D-Link®
Building Networks for People

xStack®

CLI Reference Guide

Product Model: xStack® DGS-3620 Series (G2)
Layer 3 Managed Stackable Gigabit Switch
Release 1.02

IPv6 READY

Software Release SW Rls. 1.02.000

Date: April 23, 2012

Preface

Version Description

This manual's command descriptions are based on the software release SW RIs. 1.02.000. The commands listed here are the subset of commands that are supported by the DGS-3620 series switches.

Note: Other Ethernet L2/L3 Chassis-Based Switch series Hardware using similar software may support a different subset of commands although generally the majority of the supported commands and options will be similar.

Audience

This reference manual is intended for network administrators and other IT networking professionals responsible for managing the DGS-3620 by using the D-LINK Command Line Reference (CLI). The CLI is the primary management interface to the D-LINK DGS-3620 which will be generally referred to as the "switch" within this manual. This manual is written in a way that assumes that you already have the experience and knowledge of Ethernet and modern networking principles for Local Area Networks.

Document Layout

Preface	Describes how to use the CLI reference manual.
Feature Table of Contents	A clickable command list of the DGS-3620 commands grouped by their features and linked to the command descriptions..
Command Listings	A complete list of available G2 commands arranged in alphabetical order.

Other Documentation

The documents below are a further source of information in regards to configuring and troubleshooting the switch . All the documents are available for download from D-Links web site www.d-link.com.

- DGS-3620 Series Quick Installation Guide
- DGS-3620 Series Hardware Installation Guide

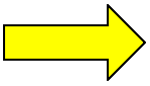
Conventions

Convention	Description
boldface font	Commands, command options and keywords are printed in **boldface**. Key words in the command line, are to be entered exactly as they are displayed.
UPPERCASE ITALICS font	Parameters or values that must be specified are printed in *UPPERCASE ITALICS*. Parameters in the command line, are to be replaced with the actual values that are desired to be used with the command.
[ ]	Square brackets enclose an optional value or set of optional arguments.
{ a | b | c }	Braces enclose alternative keywords seperated by vertical bars. Generally, one of the keywords in the seperated list can be chosen.
[a | b | c]	Optional values or arguements are enclosed in square barackets and seperated by vertical bars. Generally, one or more of the vales or arguements in the seperated list can be chosen.
`blue color screen`	**`Blue color screen font:`** is used it presents an example of a screen console display including example entries of CLI command input with the corresponding output.

Notes, Notices, and Cautions

Below are examples of the 3 types of indicators used in this manual. When administering your switch using the information in this document, you should pay special attention to these indicators. Each example below provides an explanatory remark regarding each type of indicator.

NOTE: A **NOTE** indicates important information that helps you make better use of your device



NOTICE: A **NOTICE** indicates either potential damage to hardware or loss of data and tells you how to avoid the problem

CAUTION: A **CAUTION** indicates a potential for property damage, personal injury, or death.

Command Descriptions:

The information pertaining to each command in this reference guide is presented using a number of template fields. The fields are:

- **Description -** This is a short and concise statement describing the commands functionality.
- **Syntax -** The precise form to use when entering and issuing the command. The form conventions are described in the table shown under the section “Conventions” on page iii of this guide.

- **Syntax Description -** A table where each row describes the optional or required arguments, and their use, that can be issued with the command.

- **Default -** If the command sets a configuration value or administrative state of the switch then any default settings (i.e. without issuing the command) of the configuration is shown here.

- **Command Mode -** The mode in which the command can be issued. The modes are either User EXEC, Privileged EXEC, Global Configuration or a specific configuration mode. These modes are described in the section titled “Command Modes” on page iv below.

- **Command Usage -** If necessary, a detailed description of the command and its various utilization scenarios is given here.

- **Example(s) -** Each command is accompanied by a practical example of the command being issued in a suitable scenario.

Command Modes

There are several command modes available in the command-line interface (CLI). The set of commands available to the user depends on both the mode the user is currently in and their privilege level. For each case, the user can see all the commands that are available in a particular command mode by entering a question mark (?) at the system prompt.

The command-line interface has five privilege levels:

- **Basic User** - Privilege Level 1. This user account level has the lowest priority of the user accounts. The purpose of this type of user account level is for basic system checking. The most important limitation of this account is that there is no way of changing the access right level.

- **Advanced User** - Privilege Level 3. This user account level is allowed to configure the terminal control setting. This user account can only show limited information that is not related to security.

- **Power User** - Privilege 8. This user account level can execute fewer commands than operator, including configuration commands other than the operator level and administrator level commands.

