	copy running-config startup-config	(Optional) Save the modified configuration to a file.

The below example shows how to deactivate the SLD function for port gi6/1:

```
Switch# configure terminal
Switch(config)# interface gi6/1
Switch(config-if-Giga6/1)# no service-policy input SLD_PDU
Switch(config-if-Giga6/1)# no sld enable
Switch(config-if-Giga6/1)# end
Switch# show sld
Interface  Enable  Flag   Sts    Link   Count  Last change
Gi6/1      no      PL     ok     up     0      n/a
Gi6/2      no      PL     n/a    down   0      n/a
Gi6/3      no      PL     n/a    down   0      n/a
Gi6/4      no      PL     n/a    down   0      n/a
.....
Switch#
```

Disabling SLD Port Check

If you disable SLD port-check function of a port, the switch will not check out the port for SLD packet transmission when it determine if a self-loop is developed. In order to detect a loop when receiving SLD packets from other ports, you should deactivate the port-check function for the ports that are involved. To deactivate the SLD port-check function, follow the below steps in Privileged mode.

	Command	Purpose
Step1	<i>Configure terminal</i>	Enter Global configuration mode.
Step2	interface interface-name	Enter Interface configuration mode.
Step3	no sld port-check	Deactive the SLD port-check function.
Step4	end	Return to Privileged mode.
Step5	show running-config	Check out the configuration is made.

Step6	copy running-config startup-config	(Optional) Save the modified configuration to a file.
--------------	---	---

The below example shows how to deactivate SLD port-check function for port gi6/1:

```

Switch# configure terminal
Switch(config)# interface gi6/1
Switch(config-if-Giga6/1)# no sld port-check
Switch(config-if-Giga6/1)# end
Switch# show sh sld parameters
Global SLD information:
Protocol version: 1
SLD is enabled

Interface  Enable  Hello  Action      Option
Gi6/1      yes      2      link down
Gi6/2      no       2      link down  port-check
Gi6/3      no       2      link down  port-check
Gi6/4      no       2      link down  port-check
.....
Switch#

```

Changing SLD Interval

To modify the transmission period for SLD PDU, follow the below steps in Privileged mode.

	Command	Purpose
Step1	<i>Configure terminal</i>	Enter Global configuration mode.
Step2	interface interface-name	Enter Interface configuration mode.
Step3	sld interval <1-10>	Modify the transmission period for SLD PDU.
Step4	end	Return to Privileged mode.
Step5	show running-config	Check out the configuration is made.
Step6	copy running-config startup-config	(Optional) Save the modified configuration to a file.

The below example shows how to modify the transmission period for SLD PDU to be 5 seconds for port gi6/1:

```

Switch# configure terminal
Switch(config)# interface gi6/1
Switch(config-if-Giga6/1)# sld interval 5
Switch(config-if-Giga6/1)# end
Switch# show sh sld parameters
Global SLD information:
Protocol version: 1
SLD is enabled

Interface  Enable  Hello  Action      Option
Gi6/1      yes      5      link down  port-check
Gi6/2      no       2      link down  port-check
Gi6/3      no       2      link down  port-check
Gi6/4      no       2      link down  port-check
.....
Switch#

```

Changing SLD Action

To change the SLD operation so that it will display log information rather than turn it to disabled state when a self-loop is detected. For this, follow the below steps in Privileged mode.

	Command	Purpose
Step1	<i>Configure terminal</i>	Enter Global configuration mode.
Step2	interface interface-name	Enter Interface configuration mode.
Step3	sld notify-only	Change the SLD operation to display log information.
Step4	end	Return to Privileged mode.
Step5	show running-config	Check out the configuration is made.
Step6	copy running-config startup-config	(Optional) Save the modified configuration to a file.

The below example shows how to set SLD operation to display log information for port gi6/1.

```

Switch# configure terminal
Switch(config)# interface gi6/1
Switch(config-if-Giga6/1)# sld notify-only
Switch(config-if-Giga6/1)# end
Switch# show sh sld parameters
Global SLD information:
Protocol version: 1
SLD is enabled

Interface  Enable  Hello  Action      Option
Gi6/1      yes     2       notify     port-check
Gi6/2      no      2       link down  port-check
Gi6/3      no      2       link down  port-check
Gi6/4      no      2       link down  port-check
.....
Switch#

```

Displaying Self-loop Status

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

For the case of “**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 cau
sed by SLD (minute:second)
* count : Number of shutdown events caused by SLD

* last-occur : The last shutdown time

```

To display the SLD operation status, use **show sld** command in Privileged mode.

```

Switch# show sld
Interface  Enable  Flag   Sts    Link Count  Last change
Gi6/1      no      PL     n/a    up      0  n/a
Gi6/2      no      PL     n/a    down    0  n/a
Gi6/3      no      PL     n/a    down    0  n/a
Gi6/4      no      PL     n/a    down    0  n/a
.....

```

Switch#

Chapter 14. *BFD (Bidirectional Forwarding Detection)*

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 C9500 series 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 desided 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 or routing protocol. If BFD detects an error, it informs the routing protocol. As a routing protocol can rapidly reaccount the routing table, it can reduce the time taken to change the 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 an OSPF neighbor.

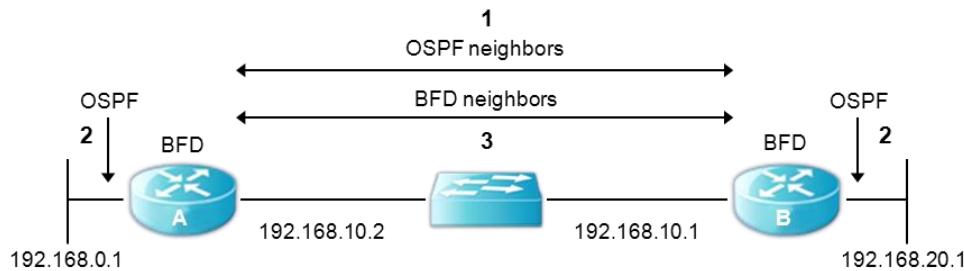


Figure 28 Establishing a BFD neighbor relationship

The following figure shows the link error to occur in the network. If the OSPF neighbor and BFD session is down, the BFD informs the OSPF process that the system can not communicate with BFD peer. The OSPF process disconnects the OSPF neighbor relation. If another path is available, the router recalculates the routing table immediately.

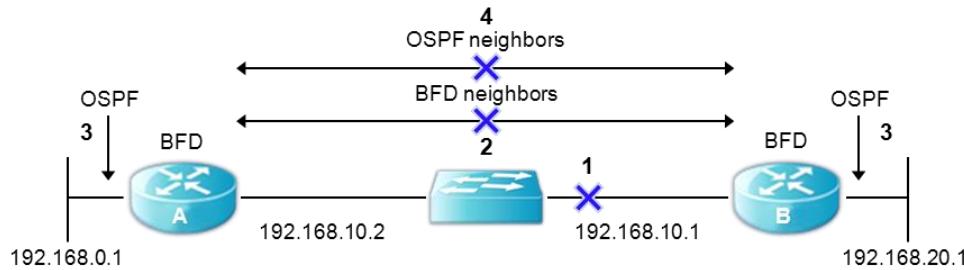


Figure 29 Tearing down an OSPF neighbor relationship

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 the C9500 series with the **bfd interval** command, BFD single hop session is made.



Figure 30 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.

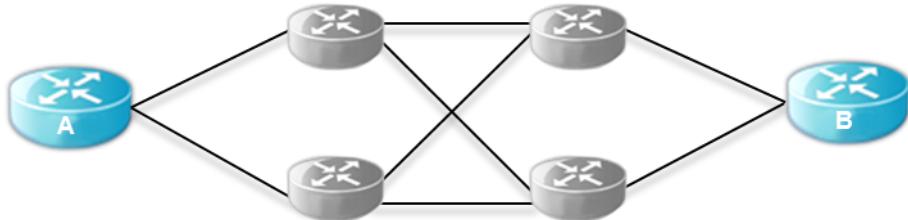


Figure 31 BFD multihop session

BFD Version Interoperability

The C9500 series 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 the C9500 series 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 183 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 184 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 interface-name Example: Switch(config)# interface gi7/1	Enter the interface configuration mode.
Step 3	ip address ip-address/prefix-length Example: Switch(config-if-Giga7/1)# ip address 33.1.1.1/24	Sets IP address on interface.
Step 4	bfd interval milliseconds min_rx milliseconds multiplier interval-multiplier Example: Switch(config-if-Giga7/1)# bfd interval 750 min_rx 500 multiplier 3	Sets BFD parameter on interface.
Step 5	end Example: Switch(config-if-Giga7/1)# end	Returns the Privileged mode.

Notice 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 185 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 milliseconds 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.

Configuring BFD support for BGP

To configure BFD on BGP, do the following tasks.

Table 186 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.

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 187 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 gi7/1	Enter interface configuration mode.
Step 6	bfd interval milliseconds min_rx milliseconds multiplier interval-multiplier Example: Switch(config-if-Giga7/1)# 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 gi7/1	Enters interface configuration mode (Optional).
Step 8	ip ospf bfd [disable] Example: Switch(config-if-Giga7/1)# ip ospf bfd disable	Disable BFD session for specific OSPF interface. disable keyword command must be used only for interface enabled BFD.
Step 9	end Example: Switch(config-if-Giga7/1)# end	Return to Privileged 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 188 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 gi7/1	Enters interface configuration mode.
Step 3	bfd interval milliseconds min_rx milliseconds multiplier interval-multiplier Example: Switch(config-if-Giga7/1)# bfd interval 750 min_rx 500 multiplier 3	Sets BFD parameter on interface.
Step 4	ip ospf bfd [disable] Example: Switch(config-if-Giga7/1)# ip ospf bfd	Sets to make BFD session via OSPF interface.
Step 5	end Example: Switch(config-if-Giga7/1)# end	Return to Privileged mode.

Configuring BFD support for Static routing

In static routing, you should configure the gateway of the static routing network to be the BFD peer. To configure BFD for Static routing, do the following tasks:

Table 189 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 gi7/1	Enters the interface configuration mode.
Step 3	ip address ip-address/prefix-length Example: Switch(config-if-Giga7/1)# 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-Giga7/1)# bfd interval 750 min_rx 500 min 3	Sets BFD session parameter value on interface.
Step 5	Exit Example: Switch(config-if-Giga7/1)# exit	Return to global configuration mode.
Step 6	ip route A.B.C.D/M gateway-addr Example: Switch(config)# ip route 7.0.0.0/8 1.1.1.254	Sets static router.
Step 7	ip route static bfd IFNAME gateway-addr Example: Switch(config)# ip route static bfd gi7/1 1.1.1.254	Assign BFD neighbor of static route.
Step 8	end Example: Switch(config)# end	Return to Privileged mode.

Configuring Passive Mode on the Interface

After BFD passive mode receives a packet from another BFD neighbor to BFD control, it will start to send a BFD control packet. In other words, it does not send BFD control packet first. If BFD runs in passive mode, you set the interface with the following tasks.

If you set all routers in the network with BFD passive mode, the BFD does not run. At least the BFD of one system must run with active mode.

Table 190 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 interface-name Example: Switch(config)# interface gi7/1	Enters interface configuration mode.
Step 3	bfd passive Example: Switch(config-if-Giga7/1)# bfd passive	Sets interface with BFD passive mode.
Step 4	end Example: Switch(config-if-Giga7/1)# end	Return to Privileged mode.

Configuring BFD Echo Mode

The system that receives a BFD echo packet from the BFD echo mode returns this packet to the sending system. In the case of using a 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 191 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 mode.

Configuring BFD slow timer

When BFD neighbors do not recognize each other, it would be of no use to transmit BFD control packets according to the set interval which has been configured by **bfd interval** command. To modify the transmission interval of BFD control packets, use **bfd slow-timer** command.

Table 192 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 milliseconds Example: Switch(config)# bfd slow-timer 2000	Sets BFD slow timer.
Step 3	end Example: Switch(config)# end	Returns Privileged mode.

Displaying BFD information

Table 193 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 an OSPF network. Let us assume the following network configuration:

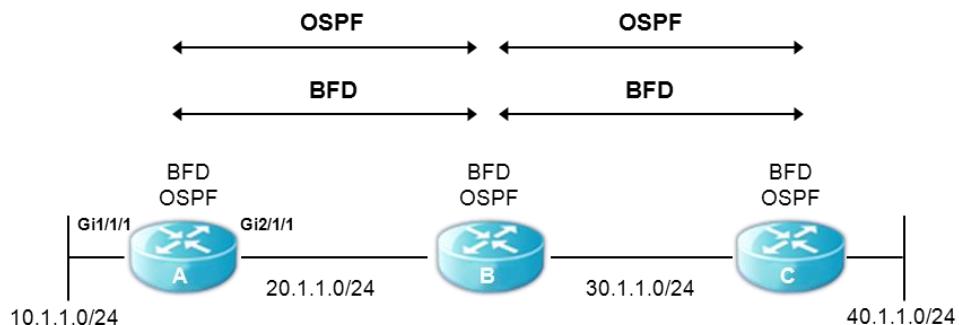


Figure 32 Configuring BFD in an OSPF Network

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 194 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 gi7/1 Switch_A(config-if-Giga7/1)# 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 gi6/1/1 Switch_A(config-if-Giga6/1/1)# ip ospf bfd disable
Step 5	Shows BFD peer information. Switch_A# show bfd neighbors


Notice

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 the switch is as follows:

```
!
interface Giga6/1/1
  ip address 10.1.1.1/24
  ip ospf bfd disable
!
interface Giga7/1
  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 195 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 gi7/1 Switch_A(config-if-Giga7/1)# bfd interval 300 min_rx 300 multiplier 3
Step 3	Sets BFD on the specific OSPF interface.

	<pre>Switch_A# configure terminal Switch_A(config)# interface gi7/1 Switch_A(config-if-Giga7/1)# ip ospf bfd</pre>
Step 4	<p>Shows BFD peer information..</p> <p>Shows BFD peer.</p> <pre>Switch_A# show bfd neighbors</pre>

The configuration of switch is as follows:

```
!
interface Giga7/1
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 a BGP Network

The example below describes the way to use BFD in a BGP network.

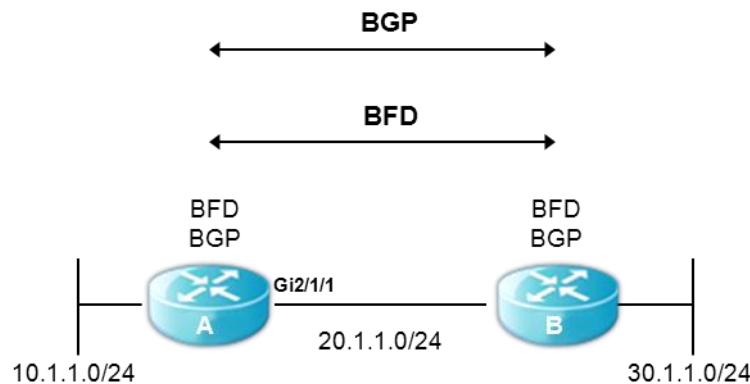


Figure 40 Configuring BFD in a BGP Network

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 196 Configuring BFD in a 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 gi7/1 Switch_A(config-if-Giga7/1)# 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 Giga7/1
ip address 20.1.1.24
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 197 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 Giga7/1
  ip address 20.1.1.24
!
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:

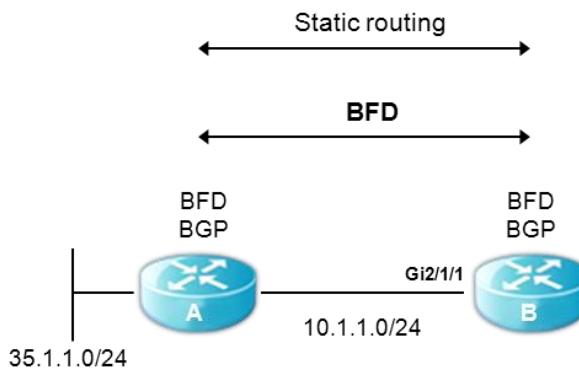


Figure 33 Configuring BFD for static routing

If you use the BFD to check that the next-hop to specific static router is active, do the following tasks:

Table 198 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 gi7/1 Switch_B(config-if-Giga7/1)# 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 gi7/1 10.1.1.254
Step 4	Shows BFD peer information. Switch_B# show bfd neighbors



Notice

To make BFD session to be UP status, you must also set BFD on Switch A connected with Switch B interface.

The configuration of Switch_B is as follows:

```
!
interface Giga7/1
    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 gi7/1 10.1.1.254
!
```

Chapter 15. ***LACP (Link Aggregation Control Protocol)***

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

This chapter consists of the following sections:

- Understanding the Link Aggregation Control Protocol
- Configuring 802.3ad Link Aggregation Control Protocol 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 Composition

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 199 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

The port group configuration of the C9500 series can be done manually or automatically with IEEE 802.3ad LACP (Link Aggregation Control Protocol).

To configure a 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 ports in passive mode passively responding to initiation and never initiating the sending of LACP packets.

The following shows a possible mode in LACP:

Table 200 LACP Modes

Mode	Description
on	This mode does 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. The higher number represents a lower priority. The default priority is 32768.

To specify LACP system priority, follow the steps below from Privileged mode:

Table 201 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 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 a 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. The higher number represents a lower priority with the default priority being 32768.



Note

Only the ports which belong to the Channel-group of LACP protocol can be configured for Port Priority.

To specify the port priority, follow the step below from Privileged mode.

Table 202 Specifying the Timeout Value

Step	Command	Purpose
Step1	configure terminal	To enter global configuration mode.
Step2	interface interface-id	To enter to interface configuration mode.
Step3	lacp port-priority priority	To specify the port priority
Step4	end	To return to Privileged 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 Mode:

Table 203 Specifying the Timeout Value

Step	Command	Purpose
Step1	configure terminal	To enter global configuration mode
Step2	interface interface-id	Enter to interface configuration mode.
Step3	lacp timeout {short long}	To specify LACPDU Timeout
Step4	end	To return to Privileged 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
```

Configuring 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 Mode.

Table 204 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 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 7/1 as a port-group 1 member.

```
Switch# configure terminal
Switch(config)# interface Giga7/1
Switch(config-if- Giga7/1)# channel-group 1 mode active
Switch(config)# end
```

The following example shows how to create port-group by static mode rather than LACP.

```
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.

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

The C9500 series provides various commands to show the information of all ports.

Table 205 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 connected with port group.
show etherchannel load-balance	Shows the information of load balance mode which are applied to 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 = Up Mstr In-Bndl
Channel group = 1           Mode = On           Gcchange = -
```

```

Port-channel = Port-channel1    GC = -          Pseudo port-channel= Port-channel1
Port index   = 0                Load = 0xFF
Protocol     = -
Age of the port in the current state: 0d:00h:00m:31s

Port-channels in the group:
-----
Port-channel: Port-channel1
-----
Age of the Port-channel = 0d:00h:05m:06s
Number of ports = 1
GC              = 0x00000000  HotStandBy port= null
Port state      = Up Mstr In-Bndl
Protocol        = -
Ports in the Port-channel:
Index  Load  Port       EC state  No of bits
-----+-----+-----+-----+
  0    FF    Gi6/1      On      4
Time since last port bundled: 0d:00h:00m:31s  Giga6/1
Time since last port un-bundled: 0d:00h:00m:34s Giga6/1

```

To search/check LACP statistics, use the Privileged command **show lacp counters**.

To search/check LACP statistics of the specific port group, use the Privileged command **show lacp aggregator-id counters**.

To search/check LACP protocol information and status of switch, use the Privileged command **show lacp internal**. To search/check LACP protocol information and status of the relative switch, use the Privileged command **show lacp neighbor**.

Chapter 16. ***IP-OPTION***

This chapter describes the IP-option of system.

IP option is the function to enable/disable the parameters related to attack prevention of the parameters under /proc/sys/net/ipv4 provided by linux kernel.

IP OPTION Command Parameters

The parameters that can be set by **IP option** command are as follows.

Table 206 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 <i>VALUE</i>	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 <i>VALUE</i>	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 <i>VALUE</i>	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 <i>VALUE</i>	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 <i>VALUE</i>	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

Chapter 17. *VRRP (Virtual Router Redundancy Protocol)*

This chapter describes the VRRP configuration of system.

Virtual Router Redundancy Protocol (VRRP) is a protocol that allows two or more routers to have the same virtual IP address to provide multiple access routes in the LAN, with one of the routers elected as a virtual router. VRRP router uses VRRP protocol to communicate with other routers connected to the LAN. If a router is elected as a master virtual router in VRRP configuration, the other routers will stand by as backup in case of any failure in the master virtual router.

Information about VRRP

VRRP Operation

There are several ways that a LAN client may choose to elect the first hop router for any specific destination. The client can use dynamic or static setting methods. The following example shows a dynamic election of router:

- Proxy ARP – The client uses Address Resolution Protocol (ARP) to get its own destination and the router will reply to the ARP request using its own MAC address.
- Routing protocol – The 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 the 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).

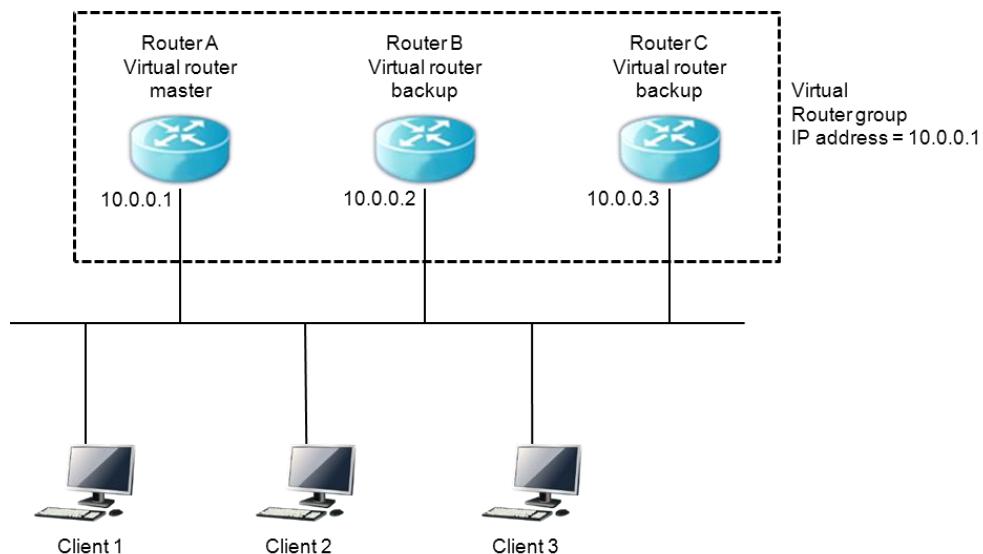


Figure 34 Basic VRRP Topology

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 router A and router B share the traffic. Router A and router B work as backup virtual routers for each other.

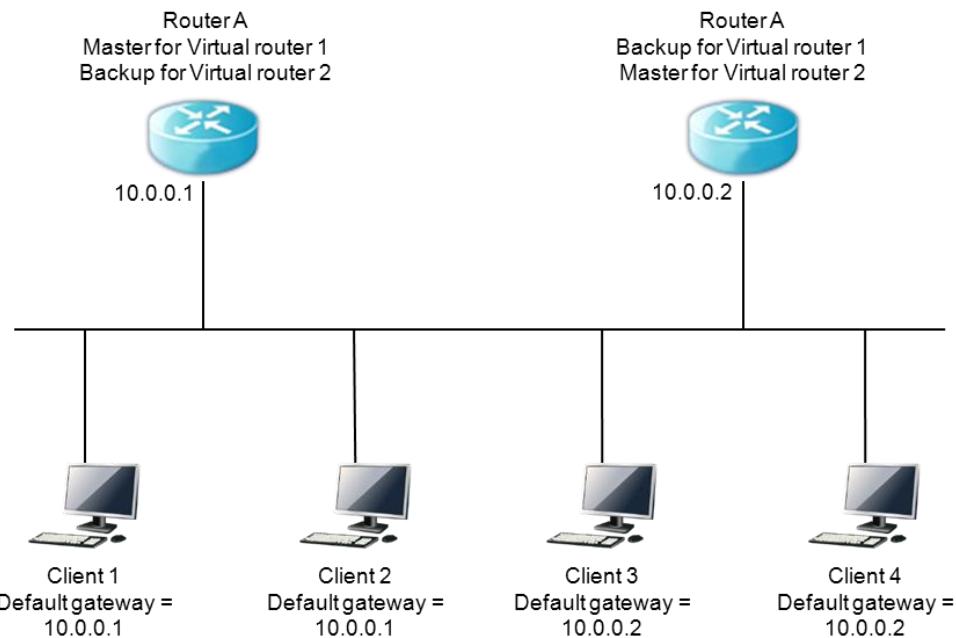


Figure 35 Load Sharing and Redundancy VRRP Topology

In this topology, two virtual routers are configured. In the virtual router 1, 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 router A. Client 1 and 2 use 10.0.0.1 for the IP address of the default gateway.