- **Operator** - Privilege Level 12. This user account level is used to grant system configuration rights for users who need to change or monitor system configuration, except for security related information such as user accounts and SNMP account settings, etc.

- **Administrator** - Privilege Level 15. This administrator user account level can monitor all system information and change any of the system configuration settings expressed in this configuration guide.

The command-line interface has a number of command modes. There are three basic command modes:

- **User EXEC mode**

- **Privileged EXEC mode**

- **Global Configuration mod**e

All other sub-configuration modes can be accessed via global configuration mode.

When a user logs in to the Switch, the privilege level of the user determines the command mode the user will enter after initially logging in. The user will either log into user EXEC mode or privileged EXEC mode. Users with a basic user level will log into the Switch in user EXEC mode. Users with advanced user, power user, operator or administrator level accounts will log into the Switch in privileged EXEC mode. Therefore, user EXEC mode can operate at basic user level and privileged EXEC mode can operate at advanced user, power user, operator or administrator level. The user can only enter global configuration mode from privileged EXEC mode. Therefore, global configuration mode can be accessed by users who have advanced user, power user, operator or administrator level user accounts. As for sub-configuration modes, a subset of those can only be accessed by users who have the highest secure administrator level privileges.

The following table briefly lists the available command modes. Only the basic command modes and some of the sub-configuration modes are enumerated. The basic command modes and basic sub-configuration modes are further described in the following chapters. Descriptions for the rest of the sub-configuration modes are not provided in this section. For more information on the additional sub-configuration modes, the user should refer to the chapters relating to these functions.

The available command modes and privilege levels are described below:

Command Mode & Privilege Level	Purpose
User EXEC mode at Basic User level	This level has the lowest priority of the user accounts. It is provided only to check basic system settings.
Privileged EXEC mode at Advanced User level	This level is allowed to configure the terminal control setting. This user account can only show limited information that is not related to security.
Privileged EXEC mode at Power User level	This level can execute less commands than operator, include the configure commands other than the operator level and administrator level commands.
Privileged EXEC mode at Operator level	For changing both local and global terminal settings, monitoring, and performing certain system administration tasks. The system administration tasks that can be performed at this level includes the clearing of system configuration settings, except for any security related information, such as user accounts, SNMP account settings etc.
Privileged EXEC mode at Administrator level	This level is identical to privileged EXEC mode at power user level, except that a user at the administrator level can monitor and clear security related settings.
Global Configuration Mode at Power User level	For applying global settings, including the configuration commands other than the operator level and administrator level commands.
Global Configuration Mode at Operator level	For applying global settings, except for security related settings, on the entire Switch. In addition to applying global settings on the entire Switch, the user can access other sub-configuration modes from global configuration mode.

Command Mode & Privilege Level	Purpose
Global Configuration Mode at Administrator level	For applying global settings on the entire Switch. In addition to applying global settings on the entire Switch, the user can access other sub-configuration modes from global configuration mode.
Interface Configuration Mode at Administrator level	For applying interface related settings.
VLAN Interface Configuration Mode	For applying VLAN interface related settings.
VLAN Configuration Mode	For applying settings to a VLAN.
IP Access-List Configuration Mode	For specifying filtering criteria for an IP access list.

User EXEC Mode at Basic User Level

This command mode is mainly designed for checking basic system settings.The most significant limitation of this command mode is that there is no way of changing the access right level of the logged in user.

This command mode can be entered by logging in as a basic user.

Privileged EXEC Mode at Advanced User Level

This command mode is mainly designed for checking basic system settings, allowing users to change the local terminal session settings and carrying out basic network connectivity verification. One limitation of this command mode is that it cannot be used to display information related to security.

This command mode can be entered by logging in as an advanced user.

Privileged EXEC Mode at Power User Level

User logged into the switch in privileged EXEC mode at this level can execute fewer commands than operator, including the configuration commands other than the operator level and administrator level commands.
The method to enter privileged EXEC mode at power user level is to login to the switch with a user account that has a privileged level of 8.

Privileged EXEC Mode at Operator Level

Users logged into the Switch in privileged EXEC mode at this level can change both local and global terminal settings, monitor, and perform system administration tasks like clearing configuration settings (except for security related information such as user accounts, SNMP account settings etc.)

The method to enter privileged EXEC mode at operator level is to login to the Switch with a user account that has a privilege level of 12.

In the following example, the user enters privileged EXEC mode at power user level by logging in with a user account called “power-user” that has a privilege level of 12:

```
User Access Verification

Username: power-user
Password:

                    DGS-3620 Chassis-based High-Speed Switch
                             Command Line Interface

                                 Firmware: 1.00.029
           Copyright (c) 2010 D-Link Corporation. All rights reserved.

DGS-3620:oper#
```

Privileged EXEC Mode at Administrator Level

This command mode has a privilege level of 15. Users logged in with this command mode can monitor all system information and change any system configuration settings mentioned in this Configuration Guide.

The method to enter privileged EXEC mode at administrator level is to login to the Switch with a user account that has a privilege level of 15.

Global Configuration Mode

The primary purpose of global configuration mode is to apply global settings on the entire Switch. Global configuration mode can be accessed at both power user and administrator level. However, security related settings are not accessible at power user level. In addition to applying global settings on the entire Switch, the user can also access other sub-configuration modes.

In order to access global configuration mode, the user must be logged in as an administrator or power user and use the **configure terminal** command in privileged EXEC mode.

In the following example, the user is logged in as an Administrator in privileged EXEC mode and uses the **configure terminal** command to access global configuration mode:

```
DGS-3620:15#configure terminal
DGS-3620:15(config)#
```

The **exit** command is used to exit global configuration mode and return to privileged EXEC mode.

The procedures to enter the different sub-configuration modes can be found in the related chapters in this Configuration Guide. The command modes are used to configure the individual functions.

Interface Configuration Mode

Interface configuration mode is used to configure the parameters for an interface or a range of interfaces. An interface can be a physical port, VLAN, or other virtual interface. Thus, interface configuration mode is distinguished further according to the type of interface. The command prompt for each type of interface is slightly different.

VLAN Interface Configuration Mode

VLAN interface configuration mode is one of the available interface modes and is used to configure the parameters of a VLAN interface.

To access VLAN interface configuration mode, use the following command in global configuration mode:

Command	Explanation
DGS-3620:15(config)#interface vlan*VLAN-ID*	Enters VLAN interface configuration mode.

Table of Contents

Address Resolution Protocol (ARP) Commands

1-1 arp

Use this command to add a permanent IP address and MAC address mapping to the ARP cache table. Use no command to remove the IP-MAC address mapping.

arp [vrf <*string 1-12*>**]** *ip-address mac-address*

no arp [vrf <*string 1-12*>**]** *ip-address*

Syntax Description	
vrf <*string 1-12*>	Specifies the VRF that the IP resides in. If no VRF name is specified, the global instance will be used.
ip-address	The IP address that corresponds to the MAC address.
mac-address	48 bit data link layer address.

Default There is no static ARP entry in the ARP cache table.

Command Mode Global configuration

Usage Guideline This command adds a static ARP mapping entry to the system. If there existed one dynamic ARP entry when create a static ARP entry for the same IP address, it will cover this dynamic entry, for the priority of static entry is higher.

If there existed one static ARP entry for the specified IP address, executing this command with different MAC address, new entry will cover the old one.

The no form of this command can delete static and dynamic entries. Local entries can't be removed.

Users can verify the settings by entering the show ip arp or show arp command.

Example The following is an example of setting an ARP static mapping record for a host in the Ethernet:

```
Switch(config)# arp 33.1.1.33 0050.BA00.0736

Remove the static ARP entry with IP address 33.1.1.33 from the ARP cache
table.

Switch(config)# no arp 33.1.1.33
```

1-2 arp timeout

Use this command to configure the timeout for the ARP static mapping record in the ARP cache. The no form of this command restores it to the default configuration.

arp timeout minutes

no arp timeout

Syntax Description	
minutes	The timeout ranging 0 to 65535 minutes.

Default The default timeout is 20 minutes

Command Mode Global configuration

Usage Guideline The ARP timeout setting is only applicable to the IP address and the MAC address mapping that are learned dynamically. The shorter the timeout, the truer the mapping table saved in the ARP cache, but the more network bandwidth occupied by the ARP. Hence the advantages and disadvantages should be weighted. Generally it is not necessary to configure the ARP timeout too short unless there is a special requirement.

Users can verify the settings by entering the show arp timeout command.

Example The following is an example of setting the timeout for the dynamic ARP mapping record to 120 minutes:

```
Switch(config)# arp timeout 120

Restore the timeout for the dynamic ARP mapping record to 20 minutes

Switch(config)# no arp timeout
```

1-3 arp gratuitous-send interval

Use this command to set the interval of sending the gratuitous ARP request message on the interface. Use no command to disable this function on the interface.

arp gratuitous-send interval seconds

no arp gratuitous-send

Syntax Description	
seconds	The time interval to send the free ARP request message in the range 1 to 3600 seconds.