In the virtual router 2, router B is the owner of IP address 10.0.0.2 and the master virtual router, and router A is a backup virtual router for router B. Client 3 and 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 Object Tracking

By changing VRRP priority according to status of interface or IP route, VRRP object Tracking 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 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 back virtual routers when there is a failure in the master virtual router. **vrrp priority** command can be used to set the priority of backup virtual routers in the range of 1 ~ 254.

For example, if there is a failure in 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 router B and router C is set to 101 and 100 respectively, 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 Object Tracking

Object tracking is an independent process that generates and monitors objects such as line-protocol status of the interface etc, and manages their removal. The clients like VRRPs register the objects to track their change status.

The object to be tracked has a unique number assigned by the tracking command-line-interface (CLI). The client processes such as VRRP specify the object to track using this number.

In the Tracking process, the status of objects is checked periodically and any change in the status value is notified to the clients. The status value of objects is expressed either in up or down.

Throughout the tracking process, VRRP can track the status change of all the objects. Tracking process provides the function to track the status of each object such as line protocol status of the interface and reachability of the route etc.

Each VRRP group can track several objects affecting the priority of VRRP routers. If the number of object to track is specified, VRRP can detect the change status of the object. VRRP increases or decreases the priority value of the virtual router according to the status of object to track.

How to Configure VRRP

This section covers the following procedures:

- Enabling VRRP
- Disabling VRRP on an Interface
- Configuring VRRP Object Tracking

Enabling VRRP

To enable VRRP, do the following steps.

Table 207 Enabling VRRP

	Command or Action	Purpose
Step 1	configure terminal Example: Switch# configure terminal	Enters the Global configure mode
Step 2	interface interface-name Example: Switch(config)# interface vlan1	Enters the Interface configuration Mode
Step 3	ip address ip-address/prefix-length Example: Switch(config-if-vlan1)# ip address 172.16.6.5/24	set the IP address of interface
Step 4	vrrp group ip address ip-address Example: Switch(config-if-vlan1)# vrrp 10 ip 172.16.6.5	Enables VRRP on the interface Note: All the routers in the VRRP group should be set to the same IP address. If other IP address is to be set, the routers in the VRRP group can't communicate with each other, and the router with wrong configuration will work as the master by itself.
Step 5	end Example: Switch(config-if-vlan1)# end	Returns the Privileged mode
Step 6	show vrrp [brief group] Example: Switch# show vrrp 10	(Option) Shows the status of VRRP group of the router
Step 7	show vrrp interface interface-name [brief] Example: Switch# show vrrp interface vlan1	(Option) Shows information of VRRP group set in a specific interface

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 208 Disabling VRRP on an Interface

	Command or Action	Purpose
Step 1	configure terminal Example: Switch# configure terminal	Enters Global configure mode
Step 2	interface interface-name Example: Switch(config)# interface vlan1	Enters the Interface configuration mode
Step 3	ip address ip-address/prefix-length Example: Switch(config-if-vlan1)# ip address 172.16.6.5/24	set the IP address of interface
Step 4	vrrp group shutdown Example: Switch(config-if-vlan1)# vrrp 10 shutdown	To shutdown VRRP interface Note: The VRRP can be disabled while VRRP settings are kept.

Configuring VRRP Object Tracking

To VRRP object tracking, follow the steps below.

If VRRP group is owner of IP address, the priority of VRRP group fixes 255. The priority does not change with circuit failover.

Table 209 Configuring VRRP Object Tracking

	Command or Action	Purpose
Step 1	configure terminal Example: Switch# configure terminal	Enters Global configure mode
Step 2	track object-number interface interface-name { line-protocol ip routing } Example: Switch(config)# track 2 interface vlan1 line-protocol	Sets the interface that effect to priority of VRRP group with interface status Use this command to set the interface. vrrp track command, corresponding object number used. line-protocol keyword is to track whether the status of the interface is 'up' or not. IP routing key word is to track whether an IP address is set and the status of the interface is 'up'. track ip route command can be used to check the reachability of specific IP route.
Step 3	interface interface-name Example: Switch(config)# interface vlan10	Enters Interface configuration mode
Step 4	ip address ip-address/prefix-length Example: Switch(config-if-vlan10)# ip address 10.0.1.1/24	set the IP address of interface
Step 5	vrrp group ip address ip-address Example: Switch(config-if-vlan10)# vrrp 10 ip 10.0.1.20	To enable VRRP on the interface and set the IP address of the virtual router
Step 6	vrrp group priority level	set the priority VRRP router

	Example: Switch(config-if-vlan10)# vrrp 10 priority 120	
Step 7	Example: Switch(config-if-vlan10)# vrrp 10 track 2 decrement 15	To set VRRP to track the status of the objects.

Configuration Examples for VRRP

Configuring VRRP: Example

In the following examples, switch A and switch B belong to 3 VRRP groups. The configuration of each group is as follows:

- Group 1:
 - The virtual IP address is 10.1.0.10.
 - The switch A becomes the master of this group, since its priority value is 120.
 - Advertising interval is 3 seconds.
 - Preemption is activated.
- Group 5:
 - The switch B becomes the master of this group, since its priority value is 200.
 - Advertising interval is 30 seconds.
 - 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

```
interface vlan1
    ip address 10.1.0.2/8
    vrrp 1 priority 120
    vrrp 1 timers advertise 3
    vrrp 1 ip 10.1.0.10
    vrrp 5 timer advertise 30
    vrrp 5 ip 10.1.0.50
    no vrrp 100 preempt
    vrrp 100 ip 10.1.0.100
```

Router B

```
interface vlan1
    ip address 10.1.0.1/8
    vrrp 1 timers advertise 3
    vrrp 1 ip 10.1.0.10
    vrrp 5 priority 200
    vrrp 5 timer advertise 30
    vrrp 5 ip 10.1.0.50
    no vrrp 100 preempt
    vrrp 100 ip 10.1.0.100
```

VRRP Object Tracking: Example

In the following examples, the tracking process is set to track the line protocol status of interface vlan10. VRRP on the interface vlan1 is registered to the tracking process to be able to get the information on changes of protocol status in the interface vlan10. If the line protocol status of interface vlan10 turns to down, the priority value of VRRP group decreases by 15.

```
track 1 interface vlan10 line-protocol
!
interface vlan1
    ip address 10.0.0.2/8
    vrrp 1 ip 10.0.0.3
    vrrp 1 priority 120
    vrrp 1 track 1 decrement 15
```

VRRP Object Tracking Verification: Example

The following example is to track the settings made in “VRRP Object Tracking: Example” section.

```
Switch# show vrrp
vlan1 – Group 1
    State is Master
    Virtual IP address is 10.0.0.3
    Virtual MAC address is 0000.5e00.0101
    Advertisement interval is 1 sec
    Preemption is enabled
    Priority is 105
    Track object 1 state Down decrement 15
    Master Router is 10.0.0.2 (local) priority is 105
    Master Advertisement interval is 1 sec
    Master Down interval is 3.531 sec

Switch# show track
Track 1
    Interface vlan10 line-protocol
    Line protocol is Down (hw down)
    1 change, last change 00:06:53
    Tracked by:
        VRRP vlan1 1
```

Disabling a VRRP Group on an Interface: Example

The following example explains how to shutdown the VRRP group on interface vlan1 while keeping the settings of interface VRRP group.

```
interface vlan1
    ip address 10.24.1.1/24
    vrrp1 ip 10.24.1.254
    vrrp 1 shutdown
```

Chapter 18. *NTP*

This chapter describes the NTP configuration of the system.

The C9500 series 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 210 Setting NTP Server

Command	Purpose
Switch(config)# ntp server ip-address	Sets NTP with Client mode.
Switch(config)# ntp peer ip-address	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 211 Configuring NTP Authentication

Step	Command or Action	Purpose
Step 1	ntp authenticate	Enables NTP authentication.
Step 2	ntp authentication-key key-number md5 value	Defines authentication key.
Step 3	ntp trusted-key key-number	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 ip-address key key-number	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 212 Configuring the Source IP Address for NTP Packets

Command	Purpose
ntp source interface	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 213 Configuring the System as an Authoritative NTP Server

Command	Purpose
ntp master [stratum]	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 214 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 do not have an available time source, you can set current time directly after system is booted.

Configuring the Time Zone

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

Table 215 Configuring the Time Zone

Command	Purpose
Switch(config)# clock timezone zone <i>hours-offset</i> [<i>minutes-offset</i>]	Sets time zone. Zone: name of time band. 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 216 Configuring Summer Time (Daylight Savings Time)

Command	Purpose
Switch(config)# clock summer-time zone recurring [<i>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 217 Configuring Summer Time

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

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 218 Manually Setting the Software Clock

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

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 219 Setting the Hardware Clock

Command	Purpose
Switch# calendar set hh:mm:ss day month year or Switch# calendar set hh:mm:ss month day year	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 220 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 221 Setting the Hardware Clock from the Software Clock

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

Monitoring Time and Calendar Services

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

Table 222 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.

Clock Calendar and NTP Configuration Examples

The system that has the hardware clock connects with two other server systems and updates the hardware clock periodically.

clock timezone KST 9

ntp update-calendar

ntp server 192.168.13.57

ntp server 192.168.11.58

Chapter 19. *Dynamic ARP Inspection*

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

This chapter consists of the following sections:

- Understanding DAI
- Default DAI Configuration
- DAI Configuration Guidelines and Restrictions
- Configuring DAI
- DAI Configuration Samples

Understanding DAI

This section describes the basic function of DAI and the method to protect the ARP spoofing attack by using of DAI function. This section comprises 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.

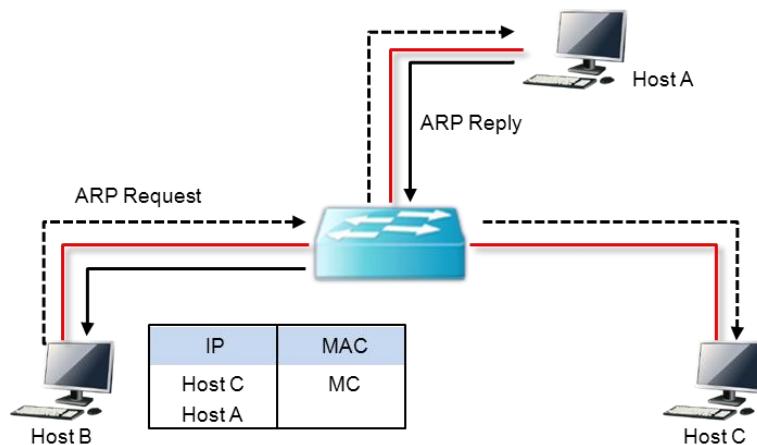


Figure 36 Understanding ARP

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.

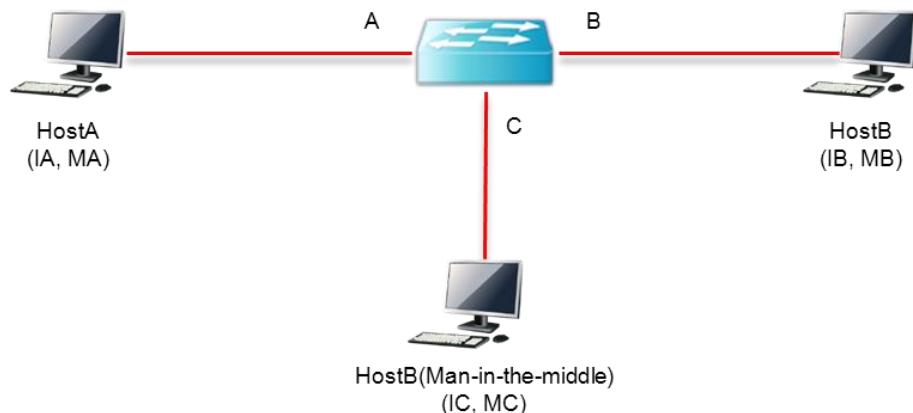


Figure 37 Understanding ARP Spoofing Attacks

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*'.

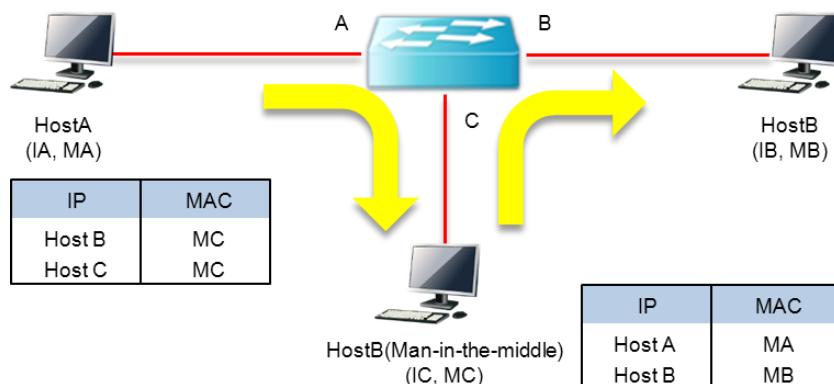


Figure 38 Understanding ARP Spoofing Attacks

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 ‘Enabling DAI on VLANs’

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.

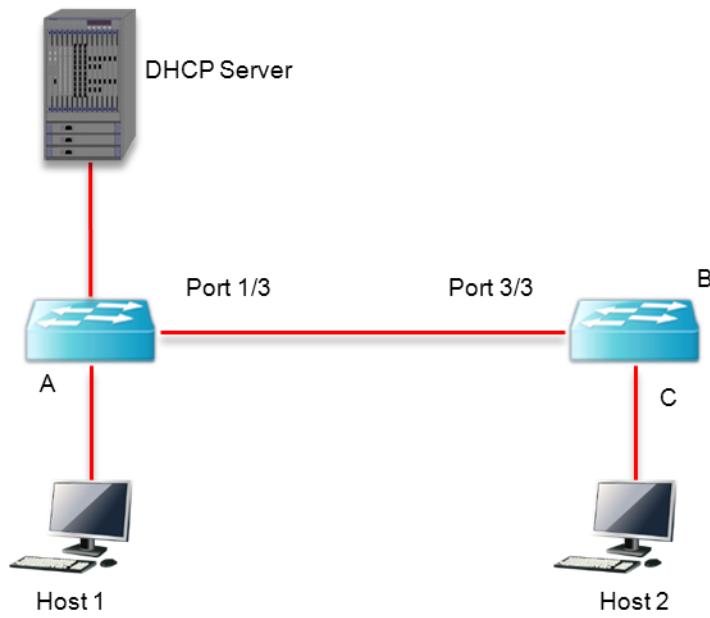


Figure 39 Interface Trust States and Network Security

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

The C9500 series support the DAI features that inspect all ARP packets.

Rate Limiting of ARP Packets

The DAI-enabled switch will control the number of ARP packets that come into the switch CPU. As a default value, with respect to untrusted interface, 15 ARP packets per second (15 pps) are allowed meanwhile there is no limitation on the rate for trusted interface. You can configure the setting by use of the command **ip arp inspection limit**.

If the rate of ARP packets at a specified port would be over the predefined value, the switch will discard all the received ARP packets at the port. This behavior shall be maintained until user would change the configuration. By use of the command **ip arp inspection limit auto-recovery**, you can make the port get back to available status after a certain amount of time.



Note

The rate limit function toward ARP packets are performed at CPU in software manner, you cannot count on it for Denial-of-Service (DoS) attack.

Relative Priority of ARP ACLs and DHCP Snooping Entries

When DAI checks out the IP-to-MAC address mapping, it used DHCP snooping binding database.

ARP ACLs are used for inspection before DHCP snooping binding database. The switch will use ACL only when it is configured by **ip arp inspection filter** command. The switch will inspect ARP packets with ARP ACLs. If the ARP packet is consistent with the deny condition of ARP ACLs, the packet will be discarded even when there is valid binding that has been made by valid DHCP snooping.

Logging of Dropped Packets

The switch will keep the information about the discarded packets at log buffer and generate system message according to the ratio that has been set in advance. Once the message is generated, the corresponding information at the log buffer will be deleted. In each log there are the flow information including received VLAN id, port number, source and destination IP address, source and destination MAC address.

By use of global configuration command **ip arp inspection log-buffer** you can adjust the size of buffer and number of log per unit time so as to control the total volume of created messages. And with the global configuration command **ip arp inspection VLAN logging** you can specify the type of packets to log.

Default DAI Configuration

The following table shows the default DAI configuration.

Table 223 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 Restriction

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 224 Enabling DAI on a VLAN

Command	Purpose
Switch# configure terminal	Enter Global configuration mode
Switch(config)# ip arp inspection VLAN VLAN-id Switch(config)# no ip arp inspection VLAN VLAN-id	Enables DAI on a VLAN Enables DAI on a VLAN
Switch# show ip arp inspection	Checks the setting



Notice

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

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 Ether-type: 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 225 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-Giga6/1)# ip arp inspection trust Switch(config-if-Giga6/1)# no ip arp inspection trust	To configure the interface to be trusted (default: untrusted)
Switch(config-if-Giga6/1)# 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 gi6/1
Switch(config-if-Giga6/1)# ip arp inspection trust
Switch(config-if-Giga6/1)# end
Switch# show ip arp inspection interfaces
Interface      Trust State   Rate (pps)  Burst Interval  Auto Recovery
-----  -----  -----  -----
Giga6/1        Trusted      None          1             Disabled
```

Applying ARP ACLs for DAI Filtering

To utilize ARP ACL feature, use the following commands.

Table 226 Applying ARP ACLs for DAI Filtering

Command	Purpose
Switch# configure terminal	Enters the global configuration mode
Switch(config)# ip arp inspection filter arp_acl_name VLAN VLAN-id [static]	Enters apply ARP ACL to a VLAN
Switch(config)# end	Return the Enable mode.
Switch# show ip arp inspection	Shows the running information.

When applying ARP ACL, please note the following points:

- To treat implicit deny of ARP ACL as explicit deny and discard packets not matching with any condition of ACL, use a static keyword. In this case, DHCP binding is not used. When the static keyword is not used, DHCP binding is used to determine whether to permit or deny for the packets with no matching condition in the ACL.
- Inspect only the ARP packets with IP-to-MAC address mapping using ACL. Only the packets permitted by Access List are permitted.

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							
Vlan	Config	Operation	ACL Match	Static ACL	ACL Log	DHCP Log	
200	Enabled	Active	example_arp_acl	No	Deny	Deny	

Configuring ARP Packet Rate Limiting

Once DAI is enabled then all ARP packets are to be inspected, which will take a lot of CPU capability. Then consequently the switch will be vulnerable to the DoS attack which mainly bombarded ARP packets. Thus by putting a certain amount of limitation on the CPU it can control the amount of ARP packets to be processed rate and lessen the burden of CPU.



Note

The ARP rate limit that is provided by DAI is a software feature, so it cannot control the usage rate of CPU in direct measure. However by reducing the ARP packets which are to be handled by DAI, the CPU usage rate by DAI can be lowered.

To set the rate limit upon ARP packets for a port, do the following steps:

Table 227 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-Giga6/1)# ip arp inspection limit {rate pps [burst interval seconds] none} Switch(config-if-Giga6/1)# no ip arp inspection limit	Sets ARP packet rate limit (optional) To go back to default configuration
Switch(config-if-Giga6/1)# ip arp inspection limit enable Switch(config-if-Giga6/1)# no ip arp inspection limit enable	To enable the ARP rate limit of an interface To disable the ARP rate limit of an interface
Switch(config)# end	To 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 and 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 gi6/1
Switch(config-if-Giga6/1)# ip arp inspection limit rate 20 burst interval 2
Switch(config-if-Giga6/1)# ip arp inspection limit enable
Switch(config-if-Giga6/1)# end
Switch# show ip arp inspection interfaces
Interface      Trust State   Rate (pps)  Burst Interval  Auto Recovery
-----          -----       -----        -----
Giga6/1         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 228 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-Giga6/1)# 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 gi6/1
Switch(config-if-Giga6/1)# ip arp inspection limit auto-recovery 10
Switch(config-if-Giga6/1)# ip arp inspection limit enable
Switch(config-if-Giga6/1)# end
Switch# show ip arp inspection interfaces
Interface      Trust State   Rate (pps)  Burst Interval  Auto Recovery
-----          -----       -----        -----
Gi6/1          Untrusted    20           2             10
Gi6/2          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 229 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 : Enabled						
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 : Enabled						
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 230 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 second.
No entries in log buffer.
```

Configuring the DAI Logging System Messages

To configure the log message that DAL generates, use the following commands:

Table 231 Configuring the DAI Logging System Messages

Command	Purpose
Switch# configure terminal	Enters global configuration mode
Switch(config)# ip arp inspection log-buffer logs	Configures the DAI log buffer

<code>number_of_messages interval length_in_seconds</code>	
<code>Switch(config)# no ip arp inspection log-buffer logs</code>	Returns to default
<code>Switch(config)# end</code>	Returns to enable mode
<code>Switch# show ip arp inspection log</code>	Checks out 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 232 Configuring the DAI Log Filtering

Command	Purpose
<code>Switch# configure terminal</code>	Enters global configuration mode
<code>Switch(config)# ip arp inspection VLAN VLAN-id {acl-match {matchlog none} dhcp-bindings {all none permit}}</code>	Applies log filtering to each VLAN
<code>Switch(config)# end</code>	Return to enable mode
<code>Switch# show running-config</code>	Check out 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 233 Displaying DAI Information

Command	Description
show arp access-list	Shows the information of ARP ACL.
show ip arp inspection interfaces	Shows the trust status of the interface.
show ip arp inspection VLAN [VLAN-id]	Shows the DAI configuration and its behavior of a VLAN.
show ip arp inspection arp-rate	Shows the rate of ARP packet reception in the interface.

To retrieve or initialize DAI statistics, use the following commands.

Table 234 Initialize DAI Statistics

Command	Description
clear ip arp inspection statistics	To initialize DAI statistics
show ip arp inspection statistics [VLAN VLAN-id]	To display the DAI statistics of ARP packets

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

Table 235 Initialize the DAI logging information

Command	Description
clear ip arp inspection log	To initialize DAI log buffer
show ip arp inspection log	To display the configuration and contents of DAI log buffer

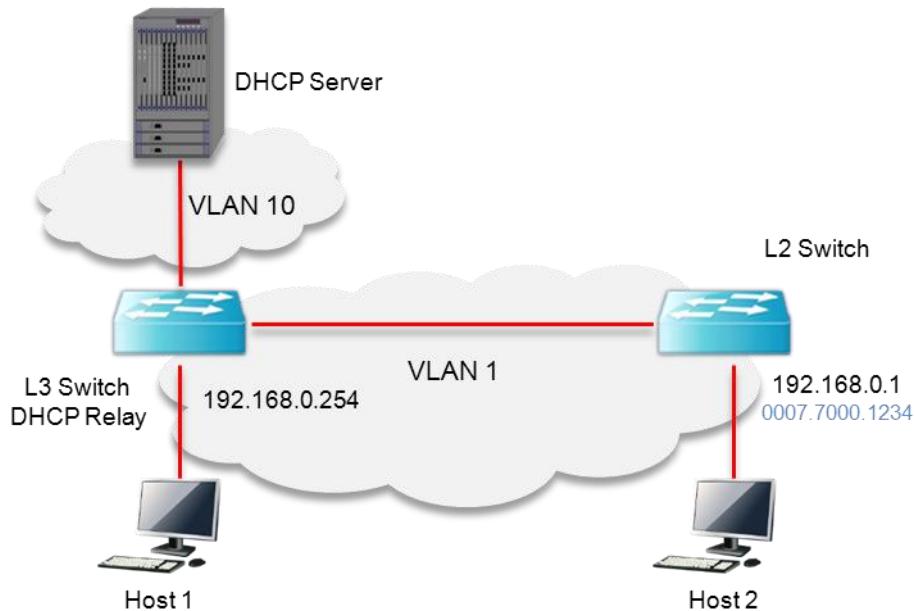
DAI Configuration Samples

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 236 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

	<pre>Switch(config)# ip dhcp snooping VLAN 10 Switch(config)# ip dhcp snooping</pre>
Step 3	<p>To permit ARP packet of switch using static ip, set ARP ACL.</p> <pre>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</pre> <p>To see if the configuration has been set correctly.</p> <pre>Switch# show ip arp inspection VLAN 1</pre>
Step 4	<p>Enables DAI to VLAN1 connected with host.</p> <pre>Switch# configure terminal Switch(config)# ip arp inspection VLAN 1 Switch(config)# end</pre> <p>To see if the configuration has been set correctly.</p> <pre>Switch# show ip arp inspection VLAN 1</pre>

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 20. *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 237 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	Privileged

All QOS-related settings of the C9500 series work only under global configuration. Most QOS-related commands are not possible to set if Mls qos is not enabled.

TX Scheduling Configuration

The C9500 series provides SPQ (Strict Priority Queue) and WRR (Weighted Round Robin) for scheduling. These two ways can be used together.

The WRR provided by the C9500 series 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 1,1,1,1,1,0,0,0,1,1,1,1,0,0,0. 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 238 TX Scheduling Configuration

Queue	Description
Queue 7	SPQ
Queue 6	SPQ
Queue 5	WRR (30)
Queue 4	WRR (30)
Queue 3	WRR (20)
Queue 2	WRR (10)
Queue 1	WRR (10)
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.
- Q5,4,3,2,1 are set for WRR and their respective weight is assigned as 30:30:20:10:10. The priority of WRR is lower than that of SPQ.

- Although Q0 is pronounced as SPQ it has the lowest priority. So it will be processes after all the other queues, i.e. from Q7 to Q1 have been done.


Notice

It is not recommended that SPQ is used in-between WRR groups or among lower priority queues. If that is the case, the actual scheduling would not work out as configured.

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 239 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.	Privileged

Set a mapping table of tx-scheduling to a designated port using the following settings:

Table 240 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 either COS or DSCP or neither.

- When a packet has a DSCP value and is in Trust DSCP mode, then use this.
- When a packet has a COS value and is in trust COS mode, then use this.
- When a packet has no COS and is in trust COS, then use the default COS value which is set for the port.
- In other cases, use default COS value.

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 241 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 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   0   1   1
1:     1   1   1   1   1   1   2   2   2   2   2
2:     2   2   2   2   3   3   3   3   3   3   3
3:     3   3   4   4   4   4   4   4   4   4   4
4:     5   5   5   5   5   5   5   5   5   6   6
5:     6   6   6   6   6   6   7   7   7   7   7
6:     7   7   7   7
```

Table 242 dscp-cos map Configuration Command

Command	Description	Mode
mls qos map dscp-cos <0-63> ... <0-63> to <0-7>	Set Dscp-cos map.	Config
no mls qos map dscp-cos	Initialize Dscp-cos map.	Config
mls qos dscp-cos	Configure the port interface to set dscp-cos.	Interface
no mls qos dscp-cos	Configure the port interface not to set dscp-cos.	Interface
show mls qos map dscp-cos	Display the current dscp-cos map setting.	Privileged

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 with the global setting. The default is 1:1. Change the map to apply to the port interface before use.

```
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						

Table 243 dscp-mutation map Setting

Command	Description	Mode
mls qos map dscp-mutation <0-63> ... <0-63> to <0-63>	Set Dscp-mutation map.	Config
no mls qos map dscp-mutation	Initialize Dscp-mutation map.	config
mls qos dscp-mutation	Configure the port interface to set dscp remarking.	Interface
no mls qos dscp-mutation	Configure the port interface not to set dscp remarking.	Interface
show mls qos map dscp-mutation	Display the current dscp-mutation map.	Privileged

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
- COS remarking operation depending on COS value

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.

```
Switch#show mls qos map cos-mutation
COS MUTATION MAP
In COS : 0 1 2 3 4 5 6 7
-----
Out cos : 0 1 2 3 4 5 6 7
```

Table 244 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.	Privileged

ACL Configuration

The C9500 series has various options in ACL configuration including a feature sorting packets into easily acceptable ones and not easily acceptable ones.

The C9500 series 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 245 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	Privileged

The command, **SRC_IP_ADDRESS** can be set as follows.

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 10.1.1.0.0.255 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 246 Extended IP ACL Configuration Command

Command	Description	Mode
<code>access-list <100-199> (permit deny) (<0-255> icmp igmp ip ospf pim tcp udp) SRC_IP_ADDRESS DST_IP_ADDRESS</code>	Sets Extended IP ACL.	Config
<code>access-list <100-199> (permit deny) icmp SRC_IP_ADDRESS DST_IP_ADDRESS ICMP-TYPE</code>	Sets Extended IP ACL of ICMP type.	Config
<code>access-list <100-199> (permit deny) igmp SRC_IP_ADDRESS DST_IP_ADDRESS IGMP-TYPE</code>	Sets Extended IP ACL of IGMP type.	Config
<code>access-list <100-199> (permit deny) (tcp udp) SRC_IP_ADDRESS DST_IP_ADDRESS eq <0-65536></code>	Sets Extended IP ACL of TCP / UDP type.	Config
<code>no access-list <100-199> (permit deny) (<0-255> icmp igmp ip ospf pim tcp udp) SRC_IP_ADDRESS DST_IP_ADDRESS</code>	Disables Extended IP ACL.	Config
<code>no access-list <100-199></code>	Deletes all ACLs with the relevant name (number).	Config
<code>access-list <100-199> remark LINE</code>	Adds the description of the relevant ACL.	Config
<code>access-list <2000-2699> (permit deny) (<0-255> icmp igmp ip ospf pim tcp udp) SRC_IP_ADDRESS DST_IP_ADDRESS</code>	Sets Extended IP ACL of Expanded range.	Config
<code>access-list <2000-2699> (permit deny) icmp SRC_IP_ADDRESS DST_IP_ADDRESS ICMP-TYPE</code>	Sets Extended IP ACL of Expanded range of ICMP type.	Config
<code>access-list <2000-2699> (permit deny) igmp SRC_IP_ADDRESS DST_IP_ADDRESS IGMP-TYPE</code>	Sets Extended IP ACL of Expanded range of IQMP type.	Config
<code>access-list <2000-2699> (permit deny) (tcp udp) SRC_IP_ADDRESS DST_IP_ADDRESS eq <0-65536></code>	Sets Extended IP ACL of Expanded range of TCP / UDP type.	Config
<code>no access-list <2000-2699> (permit deny) (<0-255> icmp igmp ip ospf pim tcp udp) SRC_IP_ADDRESS DST_IP_ADDRESS</code>	Disables Extended IP ACL.	Config
<code>no access-list <2000-2699></code>	Deletes all ACLs with the relevant name.	Config
<code>access-list <2000-2699> remark LINE</code>	Adds the description of the relevant ACL.	Config
<code>access-list extended WORD (permit deny) (<0-255> icmp igmp ip ospf pim tcp udp) SRC_IP_ADDRESS DST_IP_ADDRESS</code>	Sets Named Extended IP ACL.	Config
<code>access-list extended WORD (permit deny) icmp SRC_IP_ADDRESS DST_IP_ADDRESS ICMP-TYPE</code>	Sets Extended IP ACL of ICMP type.	Config
<code>access-list extended WORD (permit deny) igmp SRC_IP_ADDRESS DST_IP_ADDRESS IGMP-TYPE</code>	Sets Extended IP ACL of IGMP type.	Config
<code>no access-list extended WORD (permit deny) (<0-255> icmp igmp ip ospf pim tcp udp) SRC_IP_ADDRESS DST_IP_ADDRESS</code>	Disables Named Extended IP ACL.	Config
<code>no access-list extended WORD</code>	Deletes all ACLs with the relevant.	Config

	name	
access-list WORD remark LINE	Adds the description of the relevant ACL	Config
Show access-list	Searches the configuration of ACL	Privileged

The command, **SRC_IP_ADDRESS** and **DST_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,
host A.B.C.D	Add a host prefix to indicate only one IP address.
any	Use any when assigning all IP addresses.



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 should be 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 248 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	Privileged

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	When all MAC addresses are specified, "any" can be used.

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 249 Commands for the Applying 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

{in out}	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, ehtertype, cos, VLAN, protocol, dscp, ip-preedence(TOS), l4 port, tcp flag, and mlps flag, etc.

Traffic that is sorted as a class-map carries out the basic actions like permit / drop, as well 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 are 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 ethertype, cos, VLAN, protocol, dscp, ip-preedence (TOS), l4 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 250 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
match access-group NAME	Sets the classification criteria using ACL.	cmap
match cos <0-7>	Sets the classification criteria using COS.	cmap
match ethertype WORD	Sets the classification criteria using Ethertype.	cmap
match ip-dscp <0-63>	Sets the classification criteria using DSCP.	cmap
match ip-precedence <0-7>	Sets the classification criteria using IP-Precedence.	cmap
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

Traffic that is sorted as a class-map carries out the basic actions such as permit / drop, as well 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 are not related to QOS, such as trap-cpu, mirror, 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.

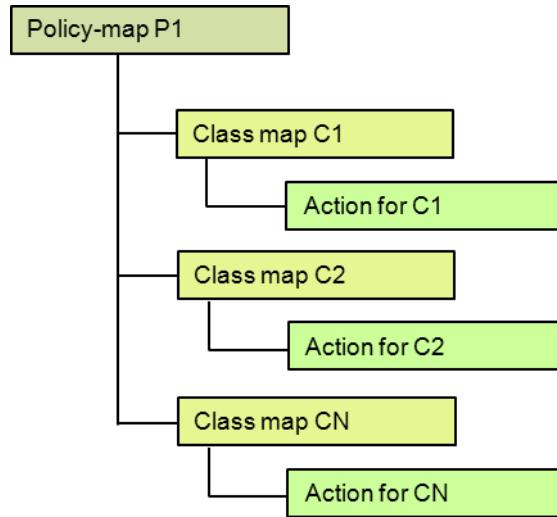


Figure 40 Hierarchy of Policy-Map

Marking and remarking are used without distinction. When there is a correspondent field to an incoming packet remarking will work, when no correspondent field marking will work. It enables other operations, which are not related to QOS, such as trap-cpu, mirror, redirect, netflow, etc.

Table 251 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 kbps <1-10000000> <1-10000000> exceed-action drop	Rate-limit setting by unit of Kbps.	pmap-c
police pps <1-10000000> <1-10000000> exceed-action drop	Rate-limit setting by unit of PPS.	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 252 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 253 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 the control-plane, only policy drop, and set queueing will operate.

Rate-limit on COPP

You can set a rate-limit of a specific traffic that flows into the CPU.

Table 254 Commands for Control-plane of Rate-limit Configuration

Command	Description	Mode
Rate-limit <0-47> <1-4096> <1-4096>	Configure the burst and rate-limit to CPU Queue ID by the unit of PPS.	Control-plane
Protocol-queue-map {arp-reply arp-request bgp bpdu dhcp filter icmp icmpv6 i gmp ipmc_rsvd isis l2-cpu l3-cpu mld nd ospf pim rsvp telnet} <0-47>	Assign CPU Queue for each protocol.	Control-plane
Show control-plane cpu-queue	Display the CPU Queue ID and protocol mapping table.	Privileged

Equipment Protection feature

Table 255 Commands for Equipment protection feature

command	Description	Mode
martian-filter	Drop the packet if its Source ip belongs to the below range. 10.0.0.0/8 127.0.0.0/8 172.16.0.0/12 192.168.0.0/16 224.0.0.0/4	Vlan Interface
Source-ip-filter	Drop the packets if its Source ip is out of the range of the Vlan interface network.	Vlan Interface
dhcp-filter	Drop the packets which come from DHCP server so as to prevent dhcp spoofing.	Vlan Interface

Chapter 21. *Utilities*

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

Status dump command

Commands used

"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 a 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      : C9500
SERIAL-NO       :
System MAC-ADDRESS: 00:07:70:74:ff:01

--- Display the system version ---
-----
CommScope Switch Operating System Software
C9500 Software (C9500), Version 1.1.0
Technical Support: http://www.CommScope.com
Copyright (c) 2001-2010 by CommScope Inc.

BOOTLDR: C9500 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_ssj"

If you require further assistance please contact us by sending email to
spot.team@CommScope.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 256 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 provides a considerable amount of detail. 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 257 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.
ic-include WORD	Shows a certain letter in the running config. Is case-insensitive.

Examples of output post processing

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

```
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)

The C9500 series supports the commands that show the status of SFP with DDM in detail. The monitoring items are as follows:

Table 258 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 259 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										
Temperature	Voltage	Current		Tx Power	Rx Power						
Port	(Celsius)	(Volts)	(mA)	(dBm)	(dBm)						
Gi7/3	42.6	3.32	17.4	-7.7	-40.0	--					
Gi7/4	41.5	3.32	15.5	-6.7	-40.0	-					
-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----
Gi7	gbic	ddm	50.6'C	3.5 V	14.0 mA	-6.08 dBm	-40.00				
dBm											
Normal	Normal	Normal	Normal	Alarm(L)	Alarm(L)						
(warn)	100.0	-10.0	4.0	1.0	131.0	0.0	8.00	0.00	8.00	0.00	
(alarm)	100.0	-10.0	4.0	1.0	131.0	0.0	8.00	0.00	8.00	0.00	
.....	gi7/2	.						
Normal	Normal	Normal	Normal	Normal	Normal						
(warn)	128.0 -128.0	6.6	0.0	131.0	0.0	8.20 -40.00	8.00 -40.00				
(alarm)	128.0 -128.0	6.6	0.0	131.0	0.0	8.20 -40.00	8.00 -40.00				
.....

Chapter 22. *Saving Config File and Software Upgrade*

This chapter describes Flash File System management and using USB or Compact Flash (CF) memory. An OS Image and Configuration File are saved in the File System provided by the C9500 series. When you boot the system, the system loads the saved OS Image and Configuration files. This chapter describes the following commands:

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

File System

The system basically provides Flash File system for saving OS image and Configuration file. Moreover, the system supports USB Port. This chapter describes several file system of this product. Flash file system is used for saving OS image and Configuration file.

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 files are as follows:

Table 260 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 [C9500] 1.1.0    -- u92h.r110  
59537056 [C9500] 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/Up Load

You can download the Image and configuration file from a remote TFTP (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.
-  **Warning** The configuration applied via FTP/TFTP is added or changed on the configuration of the current system. In other words, the configuration of the current system is not deleted completely and changes with the downloaded configuration.

Download/Upload with the FTP

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

Table 261 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
(Omission)
```

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/Up Loading File with the TFTP server

To download and upload the file with the TFTP server, use the following command.

Table 262 Down/Up Loading 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
(omitted )
```

Configuration File Management

The system configuration file is a text file that has commands for configuration when the system is booting. It is convenient that you do not need to input commands manually for the system configuration, whenever the system is 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 263 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 want to apply the current running configuration file when the system boots next, 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 command.

```
Switch# show running-config
!
no service dhcp
!
no logging console
!
ip domain-lookup
... < > ....
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
... < > ....
SWITCH#
```

Configuration File Erase

When the system restarts, the system reloads the 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# redundancy reload shelf
```

Boot Mode Setting and System Restart

You can arrange an OS Image and a Config file for the system to be used when next booting takes place. When you restart the system, the arranged OS image and config file will be applied to the system. So pay careful attention when you arrange the OS Image and Config file.

The following table shows how to arrange an OS image and config file for next booting.

Table 264 Boot Mode Setting and System Restart

Command	Description	Mode
boot system flash <i>filename</i>	Registers the OS image to be applied when next booting.	Privileged
boot system tftp <i>filename</i> A.B.C.D	Registers the OS image to be applied when next booting.	Privileged
boot config <i>filename</i>	Assigns filename as Start-up configuration file.	Privileged
reload	Restarts the currently connected SCM.	Privileged
redundancy reload shelf	Makes the entire system(i.e. both SCMs) booted up at once.	Privileged
redundancy reload (active standby peer myself)	Makes the specified SCM (e.g. active, standby, peer, myself) booted up. But the attempt by Standby SCM for the Active SCM is not allowed.	Privileged

Boot Mode Setting

You must be careful as follows:

- When you execute **boot flash** command, you must use the OS image which is for the C9500 series only.
- When you execute **boot config** command, you must use the Config file which is for the C9500 series only.

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

Restarting an SCM

You can restart the SCM by **reload** command which is currently associated with your console. The restart of SCM can be reserved for later execution by using a list of sub-commands **in** or **at**. Before you try the reservation, make sure to refer to the system time by using the **show clock** command.



Notice

When the system is equipped in redundant fashion, i.e. having two SCMs, **redundancy reload shelf** command can be used to restart the entire system at once.

Table 265 Boot Mode Setting and System Reload

Command	Description	Mode
reload	Restarts the currently connected SCM.	Privileged
reload {in <i>time</i> at <i>time [day] [month]</i> } [<i>reason</i>]	Specifies the time for reserving an upcoming system restart. <i>in</i> : in time <i>at</i> : at the specified time <i>time</i> : HH:MM <i>day</i> : 1 - 31 <i>month</i> : (ex. Jan or January) <i>reason</i> : reason for restart	Privileged
reload cancel	Cancels the reserved system restart.	Privileged
show reload	Shows the reservation information that the system is scheduled to restart.	Privileged

The following example shows how to restart an SCM with **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 system, you should always save the running configuration in Flash memory. When you execute **reload** command in config mode, you always make sure if you save the file as follows.

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


Warning

Do not forcefully restart the system while it is saving file to Flash File System.

Restarting entire system

When the system is equipped in redundant composition, meaning the system has two SCMs, **redundancy reload shelf** command can be used to restart the entire system. If **reload** command would be used for a redundantly composed system, you will have to execute the command twice; first for the standby SCM and then for active SCM. It is fair to say **redundancy reload shelf** command will be more convenient.

Table 265-2. Restart command for a redundant system

Command	Description	Mode
redundancy reload shelf	Makes the entire system(i.e. both SCMs) booted up at once.	Privileged
redundancy reload (active standby peer myself)	Makes the specified SCM (e.g. active, standby, peer, myself) booted up. But the attempt by Standby SCM for the Active SCM is not allowed.	Privileged

In case the system is not in redundant composition, meaning the system has one SCM, the result of executing **redundancy reload shelf** command is same as that of **reload**.



Warning

The attempt to reboot the active SCM by the standby SCM is prohibited because it might cause system failure.

Chapter 23. ***DPoE Provisioning***

This chapter describes how to make the setting in relation with DPoE Provisioning.

This chapter consists of the following sections:

- Background and Theory of Operations
- Cable and Bundle Interface management
- vCM and CPE's DHCP Relay management
- Source Address Verification (SAV) management
- Subscriber management
- ONU Encryption and Authentication
- Certificate Revocation List
- Online Certificate Status Protocol
- EAE Exclusion List
- ONU White List
- CM Offline List
- Optical Monitoring
- vCM TFTP Client Settings
- CM Event Management
- CM Secure Software Download
- MEF-MN Interface
- Subscriber's Provider Bridging (PB) Services
- Subscriber's Provider Backbone Bridging (PBB) Services
- IP(HSD) Services
- Quality of Service (QoS)
- Classifiers
- DPoEv2.0 Multicast

Background and Theory of Operations

This section provides a general context for understanding the DPoE operations.

The DOCSIS Network

The below Figure summarizes the primary systems and elements involved in a traditional DOCSIS Cable Modem (CM) and Cable Modem Termination System (CMTS) network.

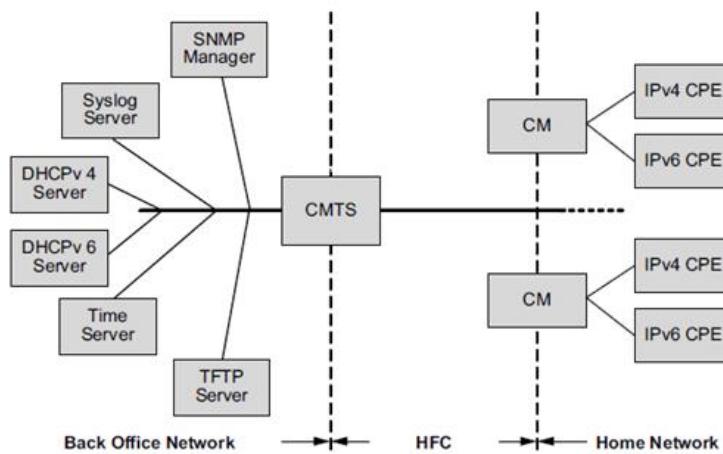


Figure 41 DOCSIS 3.0 HFC Network

DPoE Network

The below Figure summarizes the logical interfaces necessary to seamlessly replace the CMTS and CMs with Ethernet Passive Optical Network (EPON), OLT, and optical Node Unit (ONU) devices. This permits operators to take advantage of standard EPON functionality and economics while retaining their investment in back-office operations and systems and leave Customer Premise Equipment (CPE) unchanged.

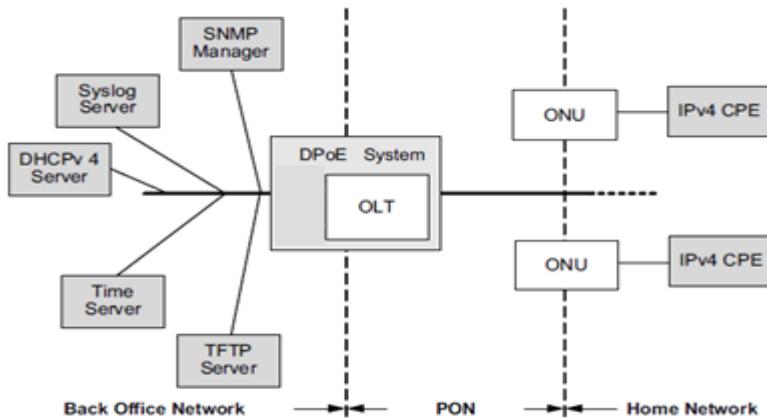


Figure 51 DPoE Reference Network

Cable and Bundle Interface management

This section describes the guideline of Cable and Bundle Interface management.

Cable Interface

A cable interface is a logical entity that represents a DOCSIS CMTS-like interface that provides MAC-domain provisioning and statistics. The cable interface functionality includes Layer 3 (L3) provisioning for vCMs and CPEs, bundle assignment, interface related MIB statistics, and provisioning of the port administrative status (enable/disable). A cable interface maps one-to-one with a PON Interface on an OLT. A cable interface also represents the DPoE MAC Domain interface that is referenced in many of the DOCSIS MIB tables defined for a CMTS.

Bundle Interfaces

Cable Bundling is a DOCSIS CMTS-like feature that allows multiple cable interfaces to share a common L3 interface. The shared L3 interface typically provides IP subnets, cable helpers, and DHCP Relay configuration. A cable bundle is defined by associating one or more physical interfaces to a bundle.

The DPoE 1.0 IP Serving Group (IP-SG) feature standardizes the concept of interface “bundling” which allows operators to apply a common set of IP configuration to one or more PON (TU) interfaces. This is illustrated in the following Figure, which shows PON Port 1, PON Port 2, and PON Port n associated with bundle number 10. The bundle has the CPE IP Gateway address (or DHCP giaddr) configured as the 30.30.30.0/24 network. This allows CPEs to be assigned IP addresses from the 30.30.30.0/24 network across several PON interfaces.

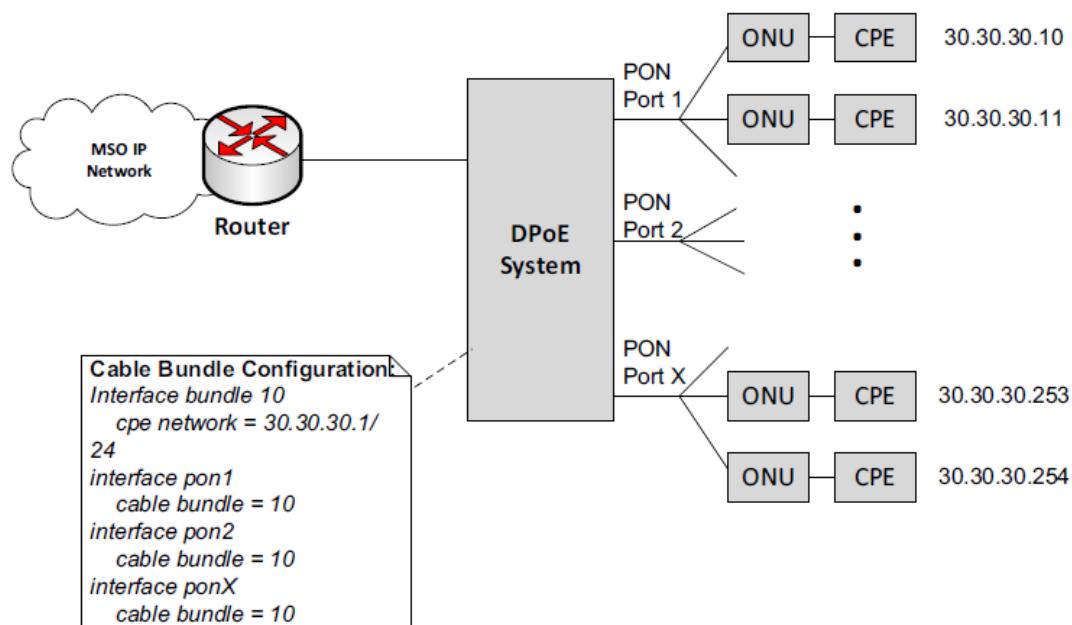


Figure 42 DPoE Reference Network

L3 parameters are configured for a cable bundle using a bundle interface, which can be provisioned with IP networks for vCMs and CPEs, cable helpers, DHCP Relay, and other Layer 3 parameters. Each cable interface that is a member of the bundle shares this configuration.

Bundle Create and View

To create the Bundle Interface or enter the Bundle Interface mode, use this command. To delete the Bundle Interface, use the 'no' form of this command.

Table 266 Bundle Interface

Command	Description
interface Bundle <1-255>	Creates the Bundle interface.

no interface Bundle <1-255>	Removes the Bundle interface.
<pre> Router# configure terminal Router(config)# interface Bundle 10 Router(config-if-Bundle10)# end Router# show bundle VLAN Name Status Ports ----- ----- 4001 BUNDLE010 active VLAN MTU BridgeNo BrdgMode ----- ----- 4001 1500 0 vlan-bridge Router# </pre>	

Bundle VLAN

VLAN IDs starting from 4001 are reserved for the bundle interface and can be easily changed using the following command.

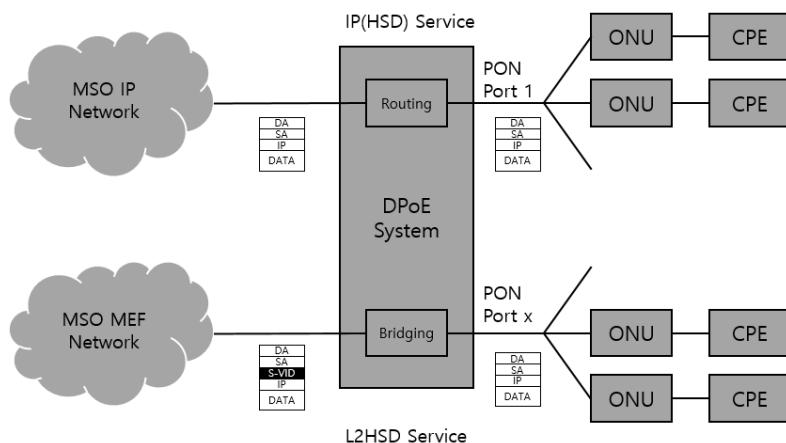
Note that the configuration is applied after the system is rebooted.

Table 268 Bundle VLAN

Command	Description
reserved-vlan bundle <2-4094> <2-4094>	Specifies the range of VLAN IDs to be reserved for the bundle interface. The configuration is applied after the system is rebooted.
no reserved-vlan bundle	Removes the Bundle interface.

IP(HSD) and L2HSD Services

IP (HSD) services provide routing functionalities within the DPoE System whereas L2HSD services are L2 bridges forwarding traffic to an external interface. The two services look alike; however, to provide L2HSD services, the DPoE system adds the operator-specified S-VID to the traffic that is received by the PON interface and sent to the NNI interface.



Bundle Sub-Interface

IP Serving Group (IP-SG) configurations are largely an organizational function that allows an operator to group a set of similar service flows together (representing similar services). IP(HSD) IP-SGs are used to forward traffic to a common IP interface on the router within the DPoE System. L2(HSD) IP-SGs are used to forward traffic to an external interface.

To create the Bundle Sub-Interface or enter the Bundle Sub-Interface mode, use this command. To delete the Bundle Sub-Interface, use the 'no' form of this command.

Table 269 Bundle Sub-Interface

Command	Description
interface Bundle <1-255>.<0-4096>	Creates the Bundle Sub-interface.
no interface Bundle <1-255>.<0-4096>	Removes the Bundle Sub-interface.

```
Router# configure terminal
Router(config)# interface Bundle 1.100
Router(config-if-Bundle1.100)# end
```

```
Router# show bundle
```

VLAN Name	Status	Ports
4001 BUNDLE1	active	
4002 BUNDLE1.100	active	
VLAN MTU BridgeNo BrdgMode		
4001 1500 0 vlan-bridge		
4002 1500 0 vlan-bridge		
Router#		

To manage subscriber traffic, the operator can specify “SF Required Attribute Mask (TLV24/25.31)” per service-flow using the configuration file or service-class. Subscriber traffic that is carried by service-flow is forwarded to a bundle sub-interface that conforms to TLV24/25.31.

The bundle sub-interface provides IP (HSD) services by default; L2 (HSD) services can be provided by specifying S-VID to the bundle sub-interface.

The following commands are available for the bundle sub-interface.

Table 270 Additional Commands of Bundle Sub-Interface

Command	Description
docsis attribute-mask HEXAVALUE	Specifies the 32bit attribute-mask value of Bundle Sub-Interface
no docsis attribute-mask	Removes the specified attribute-mask
s-vlan <2-2094>	Specifies the S-VID for L2HSD service
no s-vlan	Removes the specified S-VID for L2HSD service

```
Router# configure terminal
Router(config)# interface Bundle 1.100
Router(config-if-Bundle1.100)# docsis attribute-mask 80000001
Router(config-if-Bundle1.100)# s-vlan 30
```

Cable Bundle Setting and View

To configure a cable interface to belong to an Bundle interface, use this command in the INTERFACE mode of cable interface. To delete a cable interface of Bundle interface, use the 'no' form of this command.

Only a bundle interface can be specified as a cable interface; a bundle sub-interface cannot be specified as a cable interface because it manages subscriber traffic.

Table 267 cable bundle

Command	Description
cable bundle <1-255>	Adds cable into bundle
no cable bundle <1-255>	Removes cable from bundle

```

Router# configure terminal
Router(config)# interface EponInterface 2/1
Router(config-if- Epon2/1)# cable bundle 10
Router(config-if- Epon2/1)# end
Router# show bundle
VLAN Name                               Status      Ports
-----
4010 BUNDLE010                           active     Ep2/1

VLAN MTU      BridgeNo BrdgMode
-----
34010 1500          0      vlan-bridge
Router#

```


no cable helper-address A.B.C.D host	Removes the specified DHCP Server of vCM.
<hr/>	
Router# configure terminal	
Router(config)# interface Bundle 10	
Router(config-if-Bundle10)# cable helper-address 10.1.1.2 host	
Router(config-if-Bundle10)# end	
Router# show bundle	
VLAN Name	Status Ports
4010 BUNDLE010	active Ep2/1
<hr/>	
VLAN MTU	BridgeNo BrdgMode
4010 1500	0 vlan-bridge
<hr/>	
Router#	
Router# show ip dhcp relay	
<hr/>	
DHCP relay	: Enabled
DHCP Smart Relay feature	: Enabled
DHCP Smart Relay retry count	: 1
DHCP server-id based relay	: Disabled
Verification of MAC address	: Enabled
Insertion of option 82	: Enabled
DHCP relay information policy	: keep
DHCP Option82 Management-IP	: 0.0.0.0
DHCP maximum hop count	: 10
<hr/>	
DHCP helper-address for CPE is configured on following servers:	
10.1.1.2(Bundle10)	
<hr/>	
DHCP helper-address for vCM is configured on following servers:	
10.1.1.2(Bundle10)	
Router#	

CPE's DHCP Option82 Setting

To enable the system to insert the DHCP Option82 into CPE's DHCP message, use this command. To disable this feature, use the 'no' form of this command.

(hcpcd.)

Table 270 CPE's DHCP option82

Command	Description
cable relay-agent-option host	Specifies the CPE's DHCP Option82
no cable relay-agent-option host	Disable the CPE's DHCP Option82

Router# **configure terminal**
 Router(config)# **interface Bundle 10**
 Router(config-if-Bundle10)# **cable relay-agent-option host**
 Router(config-if-Bundle10)# **end**
 Router#

Cable GIADDR

To modify the GIADDR field for the DHCP DISCOVER and REQUEST packets with a relay IP address before they are forwarded to the DHCP server, use this command. To set the GIADDR field to its default, use the 'no' form of this command.

Table 271 cable GIADDR modification

Command	Description
cable dhcp-giaddr A.B.C.D (cable-modem host)	Specifies the GIADDR of vCM and CPE
no cable dhcp-giaddr A.B.C.D (cable-modem host)	Removes the Specified GIADDR of vCM and CPE

```

Router# configure terminal
Router(config)# interface Bundle 10
Router(config-if-Bundle10)# cable dhcp-giaddr 10.1.1.1 cable-modem
Router(config-if-Bundle10)# cable dhcp-giaddr 20.1.1.1 host
Router(config-if-Bundle10)# end
Router#

```

To select the control policy, so that the primary address is used for cable modems and the secondary address is used for hosts and other customer premises equipment (CPE) devices, use this command.

Table 272 cable GIADDR policy

Command	Description
cable dhcp-giaddr policy strict	Specifies the GIADDR policy
no cable dhcp-giaddr policy strict	Disable the Specified GIADDR policy

```

Router# configure terminal
Router(config)# interface Bundle 10
Router(config-if-Bundle10)# cable dhcp-giaddr policy strict
Router(config-if-Bundle10)# end
Router#

```

DHCP Option 43/17 for Vendor Specific Information

CableLabs defined Vendor Specific Information(Option43/17) as a DHCP IPv4/IPv6 option for cable operator's provisioning system information about product that can be used to make device and service configuration decisions during the CM provisioning process.

To add Vendor Specific Information to the DHCP option, the CM vendor model must be specified with the following command.

Command	Description
cable modem embedded vendor WORD model WORD	Specifies the embedded CM for Option43/17
no cable modem embedded vendor WORD model WORD	Removes the specified the embedded CM

```

Router# configure terminal
Router(config)# cable modem embedded vendor CommScope model C1004
Router(config)# end
Router#

```

The following sub-options of Option43/17 are currently supported for the DPoE system.

DHCP Option 43/17	Value	Description

Sub-option 2	<Device Type>	Device type of the component making the DHCP request.
Sub-option 3	"ECM:<eSAFE1:...:eSAFE _n >"	Colon-separated list of eCM and eSAFE(s) contained in the complete eDOCSIS device. First on the list MUST be "ECM" for eCM. <eSAFE> is a embedded Router in case of DPoE product.
Sub-option 5	<Hardware version>	Hardware version number. Identical to value as reported in the <Hardware version> field in the MIB object sysDescr.
Sub-option 6	<Software version>	Software version number. Identical to value as reported in the <Software version> field in the MIB object sysDescr.
Sub-option 7	<Boot ROM version>	Boot ROM version. Identical to value as reported in the <Boot ROM version> field in the MIB object sysDescr.
Sub-option 9	<Model number>	Device model number. Identical to value as reported in the <Model number> field in the MIB object sysDescr.
Sub-option 10	<Vendor name>	Vendor name or ID. Identical to value as reported in the <Vendor name> field in the MIB object sysDescr.

To use the Vendor Specific Information(Option43/17) for CableLabs, use this command.

Command	Description
cable dhcp-option-insert vendor-specific-info	Enables the Option43/17
no cable dhcp-option-insert vendor-specific-info	Disable the Option43/17

```

Router# configure terminal
Router(config)# interface Bundle 1
Router(config-if-Bundle1)# cable dhcp-option-insert vendor-specific-info
Router(config-if-Bundle1)# end
Router#

```

DHCP Option 6 for MSO defined text

Operator can specify the specific MSO definded text to a cable interface. It can be utilized by the provisioning server to determine the profile for the user.

To use the MSO defined text(Option 6), use this command.

Command	Description
cable dhcp-option-insert mso-defined-text LINE	Specifies the MSO defined text
no cable dhcp-option-insert mso-defined-text	Removes the specified MSO defined text

```
Router# configure terminal
Router(config)# interface TponInterface 1/1
Router(config-if-Tpon1/1)# cable dhcp-option-insert mso-defined-text SUB1
Router(config-if-Tpon1/1)# end
Router#
```

DHCP Option 82 Sub-option for DPoE Version

To insert the DPoE Version suboption into DHCP Option 82, use this command.

Command	Description
cable dhcp-option-insert dpoe	Enables the DPoE Version Sub-option in DHCP Option 82
no cable dhcp-option-insert dpoe	Disable the specified DPoE Version Sub-option

```
Router# configure terminal
Router(config)# interface Bundle 1
Router(config-if-Bundle1)# cable dhcp-option-insert dpoe
Router(config-if-Bundle1)# end
Router#
```

Source Address Verification (SAV) management

Source Address Verification (SAV) is a feature originally defined by DOCSIS. SAV is an enforcement mechanism that requires that all CPE IP addresses either are assigned via DHCP or are statically configured via the CM configuration file. Any upstream frames with IP source addresses that are not assigned via DHCP or statically provisioned must be dropped and counted.

CPE's SAV Setting

To enable verification of IP addresses for CPE devices on the upstream, use this command. To disable verification, use the 'no' form of this command.

Table 273 Source Address Verification (SAV)

Command	Description
cable source-verify	Enable SAV feature
no cable source-verify	Disable SAV feature

```
Router# configure terminal
Router(config)# interface Bundle 10
Router(config-if-Bundle10)# cable source-verify
Router(config-if-Bundle10)# end
Router#
Router# show cable modem cpe
MAC Address          IP Address      Dual IP      Device Class
0001c.25bc.c546 10.25.8.211 no           cpe

Router# show cable modem dpoe-cpe
CM MAC Addr        CM IP Addr      I/F      S/C      CPE MAC Addr      CPE IP Addr
000d.b641.c3e8 172.17.10.100 1(CMCI) 10/3  001c.25bc.c546 10.25.8.211

Router#
```

Static SAV Setting

SAV CM Authorizations are used to ensure that CPEs located behind CMs cannot successfully spoof addresses in order to obtain access to services or to disrupt services to others. SAV CM Authorizations define subnets from which CPEs are allowed to use statically assigned addresses and not have to obtain them via DHCP.

To enable the use of SAV CM Authorizations, use this command. This feature is only applicable when the **cable source-verify** command of bundle interface is enabled.

Table 274 Static Source Address Verification (SAV)

Command	Description
cable source-verify enable-sav-static	Enable Static SAV feature
no cable source-verify enable-sav-static	Disable Static SAV feature

```
Router# configure terminal
Router(config)# cable source-verify enable-sav-static
Router(config)# end
Router#
```

The Instances of TLV-43.7 in the CM configuration file refer to the following group name of SAV CM Authorization prefix rules. To create a group name of SAV CM Authorization prefix rules, use the following command.

Table 275 Source Address Verification (SAV) group

Command	Description
cable source-verify group GROUPNAME	Create SAV group
no cable source-verify enable-sav-static	Remove SAV group

```
Router# configure terminal
Router(config)# cable source-verify group savCfgList
Router(config-sav-group-savCfgList)# static-sav-address 10.50.1.0/24
Router(config-sav-group-savCfgList)# end
Router#
```

Subscriber Management

Subscriber Management in DPoE System focuses on two main areas. First is the learning of CPE Addresses and controlling the number allowed to be learned on a per-ONU basis. Second is the filtering of subscriber frames based on various criteria.

Both the DPoE system and the DPoE ONU take part in subscriber management functionality. This section describes the subscriber management functionality supported by system.

CPE Learning Control at the DPoE System

To specify the default value for the maximum number of IPv4 addresses allowed for CPEs behind an ONU, use this command. This value is used whenever TLV-35 (subscriber management control) is not present in a CM config file.

The default maximum number of IPv4 addresses allowed for CPEs behind an ONU is 16.

Table 276 default maximum number of IPv4 CPEs behind an ONU

Command	Description
cable submgmt default max-cpe (<1-1023> unlimit)	Specifies the default maximum number of IPv4 addresses allowed for CPEs behind an ONU.
no cable submgmt default max-cpe	Changes the specified value to default.


```
Router# configure terminal
Router(config)# cable submgmt default max-cpe unlimit
Router(config)# end
Router#
```

To define the docsSubmgt3BaseCpeActiveDef value that controls whether a limit is placed on how many CPE IP Addresses can be learned and pass data from behind an ONU, use this command. If TLV-35 is not present in a CM Configuration file, this value is used in place of the TLV-35 “Active” bit value.

This value is Disabled by default.

Table 277 docsSubmgt3BaseCpeActiveDef control

Command	Description
cable submgmt default active	Enable docsSubmgt3BaseCpeActiveDef control
no cable submgmt default active	Disable docsSubmgt3BaseCpeActiveDef control


```
Router# configure terminal
Router(config)# cable submgmt default active
Router(config)# end
Router#
```

To define the docsSubmgt3BaseCpeLearnableDef value that controls whether CPE IP Addresses will be learned and allowed to pass traffic from behind an ONU, use this command. If TLV-35 is not present in a CM Configuration file, this value is used in place of this TLV-35 “Learnable” bit value.

This value is Enabled by default.

Table 278 docsSubmgt3BaseCpeLearnableDef control

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

cable submgmt default learnable	Enable docsSubmgt3BaseCpeLearnableDef control
no cable submgmt default learnable	Disable docsSubmgt3BaseCpeLearnableDef control
<pre>Router# configure terminal Router(config)# cable submgmt default learnable Router(config)# end Router#</pre>	

CPE Learning Control at the ONU

ONUs are required by DPoE to perform dynamic learning of CPE addresses, and to limit and control the number of addresses that are allowed to exist behind the ONU. This learning and control is for L2 MAC Addresses, as well as for L3 IP Addresses.

To control the number of CPE MAC Addresses, the “Maximum Number of CPEs” TLV-18 is used in the CM Configuration File. If this override is configured, any TLV-18 value found in a CM Configuration file is ignored and the override value is used. This system only applies the TLV-18 or global override value to ONUs that are configured for IP(HSD) service.

TLV-18 does not apply to MEF services.

Although DPoE requires the control of L3 CPE addresses at the ONU, it is currently not possible because DPoE OAM does not provide any applicable messaging. Due to this, ONUs are currently only able to control L2 CPE addresses.

To define a global override for TLV-18 values found in CM Configuration files, use this command.

This value has 65535(disables override) by default.

Table 279 global override (Maximum Number of CPEs)

Command	Description
cable modem max-cpe-mac <0-65535>	Specifies the global override value. “0” means “unlimited”
no cable modem max-cpe-mac	Change specified global override value to default.
<pre>Router# configure terminal Router(config)# cable modem max-cpe-mac 10 Router(config)# end Router#</pre>	

Filtering at the DPoE System

DPoE requires filtering of subscriber frames to be performed by the DPoE System. These filtering requirements are the same as those required by DOCSIS on CMTS equipment.

To define both docsSubmgt3BaseSubFilterDownDef value that specifies the CPE downstream filter group to use and docsSubmgt3BaseSubFilterUpDef value that specifies the CPE upstream filter group to use, the docsSubmgt3FilterGrpTable must be configured.

To modify the parameters of docsSubmgt3FilterGrpTable, docsSubmgt3FilterGrpTable must be created. To create docsSubmgt3FilterGrpTable, use the following commands.

Table 280 submgt filter group creation

Command	Description
cable filter-group <1-1024> index <1-65535>	Creates docsSubmgt3FilterGrpTable “<1-1024>” means “Group Id” “<1-65535>” means index of filter group in “Group Id”.

no cable filter-group <1-1024> index <1-65535>	Removes docsSubmgt3FilterGrpTable
---	-----------------------------------

To modify the parameters of filter group, use the following command in the filter-group command node.

Table 281 parameter setting of filter group table

Command	Description
match-action (accept drop) no match-action	The action to take when this filter rule matches a packet. (default: permit)
priority <1-65535> no priority	Defines the order in which the filter rules are compared against packets. The higher the value, the higher the priority. (default: 0)
ip-tos low <1-255> high <1-255> no ip-tos	The low and high value of a range of IP ToS octet values. (default: low 0, high 0)
ip-tos-mask <1-255> no ip-tos-mask	The mask value that is bitwise ANDed with the IP ToS octet in an IP packet, and the resulting value, are used for range checking against ip-tos-low and ip-tos-high. (default: 0)
ip-proto <1-257> no ip-proto	The value of the IP Protocol field required for IP packets to match this filter rule. The value 256 matches traffic with any IP protocol value. The value 257 by convention matches both TCP and UDP. (default: 256)
ip-version ipv4 no ip-version	The type of IP address for src-ip, src-mask, dest-ip, and dest-mask. IPv6 is not currently supported. (default: unknown)
src-ip A.B.C.D src-mask A.B.C.D no src-ip	The values of the IP Source Address required for packets to match this filter rule. An IP packet matches the rule when the packet's IP Source Address, bitwise ANDed with the src-mask value, equals the src-ip value. (default src-ip: 0.0.0.0, default src-mask: 0.0.0.0)
dest-ip A.B.C.D dest-mask A.B.C.D no dest-ip	The value of the IP Destination Address required for packets to match this filter rule. An IP packet matches the rule when the packet's IP Destination Address, bitwise ANDed with the dest-mask value, equals the dest-ip value. (default dest-ip: 0.0.0.0, default dest-mask: 0.0.0.0)
range-src-port <0-65535> <0-65535> no range-src-port	The low-end and high-end inclusive range of TCP/UDP source port numbers to which a packet is compared. This command is irrelevant for non-TCP/UDP packets. (default start port: 0, default end port: 65535)
range-dest-port <0-65535> <0-65535> no range-dest-port	The low-end and high-end inclusive range of TCP/UDP destination port numbers to which a packet is compared. This command is irrelevant for non-TCP/UDP packets. (default start port: 0, default end port: 65535)
dest-mac-addr H.H.H no dest-mac-addr	This value of the Destination MAC Address required for packets to match this filter rule. An Ethernet packet matches an entry when its destination MAC address, bitwise ANDed with the dest-mac-mask, equals the value of the dest-mac-addr. (default: 0000.0000.0000)
src-mac-addr H.H.H no src-mac-addr	The value to match against an Ethernet packet source MAC address. (default: ffff.ffff.ffff)
eth-proto-type etherType no eth-proto-type	"etherType" indicates the format of the L3 protocol ID in the Ethernet packet. The filter rule applies only to frames that contain an EtherType value. (default: none)
eth-proto <1-65535> no eth-proto	This value represents the Ethernet protocol type to be matched against the packets. With eth-proto-type set to "none", this value is ignored when considering whether a packet matches the filter rule. If the value eth-proto-type is "etherType", this value gives the 16-bit value of the EtherType that the packet must match in order to match the filter rule. (default: 0)

vlan-id <1-4094> no vlan-id	This value applies only to Ethernet frames using the 802.1p/Q tag header. Tagged packets must have a VLAN Identifier that matches the value in order to match the filter rule. (default: 0)
cm-inf-mask HEXVALUE no cm-inf-mask	This value represents a bit-mask of the CM inbound interfaces to which this filter rule applies. This attribute only applies to Upstream Drop Classifiers being sent to CMs during the registration process.

```

Router# configure terminal
Router(config)# cable filter-group 1 index 1
Router(config-filter-group-1,1)# match-action drop
Router(config-filter-group-1,1)# ip-proto 257
Router(config-filter-group-1,1)# end
Router#
Router# show cable filter
FilterID      SrcAddr/Mask          DestAddr/Mask     Prot SPort DPort Action
0001,0001    0.0.0.0/00           0.0.0.0/00       257    0      0   drop
Router#
Router# show cable filter group 1 index 1
Filter Group      : 1
Filter Index      : 1
Matches
  Match Action    : drop
  Priority        : 0
  IP TOS Low      : 0
  IP TOS High     : 0
  IP TOS Mask     : 0
  IP Protocol     : 257
  InetAddrType   : unknown
  IP Src Addr    : 0.0.0.0
  IP Src Mask     : 0.0.0.0
  IP Dst Addr    : 0.0.0.0
  IP Dst Mask     : 0.0.0.0
  Src Port        : 0 ~ 65535
  Dst Port        : 0 ~ 65535
  Dst MAC Addr   : 0000.0000.0000
  Dst MAC Mask   : 0000.0000.0000
  Src MAC Addr   : FFFF.FFFF.FFFF
  Enet-Proto Type: none
  Enet-Proto      : 65535
  User Priority   : 0 ~ 7
  Vlan ID         : 0
  CM If Mask      :
Router#

```

ONU Encryption and Authentication

This system supports Early Authentication and Encryption (EAE) as defined by the DPoE 1.0 Security Specification.

To enable or disable the “ONU Encryption and Authentication” feature, use the following command in the PON Interface.

This feature is disabled by default.

Table 282 Early Authentication and Encryption (EAE) enable/disable

Command	Description
cable privacy eae-policy total-enforcement	Enables EAE on the interface
no cable privacy eae-policy total-enforcement	Disables EAE on the interface

```
Router# configure terminal  
Router(config)# interface EponInterface 2/1  
Router(config-if-Epon2/1)#cable privacy eae-policy total-enforcement  
Router(config-if-Epon2/1)#end  
Router#
```

Security and Certificate Settings

To enable or disable two ONU Authentication checks performed by system when it validates an ONU certificate, use the following command.

Table 283 security and certificate settings

Command	Description
cable privacy certificate (trusted untrusted) skip-validity-period (true false) tek-lifetime <0-604800>	Specifies the security and certificate.
no cable privacy certificate (trusted untrusted) skip-validity-period (true false) tek-lifetime <0-604800>	Changes the configured value to default

certificate (trusted|untrusted)

The default trust of the self-signed manufacturer certificate entries, contained in docsBpi2CmtsCACertTable and created after this object is set.

Default: untrusted

skip-validity-period (true|false)

Setting this object to True causes all chained and root certificates in the chain to have their validity periods checked against the current time of day when the DPoE system receives a request from the OLT SoC to authorize the ONU.

Default: True

tek-lifetime <0-604800>

The lifetime, in seconds, of the traffic encryption key (TEK) used on each ONU link.

Default: 43200

```
Router# configure terminal  
Router(config)# interface EponInterface 2/1  
Router(config-if-Epon2/1)# cable privacy certificate trusted skip-validity-period false tek-lifetime 1800
```

```
Router(config-if-Epon2/1)# end  
Router#
```

CA Certificate

CA Certificate is used to provision the trust value of a CA certificate. System makes use of the trust value when verifying the ONU device certificate chain during the ONU Authentication process.

To create a CA Certificate entry, use the following command.

Table 284 CA Certificate entry creation

Command	Description
crypto ca trustpoint <1-4294967295> cli	Creates CA Certificate entry “<1- 4294967295>” means the index of entry
no crypto ca trustpoint <1-4294967295> cli	Removes CA Certificate Table

To modify the parameters of CA Certificate entry, use the following command in the crypto-ca-trustpoint command node.

Table 285 parameter setting of CA Certificate

Command	Description
trust (1 2 3 4) no trust	Specifies the trust state of the CA certificate. - Trusted (1): CA Certificate is to be trusted even if the certificate was found to be invalid. - Untrusted (2): CA Certificate is to be untrusted even if the certificate was found to be valid. - Chained (3): CA Certificate is chained to a root CA certificate. - Root (4): CA Certificate is a root CA certificate. Default is Chained (3).
certificate DER-ENCODED-CA no certificate	Specifies the X.509 DER-encoded ONU device certificate

```
Router# configure terminal  
Router(config)# crypto ca trustpoint 1 cli  
Router(crypto-ca-trustpoint-1)# trust 1  
Router(crypto-ca-trustpoint-1)# certificate 3082036030820248a0030201  
02021009b02ee36372146e062f335b65f1653a300d06092a864886f70d0101050500304a310b300906035504  
061302555331123010060355040a13094361626c654c616273312730250603550403131e4361626c654c6162  
73204d616e75666163747572657220526f6f74204341301e1.....  
Router(crypto-ca-trustpoint-1)# end  
Router#
```

CM Certificate

CM Certificate is used to provision the trust value of an ONU device certificate. System makes use of the trust value when verifying the ONU device certificate during the ONU Authentication process.

To create a CM Certificate entry, use the following command.

Table 286 CM Certificate entry creation

Command	Description
crypto ca certificate chain H.H.H cli	Creates CM Certificate entry “H.H.H” means the MAC address of the ONU
no crypto ca certificate chain H.H.H cli	Removes CM Certificate Table

To modify the parameters of CM Certificate entry, use the following command in the crypto-ca-certificate-chain command node.

Table 287 parameter setting of CM Certificate

Command	Description
trust (1 2) no trust	Specifies the trust state of the provisioned ONU certificate. - Trusted (1): ONU certificate is to be trusted even if the certificate was found to be invalid. - Untrusted (2):ONU certificate is to be untrusted even if the certificate was found to be invalid. Default is Untrusted (2).
certificate DER-ENCODED-CERT no certificate	Specifies the X.509 DER-encoded ONU device certificate

```
Router# configure terminal
Router(config)# crypto ca certificate chain 000d.b640.5060 cli
Router(crypto-ca-certificate-chain-000d.b640.5060)# trust 1
Router(crypto-ca-certificate-chain-000d.b640.5060)# certificate 3082
036030820248a003020102021009b02ee36372146e062f335b65f1653a300d06092a864886f70d0101050500
304a310b300906035504061302555331123010060355040a13094361626c654c61627331273025060355040
3131e4361626c654c616273204d616e7566616374757265722.....
Router(crypto-ca-certificate-chain-000d.b640.5060)# end
Router#
```

Certificate Revocation List

This system supports a feature that allows an operator to configure whether system will use a Certificate Revocation List (CRL) during the ONU Authentication process, and where system Must retrieve the CRL. This feature is used to fulfill requirements of DPoE Security specification.

A CRL is a file containing a list of X.509 certificates that have been revoked. If provisioned to do so, system downloads the CRL from the provisioned CRL server URL. System then makes use of the CRL whenever it authenticates an ONU. System checks the CRL to determine if either the Manufacturer CA certificate or the ONU device certificate passed up to system have been revoked. If either or both certificates have been revoked and either or both certificates have not been provisioned as trusted, then system fails the ONU Authentication process for that ONU.

To specify the CRL method, use the following command.

Table 288 Certificate Revocation List (CRL) Method

Command	Description
cable privacy revocation method (crl ocsp both)	Specifies which certificate revocation method is to be used by system to verify the ONU certificate validity. Default: none
no cable privacy revocation method (crl ocsp both)	Changes specified CRL method to default

crl

System does not attempt to determine the revocation status of a certificate.

ocsp

System uses a Certificate Revocation List (CRL) as defined by the **cable privacy revocation crl url WORD** command.

both

System uses both CRL and OCSP.

```
Router# configure terminal  
Router(config)# cable privacy revocation method crl  
Router(config)# end  
Router#
```

To specify the URL of CRL, use the following command.

Table 289 URL of Certificate Revocation List (CRL)

Command	Description
cable privacy revocation crl (url WORD refresh-interval <1-524160>)	Specifies the URL of CRL and refresh interval.
no cable privacy revocation crl (url refresh-interval)	Changes specified value to default

url WORD

The URL from where system will retrieve the CRL. The maximum length of the URL is 255 characters.

refresh-interval <1-524160>

This is the refresh interval, in minutes, for system to retrieve the CRL with the purpose of updating its Certificate Revocation List.

Default refresh interval is 10,080 minutes (7 days)

```
Router# configure terminal
Router(config)# cable privacy revocation crl url http://www.crls.com
Router(config)# cable privacy revocation crl refresh-interval 14400
Router(config)# end
Router#
```

Online Certificate Status Protocol

This system supports a feature that allows an operator to configure whether system will use the Online Certificate Status Protocol (OCSP) during the ONU Authentication process. This feature is used to fulfill requirements of DPoE Security specification.

If provisioned to do so, system sends a request to the provisioned OCSP URL to query the revocation status of a certificate. System queries the revocation status of both the Manufacturer CA certificate and the ONU device certificate passed up to system. If the OCSP reply indicates that either or both certificates have been revoked and either or both certificates have not been provisioned as trusted, then system fails the ONU Authentication process for that ONU.

To specify the OCSP during the ONU Authentication process, use the following command.

Table 290 Online Certificate Status Protocol (OCSP)

Command	Description
cable privacy revocation ocsp (url WORD skip-sig-check timeout <1-600000>)	Specifies the OCSP feature
no cable privacy revocation ocsp (url skip-sig-check timeout)	Changes specified OCSP values to default

url WORD

The URL from which system will retrieve the OCSP information. The maximum length of the URL is 255 characters.

skip-sig-check

Used to enable or disable signature checking on OCSP response messages.

Default is False.

timeout <1-600000>

The time, in milliseconds, that system will wait for an OCSP response.

Default is 1000 msec.

```
Router# configure terminal
Router(config)#cable privacy revocation ocsp url http://www.ocsp.com
Router(config)#cable privacy revocation ocsp skip-sig-check
Router(config)#cable privacy revocation ocsp timeout 5000
Router(config)#end
Router#
```

EAE Exclusion List

This system supports a feature that allows an operator to configure which ONUs are allowed to bypass ONU Encryption and Authentication when registering with the DPoE System. This feature also allows the operator to configure which ONUs are allowed to bypass Secure Software download when they are upgraded.

Entries in the EAE Exclusion List consist of a base MAC Address and a MAC Address Mask to allow ranges of MAC addresses to be specified (similar to IP Network Address/Mask). Entries within the EAE Exclusion List are not allowed to overlap. If an entry being created overlaps an existing entry, an error status is returned in response to the provisioning request.

When an ONU starts the registration process with system, system checks if the ONU's primary link MAC address is contained within an entry of the EAE Exclusion List. MAC addresses that match an entry in the EAE Exclusion List cause system to skip link encryption and ONU Authentication for that ONU.

This feature is provided to allow operators to register ONUs that do not support EAE, so that they can be upgraded to a version of firmware that supports both ONU Link Encryption and ONU Authentication.

When the software download process is initiated for an ONU, if the ONU's primary link MAC address is contained within an entry of the EAE Exclusion List, Secure software Download is not performed. This allows a raw ONU image to be downloaded and installed onto the ONU for the case where the ONU is running an older version of firmware that does not support Secure Software Download.

To add ONU MAC Addresses in the EAE Exclusion List, use the following command.

Table 291 EAE Exclusion List

Command	Description
cable privacy eae-exclude H.H.H (mask <1-48>)	Add ONU MAC Address in the EAE Exclusion List.
no cable privacy eae-exclude H.H.H	Delete ONU MAC Address from the EAE Exclusion List

```
Router# configure terminal
Router(config)# cable privacy eae-exclude 000d.b6ea.0080 mask 48
Router(config)#end
Router#
Router# show cable privacy eae-exclude
EAE Exclusion List:
    MAC: 000d.b6ea.0080 Mask: ffff.ffff.ffff
```

```
Router#
```

ONU White List

The ONU White List is a feature that enables an operator to configure the DPoE System PON Ports on which an ONU is permitted to register. This ONU White List is used to fulfill requirements of the DPoE Security specification.

The ONU White List works by having system ignore all Link Discovery Autonomous HMI messages for a particular ONU when that ONU is trying to register on a PON port that it is not provisioned to be on.

When the ONU White List is used, it is important to note that it is necessary to configure each and every ONU that is supposed to register on the DPoE System. In other words, if the table is empty, ONUs can register on any PON interface. When the ONU White List contains one or more entries, only ONUs that match these values are permitted into the DPoE System.

If an ONU might connect to more than one PON port, the operator must include an entry for the ONU MAC address for each PON port. In this way, an ONU can be moved between PON ports while the ONU White List feature is operating.

To add ONU Maccesses for each PON port, use the following command.

Table 292 ONU White List

Command	Description
cable modem allow-list H.H.H	Add ONU MAC Address into White List
no cable modem allow-list H.H.H	Delete ONU MAC Address from White List

```
Router# configure terminal
Router(config)# int EponInterface 2/1
Router(config-if-Epon2/1)# cable modem allow-list 000d.b641.c3e8
Router(config-if-Epon2/1)# end
Router#
Router# show cable modem allowed
I/F      MAC Address
C2/1    000d.b641.c3e8
Router#
```

CM Offline List

CM Offline List

The CM Offline list is a diagnostic feature to assist operators in identifying ONUs that were once connected, but are no longer connected to the DPoE System. When a virtual CM goes offline due to an ONU reset or other virtual CM Operation (e.g., failure to complete authorization, registration, IP address acquisition, CM configuration file download, etc.), the DPoE system's representation of the virtual CM remains accessible for a provisioned period of time.

To modify the CM Offline List aging feature, use the following command.

Table 293 CM Offline List aging

Command	Description
cable offline-list aging <1-864000>	Modifies the period of time, in seconds, that a virtual CM will remain in the offline state. (Default: 86400s (1 day))

```
Router# configure terminal
Router(config)# cable offline-list aging 86400
Router(config)# end
Router#
Router# show cable modem offline
Interface    MAC address      Prim Previous Offline          Rx      Rx      SM
                           Sid   State       Time
                           Power SNR   Exhaust
                                         Count

Router# clear cable modem offline delete
Router#
```

CM Flap List

The CM Flap List is a diagnostic feature to assist operators in identifying instability associated with ONU connectivity and initialization. Operators monitor and analyze the CM Flap List to determine if a specific vCM is having difficulty completing registration (e.g., improperly configured modem provisioning files will result in the vCM, associated with the ONU, failing registration, and resetting the ONU). Operators also monitor and analyze the Flap List to determine if specific segments of the fiber plant are unstable, for example, many vCM flap entries for ONUs on a specific interface may indicate poor plant conditions.

To provision the CM Flap List, use the following command.

Table 294 CM Flap List provisioning

Command	Description
cable flap-list (aging <1-86400> size <1-65535> insertion-time <60-86400>)	Modifies the CM Flap List feature.

aging <1-86400>

The period of time, in minutes, that a virtual CM will remain on the Flap List.

Default is 10080 minutes. (7 days)

size <1-65535>

The maximum number of entries on a given downstream interface that are permitted on the Flap list. Once full, no additional entries can be inserted onto the list.

This maximum value is defined as a per-downstream limit applied to the channel-based representation of the Flap List. This maximum is multiplied by the number of provisioned downstream interfaces to define a DPoE System-wide limit for the legacy representation of the Flap List.

Default is 100.

insertion-time <60-86400>

Specifies the minimum insertion (registration) time interval in seconds. Any vCM that makes a registration request more frequently than this period of time is placed in the Flap List.

Default is 180s. (3 minutes)

```
Router# configure terminal
Router(config)# cable flap-list aging 10080
Router(config)# cable flap-list size 200
Router(config)# cable flap-list insertion-time 300
Router(config)# end
Router#
Router# show cable modem offline
Interface    MAC address      Prim Previous Offline          Rx     Rx     SM
                           Sid   State       Time
                           Power SNR   Exhaust
                                         Count

Router# show cable flap-list
MAC Address    CableIF      Ins   Hit   Miss   CRC   P-Adj Flap   Time

Router#
Router# clear cable flap-list ?
  H.H.H  MAC address (HHHH.HHHH.HHHH)
  all    All cable modems
Router# clear cable flap-list
```

Optical Monitoring

This System provides access to the PON Optical Monitoring information provided by OLTs and ONUs, which can be used to detect and diagnose problem in the optical network. Optical monitoring information includes:

■ For OLT PON Ports:

- Transmit laser power
- Laser supply voltage
- Laser bias current
- Laser Temperature
- Received idle laser power

■ For ONUs:

- Transmit laser power
- Laser supply voltage
- Laser bias current
- Laser Temperature
- Received laser power

In addition to the optical monitoring data, system also provides CRC and Line Coding errors, as well as statistics on how well Forward Error Correction (FEC) is working on the upstream PON.

The following example CLI commands demonstrate the use of the Optical Monitoring information.

Router# show interface epon downstream

I/F	Power (dBm)	VCC (V)	Bias (mA)	Temp (C)	Bytes	Frames	FEC Blks TX
C2/1	0.00	0.00	0	0.00	0	0	0
C2/2	0.00	0.00	0	0.00	0	0	0
C2/3	0.00	0.00	0	0.00	0	0	0
C2/4	0.00	0.00	0	0.00	0	0	0
C2/5	0.00	0.00	0	0.00	0	0	0
C2/6	0.00	0.00	0	0.00	0	0	0
C2/7	0.00	0.00	0	0.00	0	0	0
C2/8	5.04	3.28	10	41.07	10895936	1732749	0

Router# show interface epon upstream

I/F	Power (dBm)	Frames	CRC-8 Errs	Coding Errs	Pckt Errs
C2/1	0.00	0	0	0	0
C2/2	0.00	0	0	0	0
C2/3	0.00	0	0	0	0
C2/4	0.00	0	0	0	0
C2/5	0.00	0	0	0	0
C2/6	0.00	0	0	0	0
C2/7	0.00	0	0	0	0
C2/8	-36.99	0	0	0	0

Router# show epon onu monitor

MAC Addr	TX Power (dBm)	VCC (V)	Bias (mA)	Temp (C)	RX Power (dBm)
0010.1899.d848	2.49	3.20	33	56.27	-7.84

CM Power Levels

System provides access to transmit and receive laser power information in the following units wherever power levels are reported.

- Power in units of tenths of a microWatt
- Power in units of dBm

To support the reporting of power-level information for existing DOCSIS MIBs and existing CLI commands, System also provides power measurements in units of tenths of dBm V x 10 for power levels reported for each vCM/ONU on the DPoE System.

The following example CLI commands demonstrate the use of the power level information.

```
Router# show epon onu
MAC Address      OLT          LLID   EPON    RX     RTT   Prod  Prod  Frmwr  OAM
                           Port   Power
0007.70e8.f48c  000d.b623.0020  0000  0/0    -8.53  380  2000  0001  E324  ---
                                                               Code  Vers  Vers

Router# show cable modem
MAC Address      IP Address    I/F      MAC      Prim RxPwr Timing Num   BPI
                           State   Sid  (db)  Offset CPEs Enb
0007.70e8.f48c  10.50.101.186  C2/1    online   1     38.7   62    0   N
```

CM TFTP Client Settings

The relatively long retry and time-out duration values for the TFTP download Retry and TFTP Wait parameters may not be desired in lab environments or real deployments.

In most cases, vCM configuration files should be under 1 MB in size and ONU firmware files should be under 100 MB in size. System provides protection from operator errors or malicious activity that result in transferring huge files (hundreds of MB or GB in size) to the system. By default, system permits file transfers of no more than 500 KB.

To modify the vCM TFTP Client settings, use the following command.

Table 295 vCM TFTP Client settings

Command	Description
cable modem tftp-max-file-size <150-104857> no cable modem tftp-max-file-size	Changes the maximum file size, in 1 KB units. (Default: 1100 KB)
cable modem tftp-retries <0-99> no cable modem tftp-retries	Changes the maximum number of retries that will be attempted when retrieving a file from a TFTP server. (Default: 3)

```
Router# configure terminal  
Router(config)# cable modem tftp-max-file-size 1000  
Router(config)# cable modem tftp-retries 5  
Router(config)# end  
Router#
```

CM Event Management

In this chapter, the system for managing the CM in the Event management is described. Event of the CM collected from the system are sent to the server using the Syslog message, or, to the SNMP trap receiver using SNMP TRAP message. All the collected events can be stored in non-volatile memory for events after the system reboots so that they can be utilized to trace the events.

In order to collect CM Event the Event Id must be registered in the system, and non-registered Event Event Id will be automatically discarded.

In order to register the Event Id, use the following command.

Table 300 CM Event Id registration

Command	Description
cable event ctrl-event-id <0-4294967295>	Register the Event Id. Event Id “0” enables the Event of every CM to be collected in the system.
no cable event ctrl-event-id <0-4294967295>	Remove the registered Event Id.

```
Router# configure terminal
Router(config)# cable event ctrl-event-id 0
Router(config)# end
Router#
Router# show cable event

- Ev TrapLog Level : 5
- Ev ThrottleThresholdExceeded : FALSE

Last Issued Date   EvCounts Lv     EvId      EvText
2013-12-09 04:32:48 00000003 5 3098281942 Cmts  : Link down;ifIndex=200120
2013-12-09 04:32:48 00000003 5    80000101 Link down;ifIndex=200120;ifAlias=US-Cable2/1
2013-12-09 04:32:48 00000001 4    82010400 Failed to receive Periodic RNG-REQ from modem (SID 1), timing-out
SID:CM-MAC=00:07:70:e8:
f4:8c;CM-QOS=1.1;CM-VER=3.0;CMTS-VER=3.0;REG-ID=1;Link loss alarm, de-registering CM in state Operational (8);

Router#
Router# clear cable event
Router#
Router# show cable event

- Ev TrapLog Level : 5
- Ev ThrottleThresholdExceeded : FALSE

Router#
```

Event Log Control

The Event that occurs in each CM is written in a volatile local log which will be recorded into a permanent storage. The stored information at the permanent storage will be used to restore the Event Table to the event status after the system reboots.

The Event Logs which CM generates can be transferred to syslog servers according to the operator's preference. They can issue SNMP TRAP to SNMP Trap Receiver.

In order to manage Event Log, use the following commands.

Table 301 Event Log Control

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

<code>cable event control (all <0-8> alerts critical debugging emergencies errors informational notifications warnings trace) volatile</code>	Write the Events of specified Event Level to volatile storage only.
<code>no cable event control (all <0-8> alerts critical debugging emergencies errors informational notifications warnings trace) volatile</code>	Write the Events of specified Event Level to non-volatile storage only
<code>cable event control (all <0-8> alerts critical debugging emergencies errors informational notifications warnings trace) (local traps syslog none)</code>	Assign the Action of the Event Level.
<code>no cable event control (all <0-8> alerts critical debugging emergencies errors informational notifications warnings trace) (local traps syslog none)</code>	Change the Action of the assigned Event Level to default.

local

Write all the received Event Log to both volatile and non-volatile storage.

traps

Transfer the received Event Log via SNMP TRAP. The way to adjust the SNMP Trap Host can be found at “Chapter 1 Overview”.

syslog

Transfer the received Event Log to Syslog server. The way to configure the Syslog server can be found at Logging configure in “Chapter11 Statistics Monitoring”.

none

Make no action to the received Event Log.

The system works out the Event management as Default, which is specified in DPoE 1.0 Specification. The Default actions are summarized as below.

Table 302 Default Actions of Event Level

Event Level	Default Action
Emergencies (0)	Local
Alerts (1)	Local
Critical (2)	Local, Trap, Syslog
Errors (3)	Trap, Syslog
Warnings (4)	Trap, Syslog
Notifications (5)	Trap, Syslog, volatile local log

```
Router# configure terminal
Router(config)# cable event control all local
Router(config)# end
Router#
Router# show cable event
```

- Ev TrapLog Level : 5
- Ev ThrottleThresholdExceeded : FALSE

Last Issued Date	EvCounts	Lv	EvId	EvText
2013-12-09 17:19:45	00000003	5	3098281942	Cmts : Link down;ifIndex=200120
2013-12-09 17:19:45	00000003	5	80000101	Link down;ifIndex=200120;ifAlias=US-Cable2/1

```

2013-12-09 17:19:45 00000001 4 82010400 Failed to receive Periodic RNG-REQ from modem (SID 1), timing-out
SID;CM-MAC=00:07:70:e8:
f4:8c;CM-QOS=1.1;CM-VER=3.0;CMTS-VER=3.0;REG-ID=1;Link loss alarm, de-registering CM in state Operational (8);

Router#
Router# show cable event logging
2013-12-09 17:25:02 [5] [3098281942] Cmts : Link down;ifIndex=200101
2013-12-09 17:25:02 [5] [0080000101] Link down;ifIndex=200101;ifAlias=Cable2/1
2013-12-09 17:25:02 [5] [3098281942] Cmts : Link down;ifIndex=200110
2013-12-09 17:25:02 [5] [0080000101] Link down;ifIndex=200110;ifAlias=DS-Cable2/1
2013-12-09 17:25:02 [5] [3098281942] Cmts : Link down;ifIndex=200120
2013-12-09 17:25:02 [5] [0080000101] Link down;ifIndex=200120;ifAlias=US-Cable2/1
2013-12-09 17:25:02 [4] [0082010400] Failed to receive Periodic RNG-REQ from modem (SID 1), timing-out SID;CM-
MAC=00:07:70:e8:f4:8c
;CM-QOS=1.1;CM-VER=3.0;CMTS-VER=3.0;REG-ID=1;Link loss alarm, de-registering CM in state Operational (8);
Router#
Router#
Router# show cable event logging flash
2013-12-09 17:25:02 [5] [3098281942] Cmts : Link down;ifIndex=200101
2013-12-09 17:25:02 [5] [0080000101] Link down;ifIndex=200101;ifAlias=Cable2/1
2013-12-09 17:25:02 [5] [3098281942] Cmts : Link down;ifIndex=200110
2013-12-09 17:25:02 [5] [0080000101] Link down;ifIndex=200110;ifAlias=DS-Cable2/1
2013-12-09 17:25:02 [5] [3098281942] Cmts : Link down;ifIndex=200120
2013-12-09 17:25:02 [5] [0080000101] Link down;ifIndex=200120;ifAlias=US-Cable2/1
2013-12-09 17:25:02 [4] [0082010400] Failed to receive Periodic RNG-REQ from modem (SID 1), timing-out SID;CM-
MAC=00:07:70:e8:f4:8c
;CM-QOS=1.1;CM-VER=3.0;CMTS-VER=3.0;REG-ID=1;Link loss alarm, de-registering CM in state Operational (8);
Router#
Router#
Router#

```

Event Log Size

The size of Cable Event Table which the system manages is limited to be 10. The content of Cable Event Table can be referred by **show cable event** command as well as collected to SNMP via docsDevEventTable MIB.

To change the size limit of Cable Event Table, use the following command.

Table 296 Event Log Size

Command	Description
cable event trap-buff-size <10-128>	Change the size of Cable Event Table. (Default: 10)
no cable event trap-buff-size	Return the changed size of Cable Event Table to default.

```

Router# configure terminal
Router(config)# cable event trap-buff-size 20
Router(config)# end
Router#
Router# show cable event

- Ev TrapLog Level : 5
- Ev ThrottleThresholdExceeded : FALSE

Last Issued Date   EvCounts Lv      EvId      EvText
2013-12-09 04:32:48 00000003 5 3098281942 Cmts : Link down;ifIndex=200120
2013-12-09 04:32:48 00000003 5 80000101 Link down;ifIndex=200120;ifAlias=US-Cable2/1
2013-12-09 04:32:48 00000001 4 82010400 Failed to receive Periodic RNG-REQ from modem (SID 1), timing-out
SID;CM-MAC=00:07:70:e8:
f4:8c;CM-QOS=1.1;CM-VER=3.0;CMTS-VER=3.0;REG-ID=1;Link loss alarm, de-registering CM in state Operational (8);

```

```
Router#
```

Event Throttling

System uses the objects in the docsDevEvent to control how many traps and syslog messages are generated by system within a given time frame. The operator can throttle the events to stay under a predefined threshold, stop generating events when the threshold is reached, or stop generating events altogether.

To control the transmission of traps and syslog messages with respect to the trap pacing threshold, use the following command.

Table 297 Throttle Admin Status

Command	Description
cable event throttle-admin (unconstrained maintainBelowThreshold stopAtThreshold inhibited)	Change the Throttle Admin Status. (Default: Unconstrained)
no cable event throttle-admin	Return the changed Throttle Admin Status to default.

unconstrained

Unconstrained causes traps and syslog messages to be transmitted without regard to the threshold settings.

maintainBelowThreshold

maintainBelowThreshold causes trap transmission and syslog messages to be suppressed if the number of traps would otherwise exceed the threshold.

stopAtThreshold

stopAtThreshold causes trap transmission to cease at the threshold and not to resume until directed to do so.

inhibited

inhibited causes all trap transmission and syslog messages to be suppressed.

```
Router# configure terminal
Router(config)# cable event trap-buff-size 20
Router(config)# end
Router#
Router# show cable event

- Ev TrapLog Level : 5
- Ev ThrottleThresholdExceeded : FALSE

Last Issued Date    EvCounts Lv     EvId      EvText
2013-12-09 04:32:48 00000003 5 3098281942 Cmts   : Link down;ifIndex=200120
2013-12-09 04:32:48 00000003 5 80000101 Link down;ifIndex=200120;ifAlias=US-Cable2/1
2013-12-09 04:32:48 00000001 4 82010400 Failed to receive Periodic RNG-REQ from modem (SID 1), timing-out
SID;CM-MAC=00:07:70:e8:
f4:8c;CM-QOS=1.1;CM-VER=3.0;CMTS-VER=3.0;REG-ID=1;Link loss alarm, de-registering CM in state Operational (8);
```

```
Router#
```

To change the number of events in the configured interval when throttling will occur, use the following command.

Table 298 Event Throttle Threshold

Command	Description
cable event throttle-threshold <1-10000>	Set the value of Throttle Threshold. (Default: 0)
no cable event throttle-threshold	Return the set Throttle Threshold to default.

```
Router# configure terminal
Router(config)# cable event throttle-threshold 20
Router(config)# end
Router#
```

To change the length of time, in seconds, that defines the interval over which the event rate will be calculated, use the following command.

Table 299 Event Throttle Interval

Command	Description
cable event throttle-interval <1-3600>	Change the Throttle interval. (Default: 1s)
no cable event throttle-interval	Return the changed Throttle interval to default.

```
Router# configure terminal
Router(config)# cable event throttle-interval 10
Router(config)# end
Router#
```

CM Secure Software Download

System supports upgrading of ONU firmware using the standard mechanisms and interfaces outlined by the DPoE specifications. These specifications closely follow what specified in the DOCSIS 3.0 specifications, but there are some fundamental differences:

- ONU firmware upgrade is a “two-step” process, in which the vCM (residing on the DPoE System) first retrieves the image from the TFTP server and then sends the image to the ONU using DPoE OAM via the OLT.
- The validation of the VCVs embedded within the firmware image is performed by the vCM, not by the physical ONU. CVC validation is not performed if the ONU is provisioned on the EAE Exclusion list.
- The Time Varying Controls associated with the image are updated by the vCM in the ONU as a separate OAM operation.
- Similarly, the image filename is also stored on the ONU by the vCM. If the TVCs or filename cannot be updated, then the entire upgrade operation is deemed to have failed.

To enable or disable Secure Software Download, use the following command.

Table 300 secure software download

Command	Description
cable secure-download (enable disable)	If enabled secure-download, system assumes that the image file contains certificates that need to be extracted and validated before sending the image to the ONU. If disabled, the image is forwarded to the ONU without modification. (Default: Disabled)

```
Router# configure terminal
Router(config)# cable secure-download enable
Router(config)# end
Router#
Router# show cable firmware
MAC Address      IP Address      Op Version      Filename
000d.b640.5868  172.18.200.231 0t A263 (3CBCC658) signed_App3714_DPoE_A263_78.96
Router#
```

MEF-MN Interface

To construct PB/PBB Network over the system, the upstream interface should be included in Service VLAN so as to enable upstream and downstream traffic to flow bothway. The system may designate any particular Interface to be a MEF-MN Interface so that the Interface can be included in Service VLAN automatically. Also the interface can be included into Service VLAN in manual manner.

The system, when an ONU is connected, will bring the vCM Configuration File of the ONU from TFTP server. And the system will create the Service VLAN which is specified in the Configuration File, and assign the MEF-MN Interface to the created Service VLAN automatically.

For the way to include the MEF-MN Interface into Service VLAN manually, refer to “Chapter 3. VLAN” in this manual.

In order to include the MEF-MN Interface into Service VLAN in automatic manner, use the following command.

Table 301 MEF-MN interface

Command	Description
dpoe mef-mn (all <2-4094>)	Designate the VLAN for including MEF-MN Interface.
dpoe mef-mn range VLAN_ID_LIST	Set the range of VLAN for MEF-MN Interface.
no dpoe mef-mn	Make the assigned MEF-MN Interface to be Disabled.

```
Router# configure terminal
Router(config)# interface GigabitEthernet 6/1
Router(config-if-Giga6/1)# dpoe mef-mn all
Router(config-if-Giga6/1)# end
Router#
```

Subscriber's Provider Bridging (PB) Services

This section describes the provisioning of subscriber services supported by system

Provider Bridging Services

This section describes the Provider Bridging (PB) services and related features supported by system. DPoE defines two modes of operation for MEF services: encapsulation mode and transport mode. These modes and related features are described in the sections below.

802.1ad PB Encapsulation Mode

802.1ad PB Encapsulation Mode is a MEF service used to establish a point-to-point L2VPN for a subscriber. For this service, the ONU is responsible for adding and removing an outer SVLAN tag. The DPoE System forwards the SVLAN-tagged frames between the PON and DPoE MN without adding and removing any tags. The following Figure shows the frame formats used for 802.1ad PB encapsulation Mode.

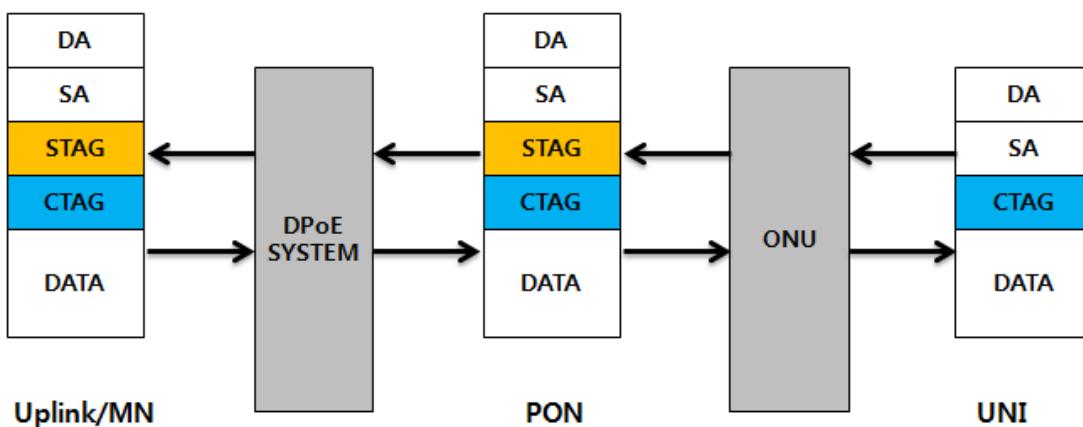


Figure 43 802.1ad PB Encapsulation Mode

For the upstream direction, ONU adds an SVLAN tag to the user frame before transmitting the frame on the PON. DPoE System forwards the frame from the PON out the MN without modifying the frame.

For the downstream direction, DPoE System forwards the SVLAN-tagged frames received from the MN to the PON interface containing the ONU that is terminating the service.

The following Figure shows a CTAGS present in each of the frames. However, System also supports encapsulation of untagged and SVLAN-tagged frames as required by DPoE.

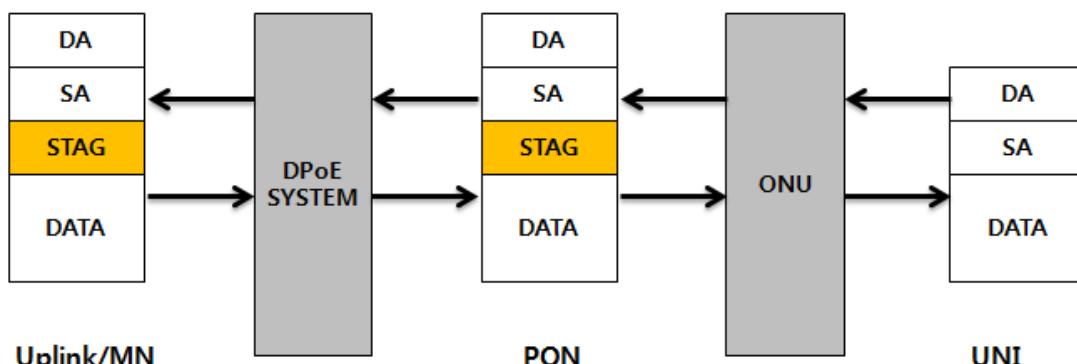


Figure 44 802.1ad PB Encapsulation Mode with Untagged Traffic

If an upstream frame arrives at the ONU UNI with an SVLAN tag, the ONU will add a second SVLAN tag to the frame before forwarding the frame upstream. For this scenario, the DPoE System receives a service frame with two SVLAN tags.

The following example shows how to setup the MEF MN interface and displaying statistics and information for PB services configured for ONUs in system.

```

Router# configure terminal
Router(config)# interface GigabitEthernet 6/1
Router(config-if-Giga6/1)# no shutdown
Router(config-if-Giga6/1)# dpoe mef-mn all
Router(config-if-Giga6/1)# dot1q ethertype 0x8100
Router(config-if-Giga6/1)# end
Router#
Router# show interface cable 3/1 l2-vpn dot1ad
Sfid Dir CM MAC Addr      VLAN ID/ Mode          NNI           CM   Customer Name/
                                         I-SID                               I/F   VPN ID
1     US  0007.7000.0000  100      dot1ad-en        1     PB-EN-S-1
2     DS  0007.7000.0000  100      dot1ad-en        1     PB-EN-S-1

Router#
Router# show interface cable 3/1 l2-vpn dot1ad tpid
Sfid Dir CM MAC Addr      VLAN ID/ Mode          NNI TPID       UNI TPID
                                         I-SID
1     US  0007.7000.0000 100      dot1ad-en      0x88a8      -
2     DS  0007.7000.0000 100      dot1ad-en      0x88a8      -

Router#
Router# show cable modem interfaces
MAC Address      IP Address      I/F Type Service    S-VLAN C-VLAN
                                         /I-SID
0007.7000.0000  10.50.101.198  1 MU    dot1ad-en    100      0

Router#
Router#

```

802.1Q PB Encapsulation Mode

802.1Q PB Encapsulation Mode is an MEF service used to establish a point-to-point L2VPN for a subscriber, and is similar to 802.1ad PB Encapsulation Mode except that the ONU is responsible for adding and removing an outer CVLAN tag.

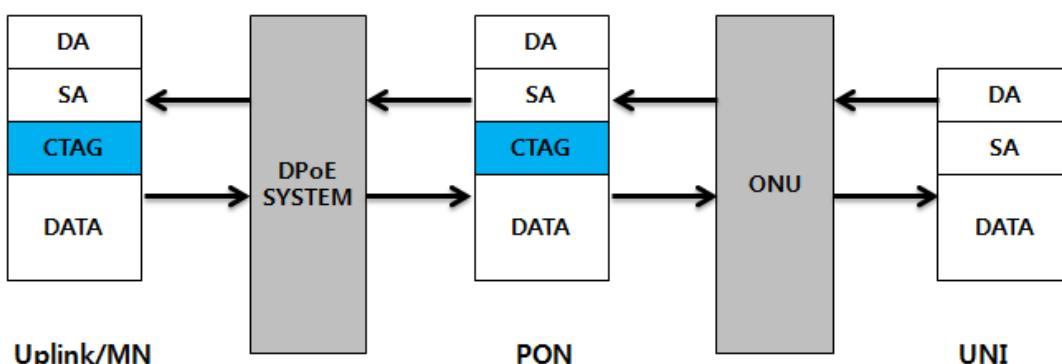


Figure 45 802.1Q PB Encapsulation Mode

For the upstream direction, ONU adds a CVLAN tag to the userframe before transmitting the frame on the PON. System forwards the frame from the PON out the MN without modifying the frame.

For the downstream direction, System forwards the CVLAN-tagged frames received from the MN to the PON interface containing the ONU that is terminating the service. ONU can remove the tag before forwarding the frame out the UNI.

The following example shows how to setup the MEF MN interface and displaying statistics and information for PB services configured for ONUs in system.

```
Router# configure terminal
Router(config)# interface GigabitEthernet 6/1
Router(config-if-Giga6/1)# no shutdown
Router(config-if-Giga6/1)# switchport mode trunk
Router(config-if-Giga6/1)# switchport trunk allowed vlan add 80
Router(config-if-Giga6/1)# end
Router#
Router# show interface cable 3/1 pb
I/F      CM MAC Addr      CM I/F Type Service    S-VLAN C-VLAN
C3/1    0007.7000.0000    1   MU   dot1ad-en     80      0
Router#
```

PB Transport Mode

PB Transport Mode is a MEF subscriber service used to establish a point-to-point L2VPN for a subscriber. For this service, the device attached to the ONU UNI (typically a DPoE DEMARC) is responsible for adding and removing VLAN tags. The ONU and DPoE System simply switch and forwards the VLAN-tagged frames to the correct destination based on the VLAN IDs in the frame. The ONU and DPoE System do not add or remove VLAN tags.

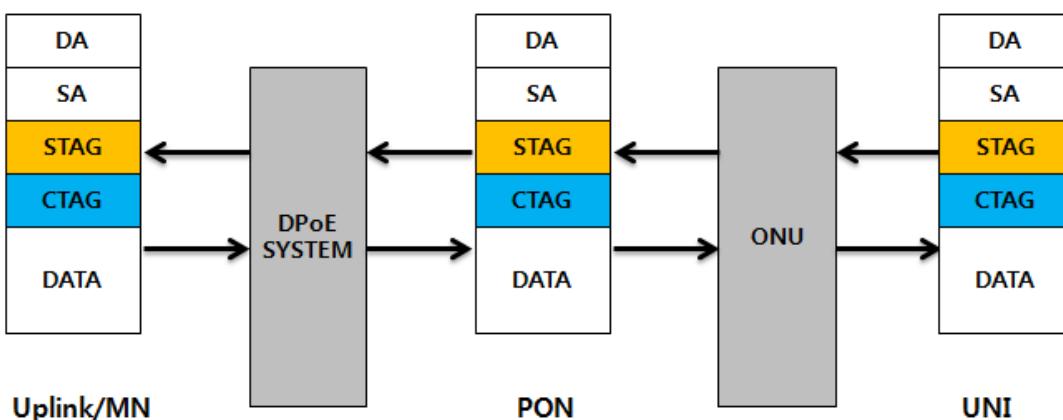


Figure 46 PB Transport Mode

In the upstream direction, ONU classifies traffic received on the UNI to EPON Links (LLIDs) based on the SVID and, if provisioned, the CVID contained in the frame. For Transport Mode configurations, the ONU never adds, removes, or modifies VLAN tags. System forwards the frame from the PON out the MN without modifying the frame.

In the downstream direction, System uses the SVID and, if provisioned, the CVID to switch and forward the VLAN-tagged frames received from the MN to the PON interface containing the ONU that is terminating the service. ONU can forward the frame from the PON to the UNI without modifying the frame.

System also supports Transport Mode for SVLAN-tagged-only frames as required DPoE. The following Figure shows the frame format used for transporting SVLAN-tagged-only frames (single-tagged frames with TPID 88A8). In addition, System supports Transport Mode Configuration for CVLAN-tagged-only frames (single-tagged frames with TPID 8100).

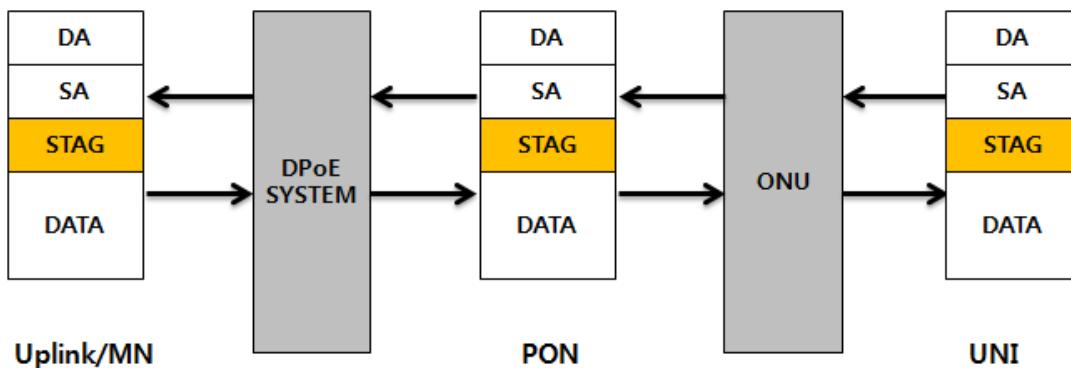


Figure 47 PB Transport Mode with SVLAN Tag Only

The following example shows how to setup the MEF MN interface and displaying statistics and information for PB services configured for ONUs in system.

```

Router# configure terminal
Router(config)# interface GigabitEthernet 6/1
Router(config-if-Giga6/1)# no shutdown
Router(config-if-Giga6/1)# dpoe mef-mn all
Router(config-if-Giga6/1)# end
Router#
Router# show interface cable 3/1 l2-vpn dot1ad
Sfid Dir CM MAC Addr      VLAN ID/ Mode      NNI      CM      Customer Name/
I-SID                                     I/F      VPN ID
1     US   0007.7000.0000  100      dot1ad-tr      1      PB-TR-S-1
2     DS   0007.7000.0000  100      dot1ad-tr      1      PB-TR-S-1

Router#
Router# show interface cable 3/1 l2-vpn dot1ad tpid
Sfid Dir CM MAC Addr      VLAN ID/ Mode      NNI TPID      UNI TPID
I-SID                                     I-SID
1     US   0007.7000.0000 100      dot1ad-tr      0x88a8    0x88a8
2     DS   0007.7000.0000 100      dot1ad-tr      0x88a8    0x88a8

Router#
Router# show cable modem interfaces
MAC Address      IP Address      I/F Type Service      S-VLAN C-VLAN
                                         /I-SID
0007.7000.0000  10.50.101.198   1 MI   dot1ad-tr      100      0

Router#
Router# show cable l2-vpn dot1q-vc-map
MAC Address      Ethernet Intf  VLAN ID Cable Intf  SID  Customer Name/VPN ID
0007.7000.0000  GigE3/1        100      Cable3/1      1      PB-TR-S-1

Router#

```

Subscriber's Provider Backbone Bridging (PBB) Services

This section describes the Provider Backbone Bridging (PBB), otherwise known as “mac-in-mac” services and related features supported by system.

PBB Encapsulation Mode

802.1ah PBB Encapsulation Mode is an MEF service used to establish a point-to-point L2VPN for a subscriber. For this service, the ONU is responsible for adding and removing the entire 902.1ah header, including the backbone destination MAC address (B-DA), backbone source MAC address (B-SA), and the six-byte I-Tag. The DPoE System forwards the 902.1ah encapsulated frames from the PON to the uplink/MN without adding or removing any 802.1ah encapsulation headers. DPoE PBB Encapsulation Mode does not insert or use a backbone VLAN tag (B-Tag).

The following Figure shows the frame formats used for 902.1ah PBB Encapsulation mode.

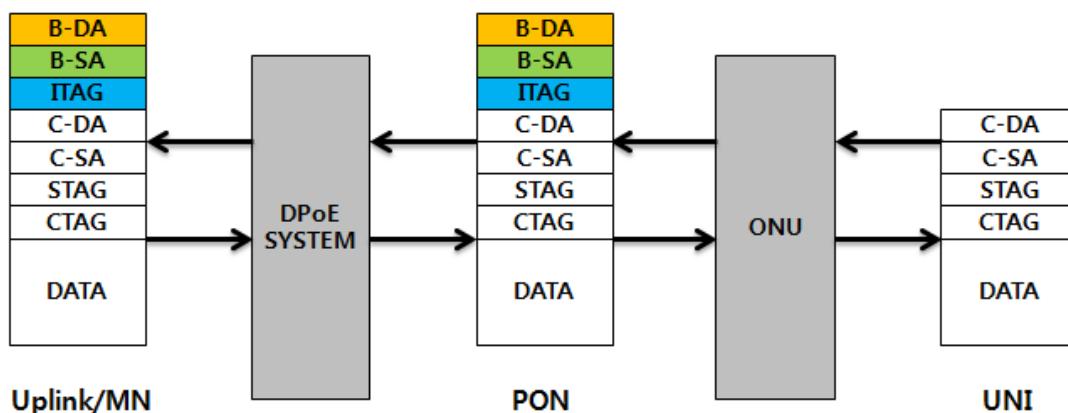


Figure 48 PBB Encapsulation Mode

For the upstream direction, ONU adds a B-DA, B-SA, and I-Tag to the service frame before transmitting the frame on the PON. System forwards the frame from the PON out the MN without modifying the frame.

For the downstream direction, system uses the I-SID to switch and forward the I-Tagged frames received from the MN to the PON interface containing the ONU that is terminating the service. ONU can remove the 802.1ah encapsulation (B-DA, B-SA, and I-Tag) before sending the frame out the UNI.

PBB Transport Mode

802.1ah PBB Transport Mode is an MEF service used to establish a point-to-point L2VPN for a subscriber. For this service, the device attached to the ONU UNI (typically a DPoE DEMARC) is responsible for adding and removing the 802.1ah, “mac-in-mac” encapsulation. The ONU and DPoE System switch and forward the encapsulated frames to the correct destination based on the I-SID in the frame. The ONU and DPoE System are not responsible for adding or removing 802.1ah encapsulation.

The following Figure shows the frame formats used for PBB Transport Mode

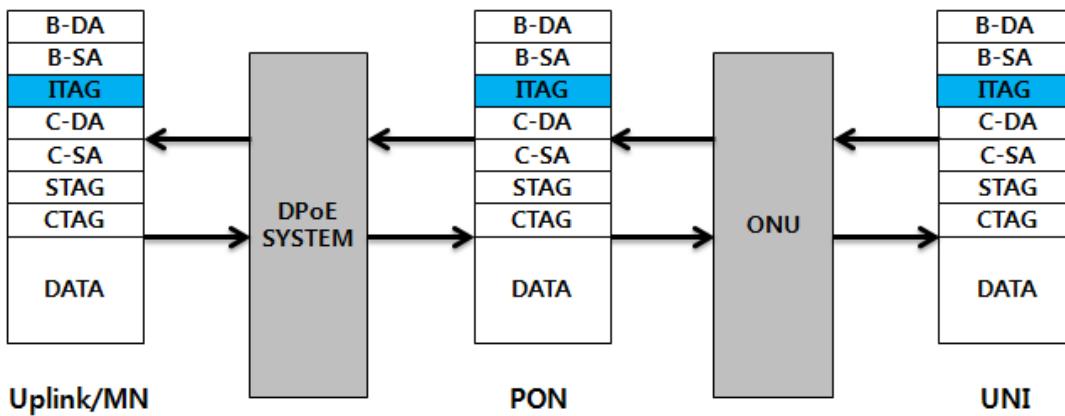


Figure 49 PBB Transport Mode

For the upstream direction, ONU classifies traffic received on the UNI to EPON Links(LLIDs), based on the I-SID contained in the frame. For Transport Mode configurations, the ONU never adds, removes, or modifies the 802.1ah encapsulation header (B-DA, B-SA, I-Tag). System forwards the frame from the PON out the MN without modifying the frame.

For the downstream direction, System uses the I-SID to switch and forward the I-Tagged frames received from the MN to the PON interface containing the ONU that is terminating the service. ONU can forward the frame from the PON to the UNI without modifying the frame.

Unlike PBB Encapsulation Mode, DPoE requires the ONU and DPoE System to forward 802.1ah frames that contain a B-Tag. However, the B-Tag should be “ignored” by the DPoE System and ONU, and the B-Tag should not be used for switching purpose. In DPoE 1.0, the ONU always forwards frames with or without B-Tags.

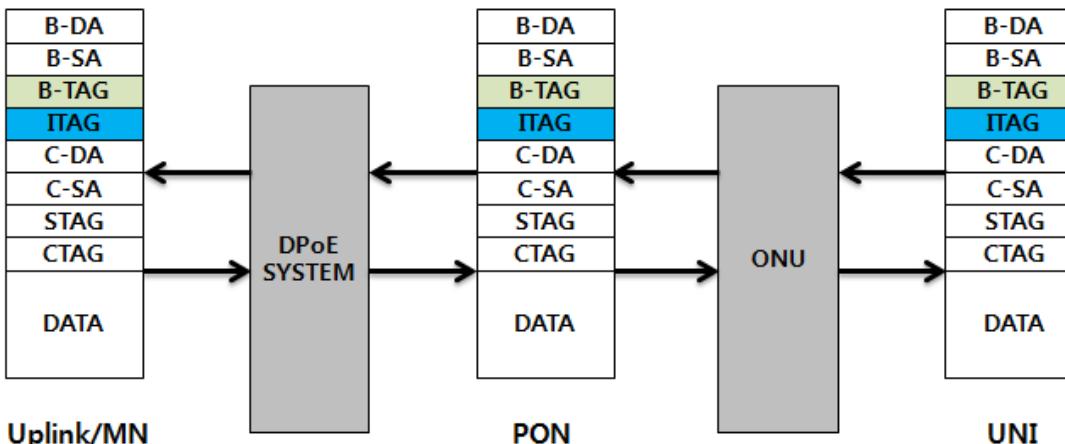


Figure 50 PBB Transport Mode with B-Tags

The following example shows information for PBB services configured for ONUs in system.

```

Router# show interface cable 3/1 I2-vpn dot1ah
Sfid Dir CM MAC Addr      VLAN ID/ Mode          NNI           CM     Customer Name/
                                         I-SID
                                         I/F   VPN ID
1    US  0007.7000.0000  256      dot1ah-tp        1      EPL-1
2    DS  0007.7000.0000  256      dot1ah-tp        1      EPL-1
3    US  0007.7000.0001  65536    dot1ah-en        1      EPL1
4    DS  0007.7000.0001  65536    dot1ah-en        1      EPL1

Router#
Router# show interface cable 3/1 I2-vpn dot1ah bmac
Sfid Dir CM MAC Addr      B-DA          B-SA          I-SID   Mode
1    US  0007.7000.0000  -            0000.0011.1111  256   dot1ah-tp
2    DS  0007.7000.0000  0000.0011.1111 -          256   dot1ah-tp
3    US  0007.7000.0001  0000.5e01.0203 0000.0011.1111  65536  dot1ah-en
4    DS  0007.7000.0001  0000.0011.1111 0000.5e01.0203  65536  dot1ah-en

Router#
Router# show interface cable 3/1 I2-vpn dot1ah tpid
Sfid Dir CM MAC Addr      VLAN ID/ Mode          NNI TPID      UNI TPID
                                         I-SID
1    US  0007.7000.0000  256      dot1ah-tp        0x88e7    0x88e7
2    DS  0007.7000.0000  256      dot1ah-tp        0x88e7    0x88e7
3    US  0007.7000.0001  65536    dot1ah-en        0x88e7    -
4    DS  0007.7000.0001  65536    dot1ah-en        0x88e7    -

Router#
Router#show interface cable 3/1 pbb
I/F      CM MAC Addr      CM I/F Type Service      I-SID
C3/1    0007.7000.0000    1   MI  dot1ah-tp      256
C3/1    0007.7000.0001    1   MU  dot1ah-en      65536

Router#
Router# show cable modem interfaces
MAC Address     IP Address     I/F Type Service      S-VLAN C-VLAN
                                         /I-SID
0007.7000.0000 10.50.101.197  1 MI  dot1ah-tp      256    0
0007.7000.0001 10.50.101.198  1 MU  dot1ah-en      65536   0

```

Router#

IP(HSD) Services

This section describes the IP(HSD) service-related features supported by system. System supports DPoE IP(HSD) and system also supports as defined by DOCSIS, which is referred to as Legacy IP(HSD).

The difference between DPoE IP(HSD) and Legacy IP(HSD) services is that in DPoE IP(HSD) MEF Provider Bridging tags are added to the IP(HSD) frames prior to transmission on the PON. These tags only on the PON, and are not allowed to exit the DPoE System "D" interface or the ONU UNI. In Legacy IP(HSD) mode, no additional tags are added to frames.

DPoE IP(HSD)

In DPoE IP(HSD) mode, MEF PB tags (S+C) are added to IP frames prior to transmission on the PON. The following Figure shows the frame formats used when in DPoE IP(HSD) mode.

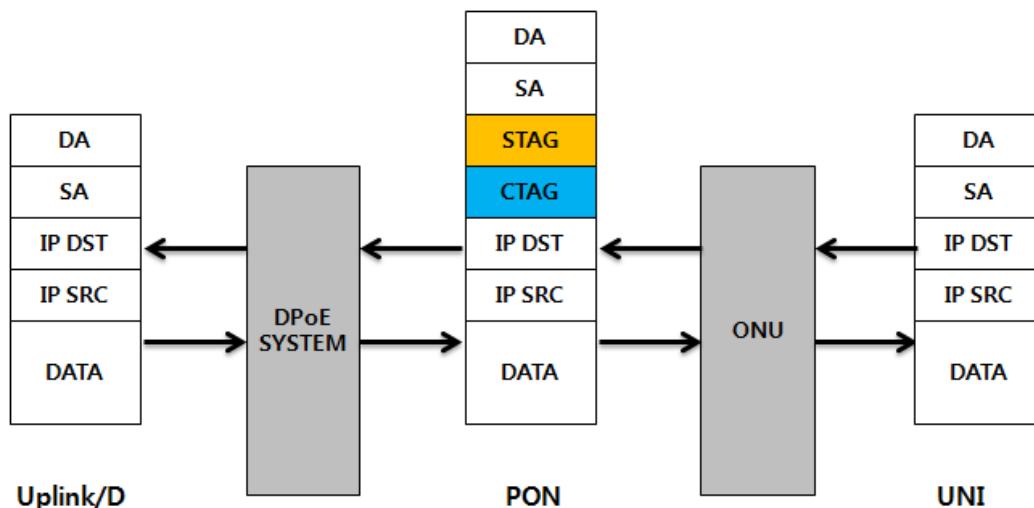


Figure 51 DPoE IP(HSD)

As shown above, tags are added by the ONU and OLT prior to transmission on the PON. Tags are removed before transmitting over the Uplink/D and ONU UNI.

To enable or disable IP(HSD), use the following command.

Table 302 IP(HSD)

Command	Description
iphsd tagging (enable disable)	Specifies the IP(HSD) traffic over the PON interfaces. (Default: Disabled)

```
Router# configure terminal  
Router(config)# iphsd tagging enable  
Router(config)# end  
Router#
```

Serving Groups

The DPoE IP Network Elements specification introduced the concept of an IP Serving Group, or IP-SG. An IP-SG is used to define which S-VID(s) are used for tagging the IP(HSD) traffic going to/from a particular set of ONUs over the PON.

In System, a serving group is assigned to a particular Bundle Interface as a Sub-Interface. Each serving group has a configurable type and can be assigned S-VID. When DPoE IP(HSD) is in use, all IP(HSD) traffic to/from ONUs registering on a “cable interface” or “cable bundle” referencing a serving group of type IP, gets tagged in accordance with the S-VID(s) defined by the serving group.

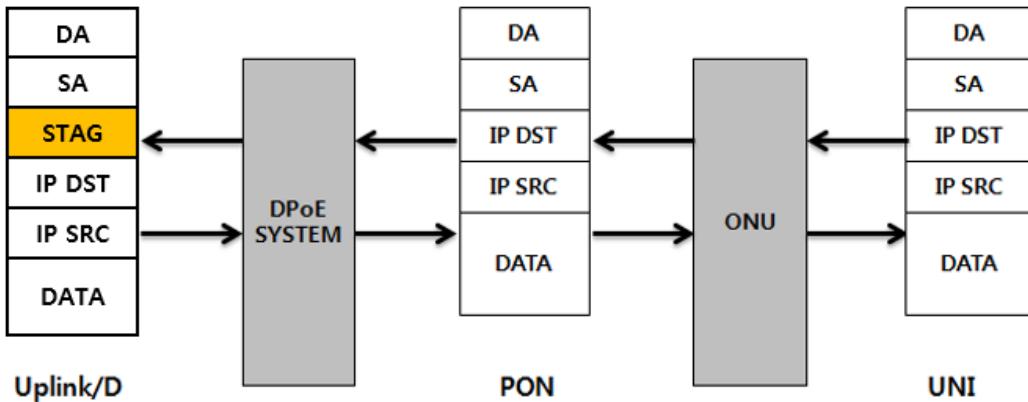


Figure 60 Serving-Group Frame Formats

Legacy IP(HSD)

The Tagging Style can be set so that system does not use DPoE IP(HSD) tagging on the PON. In this case, IP frames traverse the PON without any additional S+C tagging. This is similar to how a DOCSIS CMTS operates today. The following Figure shows the frame formats used when in Legacy IP(HSD) Mode.

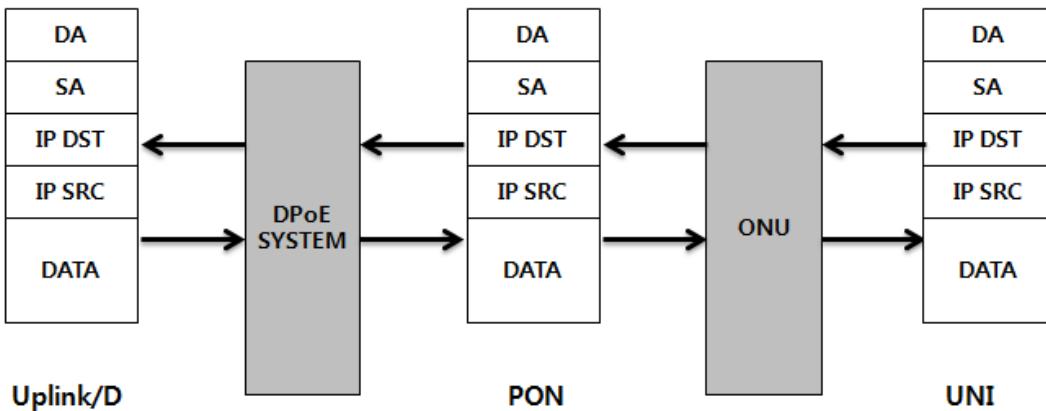


Figure 52 Legacy IP(HSD) Frame Formats

As shown above, no tags are added by the ONU or the DPoE System prior to transmission on the PON. Frames are forwarded based on either L2 or L3 learned address information. The OLT and ONU switch based on the Destination MAC Address. The DPoE System uses IP Destination Address to make its forwarding decisions.

Quality of Service (QoS)

System provides support for DPoE Quality of Service functionality.

Service Flows

A service flow is defined as a DPoE MAC-layer service that provides unidirectional transport of frames. System supports the concept of service flows and uses the EPON Link as the transport mechanism. System maps pairs of upstream and downstream flows to EPON Links and provides support for all required MIBs that provide service flow related information.

DPoE requires support for a subset of the DOCSIS Quality of Service parameters that define service flow scheduling behavior. Typically, these parameters are configured via TLVs in the CM configuration file, but they can also be preconfigured in the DPoE System via Service Classes.

The QoS parameters currently supported by system are listed below. System configures SLAs and Shapers in the OLT and ONU devices using these parameters.

Table 303 QoS parameters

Parameters	Description
Maximum Sustained Traffic Rate	This parameter defines a rate in bits per second that frame transmissions over a service flow cannot exceed. This parameter applies to both upstream and downstream flows.
Maximum Traffic Burst	This parameter defines a limit on the number of “back-to-back” data bytes that can be sent on a service flow at the maximum speed of the underlying media. This parameter applies to both upstream and downstream flows.
Minimum Reserved Traffic Rate	This parameter defines a rate in bits per second that must be guaranteed for frame transmissions over a service flow. This parameter applies to both upstream and downstream flows.
Traffic Priority	This parameter specifies a priority assigned to service flow transmissions and allows a DPoE System to provide differentiated scheduling services based on the value. This parameter applies to both upstream and downstream flows.
Scheduling Type	This parameter specifies a method of upstream scheduling. Although this parameter is more applicable to CMTS Scheduling of RF channels, it is required in DPoE. Only BE and RTP types are required to be supported, but System also supports NRTP. The scheduling types determine which additional QoS parameters need to be specified for upstream service flows. In other words, there are parameter interdependencies that must be enforced. This parameter applies only to upstream flows.
Request/Transmission Policy	This parameter is a bitmap that provides a means to enable or disable various features of a DOCSIS CMTS scheduler. For DPoE, only support for Bit #4 is required. It controls the “force report” behavior of the OLT scheduler. This parameter applies only to upstream flows.
Nominal Polling Interval	This parameter defines how often (in microseconds) an EPON Link is asked to send an MPCP REPORT message advertising how much data it has to send. The DPoE System is not required to implement the Nominal Polling Interval exactly as configured. It may be approximated, as long as the approximated value is displayed in the relevant MIB tables. This parameter applies only to upstream flows.
Maximum Concatenated Burst	This parameter defines how many bytes can be sent upstream on an EPON Link in response to a single MPCP GATE allocation. DPoE requires that this parameter NOT be supported and that it must be

	ignored if configured, which system does by default. This parameter applies only to upstream flows.
IP TOS Overwrite	This parameter defines a masking capability that allows modification of the IPv4 TOS field of frames passing through a service flow. This parameter applies to upstream and downstream flows.

QoS parameters can be configured via Service Classes. A Service Class is a set of service flow parameters that are preconfigured in the system. A CM configuration file can reference a Service Class via TLV in a service flow encoding, and these Service Class parameters will be used in the absence of explicit TLVs.

To create a Service Class Table, use the following command.

Table 304 Service Class Table

Command	Description
cable service-class downstream class-index WORD no cable service-class downstream class-index WORD	Creates or Removes Service Class Table for downstream
cable service-class upstream class-index WORD no cable service-class upstream class-index WORD	Creates or Removes Service Class Table for upstream

To configure parameters of Service Class, use the following command in the config-cable-service command node.

Table 305 parameters of Service Class Table

Command	Description
max-burst <1522-4294967295> no max-burst	Specifies the value for Maximum Transmit Burst, in units of bytes. (Default: 3200)
max-concat-burst (<1-65535> unlimit) no max-concat-burst	Specifies the value for Maximum Concatenated Burst, in units of bytes. (Default: 1600)
max-rate <1-4294967295> no max-rate	Specifies the value for Maximum Sustained Traffic Rate, in bits per second. (Default: 0)
min-rate <1-4294967295> no min-rate	Specifies the value for Minimum Reserved Traffic Rate, in bits per second. (Default: 0)
poll-interval <1-4294967295> no poll-interval	Specifies the value for Nominal Polling Interval, in units of microseconds. (Default: 0)
priority <1-7> no priority	Specifies the value for Traffic Priority. (Default: 0)
req-trans-policy HEXA-DECIMAL no req-trans-policy	Specifies the value for Request/Transmission Policy. There is no enforced range for this parameter, but this parameter is a bitmap and only Bit #4 has meaning in DPoE. (By default, all bits in this bitmap are set to 0)
sched-type (be nrtp rtp ugsad ugs) no sched-type	Specifies the value for Scheduling Type. - BE: Best Effort - NRTP: Non-Real-Time Polling - RTP: Real-Time Polling - UGS: Unsolicited Grant Service - UGSAD: Unsolicited Grant Service with Activity Detection (Default: BE)
tos-overwrite (and-mask or-mask) HEXA-DECIMAL no tos-overwrite (and-mask or-mask)	Specifies the value for the "And Mask" or "Or Mask" portion of the IP TOS Overwrite

	field. There is no enforced range for this parameter. The default value for "And Mask" is 255, which means IP TOS will not be overwritten if "Or Mask" is also set to its default value. The default value for "Or Mask" is 0, which means IP TOS will not be overwritten if "And Mask" is also set to its default value.
req-attr-mask HEXAVALUE no req-attr-mask	Specifies the 32bit attribute-mask value of TLV24/25.31 for IP Serving-Group

```

Router# configure terminal
Router(config)# cable service-class upstream class-index Upstream_RTP
Router(config-cable-service-upstream,Upstream_RTP)# max-burst 16000
Router(config-cable-service-upstream,Upstream_RTP)# max-rate 1000000
Router(config-cable-service-upstream,Upstream_RTP)# sched-type rtp
Router(config-cable-service-upstream,Upstream_RTP)# poll-interval 5000
Router(config-cable-service-upstream,Upstream_RTP)# end
Router#
Router# show cable service-class
Index Name Dir Sched Prio MaxSusRate MaxBurst MinRsvRate
1 Upstream_RTP US BE 0 0 3200 0
Router#

```

```

Router# show cable modem
MAC Address IP Address I/F MAC Prim RxPwr Timing Num BPI
              State Sid (db) Offset CPEs Enb
0007.70e8.f48c 10.50.101.186 C2/1 online 1 0.0 62 0 N
Router#
Router# show cable modem 0007.70e8.f48c qos
Sfid Dir Curr Sid Sched Prio MaxSusRate MaxBrst MinRsvRate Throughput
              State Type
1 US act 1 BE 7 0 12800 0 374
2 DS act N/A UNDEF 7 0 12800 0 15613

```

```

Router#
Router# show cable modem 0007.70e8.f48c qos verbose

Sfid : 1
Current State : Active
Sid : 1
Traffic Priority : 7
Maximum Sustained rate : 0 bits/sec
Maximum Burst : 12800 bytes
Minimum Reserved rate : 0 bits/sec
Minimum Packet Size : 0 bytes
Admitted QoS Timeout : 200 seconds
Active QoS Timeout : 0 seconds
Maximum Concatenated Burst : 0 bytes
Scheduling Type : Best Effort
Request/Transmission policy : 0x00
IP ToS Overwrite[AND-mask, OR-mask] : 0xff,0x00
Current Throughput : 373 bits/sec, 5 packets/sec

Sfid : 2
Current State : Active
Sid : N/A
Traffic Priority : 7

```

Maximum Sustained rate	: 0 bits/sec
Maximum Burst	: 12800 bytes
Minimum Reserved rate	: 0 bits/sec
Minimum Packet Size	: 0 bytes
Admitted QoS Timeout	: 200 seconds
Active QoS Timeout	: 0 seconds
Maximum Concatenated Burst	: 0 bytes
Scheduling Type	: Undefined
Request/Transmission policy	: 0x00
IP ToS Overwrite[AND-mask, OR-mask]	: 0xff,0x00
Current Throughput	: 15594 bits/sec, 10 packets/sec

Router#

Router# **show interface cable 2/1 service-flow**

Sfid	Sid	Mac Address	QoS	Param Index	Type	Dir	Curr	Active	BG / CH	
									State	Time
1	1	0007.70e8.f48c 0	0	0	prim	US	act	0h43m	N/A	
2	N/A	0007.70e8.f48c 0	0	0	prim	DS	act	0h43m	N/A	

Router#

Statistics per Service Flow

The following real-time statistics are available for the service-flows being provisioned as the CM becomes ONLINE.

Command	Description
dpoe service-flow counter (enable disable)	Enables the service-flow counter (Default: Enabled)
dpoe service-flow counter interval <60-600>	Specifies the retrieving interval of service-flow counter (Default: 300s)

Router# **show cable modem 0024.4503.77c8 service-flow counter**

Sfid	Packets	Bytes	FCS Errors	Bits/Sec	Bytes/Sec
1	388	68676	0	40	5
2	388	79540	0	48	6
3	0	0	0	0	0
4	0	0	0	0	0
5	0	0	0	0	0

Router#

Router# **show cable modem 0024.4503.77c8 service-flow counter detail**

Service-Flow 01 (Upstream)

Frames	:	388
Bytes	:	68676
MulticastFrames	:	0
BroadcastFrames	:	0
UnicastFrames	:	388
64ByteFrames	:	194
65To127ByteFrames	:	0
128To255ByteFrames	:	0
256To511ByteFrames	:	194
512To1023ByteFrames	:	0
1024To1518ByteFrames	:	0
1519BytePlusFrames	:	0
FcsErrors	:	0

Service-Flow 02 (Downstream)

Frames	:	388
Bytes	:	79540

MulticastFrames	:	0
BroadcastFrames	:	0
UnicastFrames	:	388
64ByteFrames	:	194
65To127ByteFrames	:	0
128To255ByteFrames	:	0
256To511ByteFrames	:	194
512To1023ByteFrames	:	0
1024To1518ByteFrames	:	0
1519BytePlusFrames	:	0
FcsErrors	:	0
 Service-Flow 03 (Downstream)		
Frames	:	0
Bytes	:	0
MulticastFrames	:	0
BroadcastFrames	:	0
UnicastFrames	:	0
64ByteFrames	:	0
65To127ByteFrames	:	0
128To255ByteFrames	:	0
256To511ByteFrames	:	0
512To1023ByteFrames	:	0
1024To1518ByteFrames	:	0
1519BytePlusFrames	:	0
FcsErrors	:	0
 Service-Flow 04 (Downstream)		
Frames	:	0
Bytes	:	0
MulticastFrames	:	0
BroadcastFrames	:	0
UnicastFrames	:	0
64ByteFrames	:	0
65To127ByteFrames	:	0
128To255ByteFrames	:	0
256To511ByteFrames	:	0
512To1023ByteFrames	:	0
1024To1518ByteFrames	:	0
1519BytePlusFrames	:	0
FcsErrors	:	0
 Service-Flow 05 (Downstream)		
Frames	:	0
Bytes	:	0
MulticastFrames	:	0
BroadcastFrames	:	0
UnicastFrames	:	0
64ByteFrames	:	0
65To127ByteFrames	:	0
128To255ByteFrames	:	0
256To511ByteFrames	:	0
512To1023ByteFrames	:	0
1024To1518ByteFrames	:	0
1519BytePlusFrames	:	0
FcsErrors	:	0

Router#

Classifiers

System provides support for required DPoE Classification functionality.

Downstream

Down classifiers are used to match frames coming from the northbound interface of a DPoE System, and determine which service flows (and therefore which EPON Links) they should be sent on to traverse the PON and arrive at a particular ONU.

Downstream classifiers are configured via the CM configuration file, using TLV-23. System creates classification rules based on these TLV settings and communicates them to the OLT which services the ONU.

Upstream

Upstream classifiers match frames coming into the UNI interfaces of a DPoE ONU and determine which service flows (and therefore which EPON Links) they should be sent on to traverse the PON and arrive at the DPoE System.

Upstream classifiers are configured via the CM configuration file, using TLV-22. System creates classification rules based on these TLV settings and communicates them to the OLT that services the ONU. In turn, the OLT sends DPoE OAM to configure the ONU as appropriate.

Upstream Drop Classifiers

Upstream Drop classifiers match frames coming into the UNI interfaces of a DPoE ONU and determine whether they should be dropped. They are packet filters, implemented in the ONU so that frames are dropped prior to traversing the PON.

Upstream Drop classifiers are configured via the CM configuration file, using TLV-60 or TLV-62. System creates filter rules based on these TLV settings and communicates them to the OLT that services the ONU. In turn, the OLT sends DPoE OAM to configure the ONU as appropriate.

To enable the Upstream Drop Classifier, use the following command.

Table 306 parameters of IP(HSD) Serving Group Table

Command	Description
cable privacy udc-policy (enable disable)	Enable Upstream Drop Classifier on the specified cable interface. (default: Disabled)

```
Router# configure terminal
Router(config)# int EponInterface 2/1
Router(config-if-Epon2/1)# cable privacy udc-policy enable
Router(config-if-Epon2/1)# end
Router#
Router#
Router# show interface cable 2/1 service-flow
Sfid Sid Mac Address QoS Param Index Type Dir Curr Active BG / CH
          Prov Adm Act
          State Time
1      1    0007.70e8.f48c 0    0    0 prim   US act   0h33m N/A
2      N/A  0007.70e8.f48c 0    0    0 prim   DS act   0h33m N/A

Router#
Router# show interface cable 2/1 service-flow 1 verbose
Sfid : 1
```

MAC Address	: 0007.70e8.f48c
Type	: Primary
Direction	: Upstream
Current State	: Active
Current QoS Indexes [Prov, Adm, Act] : [0,0,0]	
Active Time	: 0h33m
Sid	: 1
Admitted QoS Timeout	: 200 seconds
Active QoS Timeout	: 0 seconds
Packets	: 4904358
Bytes	: 349481904
Rate Limit Delayed Packets	: 0
Rate Limit Dropped Packets	: 0
Current Throughput	: 1388899 bits/sec, 2436 packets/sec
Classifiers:	

Router#

DPoEv2.0 Multicast

System provides support for required DPoEv2.0 Multicast functionality.

Multicast Operation

The DPoEv2.0 Specifications support IP multicast for IP(HSD) services by adopting the IP multicast model defined in [MULPlv3.0]. This model supports the delivery of Any Source Multicast (ASM) and Source-Specific Multicast (SSM) IP multicast streams to D-ONUs. As defined in [MULPlv3.0], the D-ONU is not aware of IP multicast control protocols. In DPoE specifications, the D-ONU does not proxy or snoop to track Layer-3 IP multicast group membership. Instead, all of the processing and management functionality related to multicast group membership is at the DPoE System.

System supports the provisioning and operation of IP multicast for IP(HSD) as defined in [MULPlv3.0], and this includes:

- Support for forwarding Source Specific Multicast traffic for IGMPv3 [RFC 3376] and MLDv2 [RFC 3810] CPE devices
- Support for forwarding Any Source Multicast traffic for IGMPv1/v2 and MLDv1 CPE devices
- Support for downstream multicast QoS
- Support for static multicast
- Support for downstream encrypted multicast
- Support for IPv4 and IPv6 multicast traffic
- Explicit tracking at the DPoE System of CPEs joined to a given multicast group

The following exceptions and differences from [MULPlv3.0] for support of IP multicast apply to this version of DPoE specifications:

- Upstream multicast is not defined in this version of the DPoE specification but the forwarding of upstream multicast traffic is not actively prevented. There is no upstream support defined for functionality such as multicast QoS or upstream multicast encryption.
- Pre-Registration IP multicast is not supported.
- Downstream Service ID (DSID) defined in [MULPlv3.0] is replaced with a multicast LLID (mLLID).

Single Session vs Aggregate Session

Single Session is that one channel is forwarded by one Multicast LLID, and each channel must belong to Multicast Service Profile. In short, the Multicast LLID is assigned to each channel.

Aggregate Session is that multiple channels are forwarded by one multicast LLID. The traffic of channels that do not match Multicast Service Profile is forwarded through the Broadcast Domain.

Multicast QoS

To perform DPoEv2.0 Multicast in 10G Line-Card, Downstream Service-Class, Group-QoS-Config (GQC) and Group-Config (GC) should be defined in advance.

To specify a Group-QoS-Config, use this command.

Command	Description
cable multicast group-qos default scn SCN-NAME aggregate (session-limit <1-1000>)	Specifies the default aggregate session for GQC
no cable multicast group-qos default scn SCN-NAME aggregate	Removes the specified default aggregate session for GQC
cable multicast group-qos GQC-ID scn SCN-NAME single	Specifies the single session for GQC. GQC-ID is used for identifying Group-Config (GC).
no cable multicast group-qos GQC-ID scn SCN-NAME single	Removes the specified single session for GQC

```

Router# configure terminal
Router(config)# cable multicast group-qos default scn MDEFAULT aggregate
Router(config)# cable multicast group-qos 10 scn MSINGLE single

```

To create a Group-Config (GC), use this command.

Command	Description
cable multicast qos group <1-255>	Creates the Group-Config profile
no cable multicast qos group <1-255>	Removes the Group-Config profile
session-range A.B.C.D A.B.C.D	Specifies the session range to Group-Config
group-qos <1-255>	Specifies the GQC-ID to Group-Config

```

Router# configure terminal
Router(config)# cable multicast qos group 1
Router(config-mqos-1)# session-range 231.1.1.0 255.255.255.0
Router(config-mqos-1)# group-qos 10
Router(config-mqos-1)# end
Router#

```

To associate Group-Config into forwarding cable interface, use this command.

Command	Description
cable multicast-qos group <1-255>	Specifies the GC-ID for multicast QoS
no cable multicast-qos group <1-255>	Removes the multicast QoS

```

Router# configure terminal
Router(config)# interface TponInterface 1/1
Router(config-if-Tpon1/1)# cable multicast-qos group 1
Router(config-if-Tpon1/1)# end
Router#
Router# show cable modem 0024.4504.812e multicast
Group address      CPE IP Address CPE Mac Address      Uptime      Exptime    GQC-ID GC-ID
Router#
Router# show cable multicast 10/1 db
Group address      CPE IP Address CPE Mac Address CM Mac Address      Uptime      Exptime    Mode LLID
Router#
Router# show cable multicast 10/1 dsid
Session      LLID      Ch #          Total bytes      Current Kbps
-----
Router#

```

Rate setting for PON interface port

PIM-8XE card which takes care of 10Gbps transmission rate for subscriber side communication in DPoE the C9500 series is able to support different rate combinations unlike PIM-8EB which supports only 1Gbps rate.



Notice

PIM-8EB supports only the transmission rate of 1Gbps/1Gbps (downstream/upstream)

Available rates for PIM-8XE

Depending on the factors like what kind of optic modules are used in OLT and ONU and whether OLT is configured for Turbo mode or not, transmission speed will be determined.

Table 307 Transmission rates of DPoE the C9500 series PON segment

Optic module in OLT	Optic module in ONU	OLT configuration	Transmission rates (downstream/upstream)
Turbo Optics	Turbo optic	Turbo mode	2Gbps/1Gbps
	1GE optic		Not supported
	Turbo optic	None	1Gbps/1Gbps
	1GE optic		1Gbps/1Gbps
10/10/1 Coexistence Optics	1GE optic	None	1Gbps/1Gbps
	10/1 optic		10Gbps/1Gbps
	10/10 optic		10Gbps/10Gbps
10/10/1 Coexistence Optics	Turbo optic	Turbo mode	2Gbps/1Gbps
	10/1 optic		10Gbps/1Gbps
	10/10 optic		10Gbps/10Gbps

Setting for Turbo PON mode

OLT Configuration has two modes of Turbo mode and None mode. When OLT is configured to be Turbo mode and the optic modules in both OLT and ONU are Turbo optic modules, the outcome speed will be 2Gbps/1Gbps which is expected as Turbo mode operation.

1) CLI sequence for Turbo PON mode setting

```
Switch[A/L](config-if-Tpon2/1)#shutdown  
Switch[A/L](config-if-Tpon2/1)#pon speed 2Gbps  
Switch[A/L](config-if-Tpon2/1)#no shutdown
```

...

2) CLI sequence to release from Turbo PON mode (Returning to None mode)

```
Switch[A/L](config-if-Tpon2/1)#shutdown  
Switch[A/L](config-if-Tpon2/1)#no pon speed 2Gbps  
Switch[A/L](config-if-Tpon2/1)#no shutdown
```

...

Chapter 24. ***Netflow***

Netflow Overview

Introduction to Netflow

Netflow is a feature that collects and distributes data about the amount and duration of network traffic per network application (e.g., ftp, http, IPTV).

Netflow can serve the following purposes:

- Network Monitoring
 - Distribute data about traffic passing through switches or routers in near real time.
 - Provide data feeds to visualization applications. These applications would be able to clearly communicate traffic patterns in the form of graphs and tables to users.
- Application Monitoring and Profiling
 - List changes in the use of network resources for each network application in chronological order.
 - This data could be beneficial for planning new services, allocating network resources (e.g., switches or routers) and application resources (e.g., web servers) to meet user demands.
- User Monitoring and Profiling
 - Obtain information about the preferred networks and resources of (selected) users.
 - Apart from commercial purposes, this information could also strengthen defense against potential security threats.
- Network Planning
 - Collect long-term data about network traffic to trace and predict network growth.
 - This data could determine the most effective network infrastructure upgrade (e.g., number or performance of routers/ports/interfaces).
- Accounting/Billing
 - Gather statistics for IP, TCP/UDP ports, bytes, and packets.
 - Internet service providers (ISPs) could impose surcharges based on statistics about bandwidth/daily/application usage.

Netflow Deployment

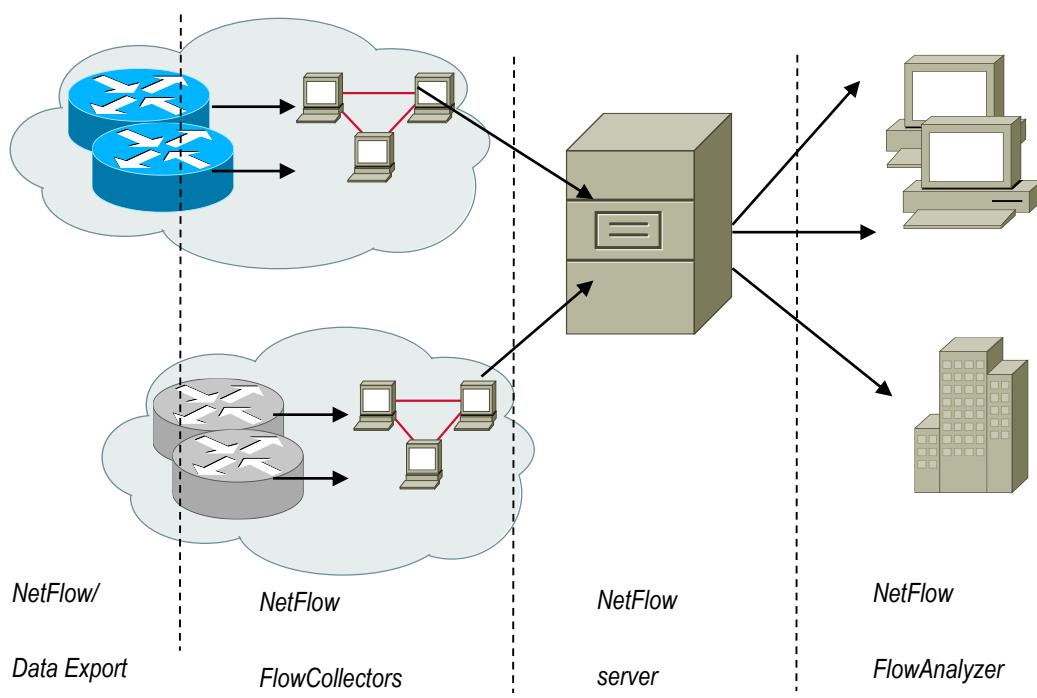


Figure 53 Netflow Deployment

End-user Apps

A netflow setup consists of the following:

- Netflow exporter (*Netflow Data Export* in Figure 1)
 - Collects netflow data and sends this data to the collector.
 - Routers usually assume this role; however, you can also use network application servers.
- Netflow collector (*Netflow Flow Collectors* and *Netflow Server* in Figure 1)
 - Receives the netflow data and stores it on a physical storage device or sends it to another collector or netflow analyzer.
- Netflow analyzer
 - Processes the stored data for user legibility.

Netflow Flow

A flow (or IP flow) is the collection of groups of IP packets for fixed time periods. A flow consists of packet components such as IP and UDP/TCP ports; IP packets from the same flow have the same components. The netflow exporter creates/removes/checks flows to monitor netflow data, and sends this data to the netflow collector.

Flows that have been created by the netflow exporter can be removed; removed flows are sent to the netflow collector. The netflow exporter removes flows under the following circumstances:

- When the exporter detects that the flow has finished (when no more packets are to be collected from the flow).
 - For example, if a TCP packet contains the FIN or RST flag, the exporter determines that the TCP connection has closed and that the corresponding flow has finished. This flow will be removed.
- When the flow remains inactive for a certain period of time (when packets have not been collected from the flow)
- When the flow continues for longer than it should (when packets continue to be collected from the same flow)
- When the netflow exporter cannot maintain flows.
 - For example, if the netflow exporter lacks system memory or the counter (that counts bytes or packets) reaches its limit.

Netflow Packets

Depending on the netflow version, netflow data is sent from the netflow exporter to the netflow collector in different packet formats. This section discusses the packet format for netflow version 5 on U9500.

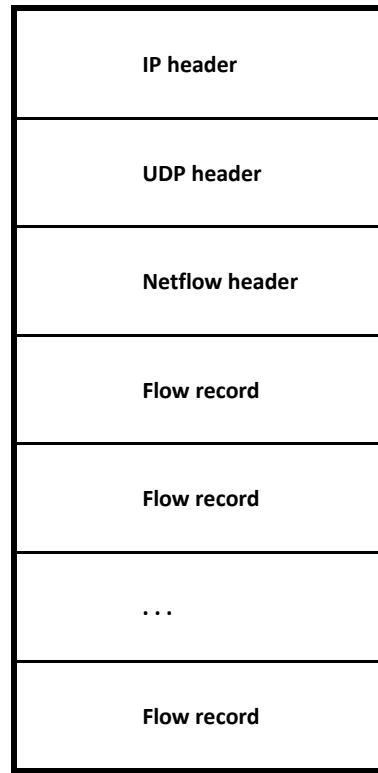


Figure 54 Netflow V5 Packet Format

Netflow version 5 sends data using the User Datagram Protocol (UDP). The packet format consists of a header field followed by the flow (flow record), that is to be sent to the netflow collector. Flow records carry the following information.

- Source IP
- Destination IP
- Next hop IP
- SNMP interface index that receives the flow
- SNMP interface index that sends the flow
- Number of accumulated packets in the flow
- Number of accumulated bytes in the flow
- Amount of time taken to create the flow
- The point in time at which the last packet was received from the flow
- TCP/UDP source port
- TCP/UDP destination port
- TCP flag
- IP Protocol type
- IP Type Of Service (TOS)
- Source AS number
- Destination AS number
- Source address prefix mask bits
- Destination address prefix mask bits

U9500 Netflow

Requirements and Characteristics

The netflow feature of U9500 becomes available once you have installed the netflow processing engine (NP). The NP does not affect router performance and is separated from U9500's Routing Engine (PFE). Therefore, enabling the netflow feature will not drop a packet that needs to be routed.

Creating Flows

The NP uses the PFE to collect routed packets, and categorizes these packets into flows, and then stores these flows in a flow table. U9500's netflow feature categorizes packets according to the following criteria:

- Source IP
- Destination IP
- source PORT
- Destination PORT
- Protocol field of the IP header

These are called the key fields; packets with the same key fields are categorized into the same flow. U9500's netflow feature supports UDP/TCP/ICMP/U9500 as transport layer protocols. ICMP uses ICMP types instead of source/destination ports to differentiate between flows; UDP and TCP differentiate between flows without using ports.

Removing Flows

The NP periodically checks the flow table for flows to be removed. Removed flows can be sent to the netflow collector; if a netflow collector does not exist, the removed flow is immediately purged. The NP purges flows under the following circumstances:

- When the long aging time has expired
 - The long aging time is the maximum amount of time that a flow can be stored in the flow table.
- When the normal aging time has expired
 - The normal aging time is the maximum amount of time that a flow can be stored in the flow table without being updated (when the NP can no longer collect packets from the flow).
- When a TCP connection is broken (for TCP flows)
- When the accumulated number of bytes from the flow has exceeded 2G.



Notice

The Octet of netflow version 5 packets is 4 bytes; the largest value that can be expressed for an integer is 4 gigabytes. Therefore, a flow needs to be removed before it accumulates more than 4 gigabytes.

Restrictions

U9500's Netflow feature is restricted as follows:

- Only packets that have been routed using the PFE can be collected.
- Only IPv4 packets can be collected.
- Packets that are sent from the flow cannot be collected.

- The netflow collector only supports the netflow version 5 protocol when sending data.
- The port mirroring feature is not available for use when the netflow feature has been enabled.

U9500 Default Netflow Settings

Table 308 Default Netflow Settings

Item	Default
Collects statistical data about IP traffic routed by the PFE	Disabled
Sampled Netflow	1 Gigabit module: Disabled
	10 Gigabit module : 1/30
Sends statistical data to the netflow collector	Disabled

Commands for Collecting Statistical Data about Netflow Traffic

Configuring the Settings for Collecting Statistical Data about Netflow Traffic

Table 309 Commands for Setting Statistical Data Collection

Command	Description
mls netflow	Collects statistical data about IP traffic.
ip flow ingress	Collects statistical data about IP packets that are received from the flow
mls aging	Sets the aging out time for the flow
flow-sampler module	Sets the sampling rate for each module

Enabling/Disabling the Collection of Statistical Data for Netflow Traffic

Table 310 Commands for Setting the Collection of Statistical Data

Command	Description
Router(config)# mls netflow	Enables the collection of statistical data of IP traffic
Router(config)# no mls netflow	Disables the collection of statistical data of IP traffic
Router(config-if-<interface>)# ip flow ingress	Enables the collection of statistical data of IP traffic from an interface
Router(config-if-<interface>)# no ip flow ingress	Disables the collection of statistical data of IP traffic from an interface

To collect statistical data about IP traffic on U9500:

- Use the **mls netflow** command to enable the netflow feature
- Use the **ip flow ingress** command in an ingress interface to enable the NP to view packets that are received, from the interface.

Since statistical data can only be collected for packets that are routed by the PFE, the **ip flow ingress command** must only be used in an interface that has an IP configured.

Setting the Flow Aging Out Time

Flows should be purged to prevent flows from increasing beyond management and accumulating values beyond expression of the NP. Purged flows can be sent to the netflow collector and can be removed from the NP. The aging out time determines when a flow is to be purged. There are two types of aging out times.

Table 311 Commands for Setting Flow Aging Out Time

Type	Description
Normal	A flow is purged if the NP fails to collect a packet from a flow

	within the normal aging out time.
Long	A flow is purged if a flow remains in the NP for longer than the long aging out time.

The long aging out time has priority over the normal aging out time. A flow will be purged if it has exceeded the long aging out time, but not the normal aging out time.

The following commands set the aging out times.

Table 312 Commands for Setting Aging Out Time

Command	Description
Router(config)# mls aging {long 64-1920 normal 32-4092}	Sets the aging out time of a flow Default for long aging out time: 1920 seconds Default for normal aging out time: 600 seconds
Router(config)# no mls aging {long normal}	Reverts the aging out time of a flow to the default.

Due to performance issues of the NP, a time lag can exist between the point in time that a flow has aged out and the point in time that the NP actually purges the flow. This time lag amounts to a maximum of 10 seconds.

The following commands display the times set for aging out.

Table 313 Commands for Displaying Aging Out Time

Command	Description
Router# show mls netflow aging	Displays the aging out time of the flow

Router# show mls netflow aging			
	enable	timeout	packet threshold
normal aging	true	600	N/A
long aging	true	1920	N/A

Setting the Maximum Number of Flows

The maximum number of flows that can be stored in the NP is limited. You can set the number of flows to be created - the corresponding packets that were collected by the NP will be deleted immediately.

Table 314 Commands for Setting Maximum Number of Flows

Command	Description
Router(config) # mls netflow maximum-flows <1024- 65536 >	Sets the maximum number of flows The default is 524288.
Router(config) # no mls netflow maximum-flows	Reverts the maximum number of flows to the default.

Commands for Viewing Statistical Data about Netflow Traffic

Viewing Statistical Data about Netflow Traffic

Table 315 Commands for Viewing Statistical Data of Netflow Traffic

Command	Description
show mls netflow ip	Displays flows
show mls netflow ip count	Displays the number of flows
clear mls netflow ip	Immediately purges flows

Commands for Viewing Flows

Table 316 Commands for Viewing Flows

Command	Description
show mls netflow ip [detail/] [nowrap] [LINE]	Displays flows in the NP that have not been purged. The following information is displayed: <ul style="list-style-type: none">● Output interface (SNMP interface index)● Source/destination AS number● Next hop address● Source/destination MASK● TCP FIN/RST flag nowrap: Does not display the information with new lines. LINE: If bpf filter syntax (used in bpf filter and tcpdump) is used, only the flows that match the filter are displayed (for further information about bpf filter syntax, please refer to the <i>tcpdumpfilter Manual.</i>).
show mls netflow ip [detail/] [nowrap] [LINE]	Displays the number of flows that have not been purged in the NP. LINE: If bpf filter syntax (used in bpf filter and tcpdump) is used, only the flows that match the filter are displayed (for further information about bpf filter syntax, please refer to the <i>tcpdumpfilter Manual.</i>).

The following example displays information about 5 flows.

```
Router# show mls netflow ip
DstIP          SrcIP          Prot:SrcPort:DstPort   Src i/f
-----:-----:-----:-----
Pkts          Bytes          Age    LastSeen
-----
20.2.1.2      10.2.1.2      udp :1000  :1003    1101
920752        47879104     63     2010-02-08T14:08:11
20.2.1.2      10.2.1.2      udp :1000  :1004    1101
```

921432	47914464	63	2010-02-08T14:08:11			
20.2.1.2	10.2.1.2	udp :1000	:1005	1101		
921957	47941764	63	2010-02-08T14:08:11			
20.2.1.2	10.2.1.2	udp :1000	:1006	1101		
922770	47984040	63	2010-02-08T14:08:12			
20.2.1.2	10.2.1.2	udp :1000	:1007	1101		
923127	48002604	63	2010-02-08T14:08:12			

Router# show mls netflow ip detail							
DstIP	SrcIP	Prot:SrcPort:DstPort			Src i/f		
-----	-----	-----	-----	-----	-----	-----	-----
Pkts	Bytes	Age	LastSeen				
-----	-----	-----	-----	-----	-----	-----	-----
Out i/f	Src AS Dst AS Nh Addr			Src Mask Dst Mask FIN/RST			
-----+-----+-----+-----+-----+-----+	-----+-----+-----+-----+-----+-----+			-----+-----+-----+-----+-----+-----+			
20.2.1.2	10.2.1.2	udp :1000	:1003	1101			
108269	5629988	7	2010-02-08T14:09:26				
1102	0 0	0.0.0.0	16	16	0		
20.2.1.2	10.2.1.2	udp :1000	:1004	1101			
108950	5665400	7	2010-02-08T14:09:26				
1102	0 0	0.0.0.0	16	16	0		
20.2.1.2	10.2.1.2	udp :1000	:1005	1101			
109474	5692648	7	2010-02-08T14:09:26				
1102	0 0	0.0.0.0	16	16	0		
20.2.1.2	10.2.1.2	udp :1000	:1006	1101			
110263	5733676	7	2010-02-08T14:09:26				
1102	0 0	0.0.0.0	16	16	0		
20.2.1.2	10.2.1.2	udp :1000	:1007	1101			
110624	5752448	7	2010-02-08T14:09:26				
1102	0 0	0.0.0.0	16	16	0		

The following example displays only flows with the destination port 1005.

Router# show mls netflow ip detail dst port 1005							
DstIP	SrcIP	Prot:SrcPort:DstPort			Src i/f		
-----	-----	-----	-----	-----	-----	-----	-----
Pkts	Bytes	Age	LastSeen				
-----	-----	-----	-----	-----	-----	-----	-----

The following example displays the number of flows.

```
Router# show mls netflow ip count  
Number of shortcuts = 5
```

```
Router# show mls netflow ip count dst port 1005  
Number of shortcuts = 1
```

Purging All Flows

Table 317 Command for Purging Flows

Command	Description
Router# clear mls netflow ip	Immediately purges all flows

Commands for the Settings for Sending Statistical Data

If a flow has been purged, and a netflow collector to send statistical data exists, the purged flow will be sent to the netflow collector. U9500 uses netflow packet version 5 to send data.

Sending Statistical Data about Netflow Traffic

Table 318 Commands for Sending Statistical Data of Netflow Traffic

Command	Description
mls nde sender	Sends statistical data about netflow traffic
ip flow-export destination	Configures the netflow collector
ip flow-export source	Configures the source interface to send statistical data

Configuring the Settings for Sending Statistical Data about Netflow Traffic

Table 319 Commands for Configuring Settings for Sending Statistical Data

Command	Description
Router(config)# mls nde sender	Enables the export of statistical data about netflow traffic
Router(config)# no mls sender	Disables the export of statistical data about netflow traffic

Setting the Receiver of Statistical Data about Netflow Traffic

Table 320 Commands for Setting Receiver of Statistical Data

Command	Description
Router(config)# ip flow-export destination A.B.C.D <1-65535>	Sets the IP, UDP PORT of the netflow collector to receive statistical data about netflow traffic. You are allowed to set values for two netflow collectors.
Router(config)# no ip flow-export destination A.B.C.D <1-65535>	Excludes the netflow collector from the receiver of statistical data about netflow traffic

Setting the Source Interface to Send Statistical Data

The following commands allow you to change the interface with which to send statistical data, for security purposes.

Table 321 Commands for Changing Interfaces

Command	Description
Router(config)# ip flow-export source <i>IFNAME</i>	Changes the source IP of the packet that is to send statistical data about the netflow traffic to the IP of the specified interface.
Router(config)# no ip flow-export source	Changes the source IP of the packet that is to send statistical data about the netflow traffic to the IP of the interface that is connected to the netflow connector.

Viewing the Export Status of Statistical Data about Netflow Traffic

Table 322 Command for Viewing Export Status of Statistical Data

Command	Description
Router# show mls nde	Displays the export status of statistical data about netflow traffic

```
Router# show mls nde
Netflow Data Export enabled
Exporting flows to 30.2.1.2 (55555) 40.2.1.2 (33333)
Exporting flows from Loopback0
Version: 5
Total Netflow Data Export Packets are:
    8 packets, 10 records
Total Netflow Data Export Send Errors:
    0 packets, 0 records dropped
Total Netflow Data Export Packets are:
    8 packets, 10 records
Total Netflow Data Export Send Errors:
    0 packets, 0 records dropped
```