Default This function is disabled on the interface to send the gratuitous ARP request regularly.

Command Mode Interface configuration mode

Usage Guideline If an interface of the switch is used as the gateway of its downlink devices and counterfeit gateway behavior occurs in the downlink devices, you can configure to send the gratuitous ARP request message regularly on this interface to notify that the switch is the real gateway.

Users can verify the settings by entering the show ip interface command.

Example The following configuration sets to send one free ARP request to SVI 1 per second:

```
Switch(config)# interface vlan 1

Switch(config-if)# arp gratuitous-send interval 1
```

The following configuration stops sending the free ARP request to SVI 1:

```
Switch(config)# interface vlan 1

Switch(config-if)# no arp gratuitous-send
```

1-4 ip proxy-arp

Use this command to enable ARP proxy function on the interface. The no form of this command disables ARP proxy function.

ip proxy-arp

no ip proxy-arp

Syntax None

Default This function is disabled by default.

Command Mode Interface configuration mode.

Usage Guideline Proxy ARP helps those hosts without routing message obtain MAC address of other networks or subnet IP address. For example, a device receives an ARP request. The IP addresses of request sender and receiver are in different networks. However, the device that knows the routing of IP address of request receiver sends ARP response, which is Ethernet MAC address of the device itself.

Use **show ip interface** to see the current setting of ARP proxy.

Example The following is an example of how to enter the interface configuration mode to enable arp proxy for the IP interface whose VID is 100:

```
Switch(config)# interface vlan 100
Switch(config-if)# ip proxy-arp
```

Example The following is an example of how to disable arp proxy on this interface:

```
Switch(config)# no ip proxy-arp
```

1-5 clear arp-cache

Use this command to remove a dynamic ARP mapping record from the ARP cache table and clear an IP route cache table in the global configuration mode.

clear arp-cache [vrf <*string 1-12*>**] [***ip-address***] [interface** *interface-name***]**

Syntax Description	
vrf <*string 1-12*>	Specifies the VRF that the IP resides in. If no VRF name is specified, the global instance will be used.
ip-address	(Optional) Specify the IP address of the dynamic ARP entry
interface *interface-name*	(Optional) Specify the interface from which the dynamic ARP entry was learned

Default None

Command Mode Privileged mode

Usage Guideline This command can be used to refresh an ARP cache table.

Example The following is an example of removing all dynamic ARP mapping records:

```
Switch# clear arp-cache
```

Example The following is an example of removing dynamic ARP table entry 1.1.1.1:

```
Switch# clear arp-cache 1.1.1.1
```

Example The following is an example of removing dynamic ARP table entry on interface SVI1:

```
Switch# clear arp-cache interface Vlan1
```

1-6 show arp

Use this command to show the Address Resolution Protocol (ARP) cache table.

show arp [vrf *<string 1-12>***] [***ip-address* **[***net-mask***] | ***mac-address* **| {static | complete}]**

Syntax Description	
vrf *<string 1-12>*	Specifies the VRF that the IP resides in. If no VRF name is specified, the global instance will be used.
ip-address	(Optional) Show the ARP entry of the specified IP address.
net-mask	(Optional) Show the ARP entries of the network segment included within the mask.
mac-address	(Optional) Show the ARP entry of the specified MAC address
static	(Optional) Specify to show all the static ARP entries.
complete	(Optional) Specify to show all the resolved dynamic ARP entries.

Default All entries in the ARP cache table will be displayed if no option is specified.

Command Mode User mode or Privileged mode.

Usage Guideline Use this command to display the ARP cache table. Static and complete is mutually exclusive with each other.

Example

```
Switch# show arp

ARP timeout is 20 minutes.

Interface      IP Address        MAC Address         Type
-------------  ----------------  ------------------  ---------------
System         10.0.0.0          FF-FF-FF-FF-FF-FF   Local/Broadcast
System         10.90.90.90       00-12-21-12-21-11   Local
System         10.1.1.5          00-12-21-12-21-18   Static
System         10.1.1.8          00-12-21-12-21-48   Static
System         10.1.1.9          00-05-5D-A5-32-3F   Dynamic
System         10.255.255.255    FF-FF-FF-FF-FF-FF   Local/Broadcast

Total Entries: 6
```

```
Switch# show arp 10.1.1.9

ARP timeout is 20 minutes.

Interface      IP Address        MAC Address         Type
-------------  --------------  -----------------  ---------------
System         10.1.1.9          00-05-5D-A5-32-3F   Dynamic

Total Entries: 1
```

```
Switch# show arp 10.1.0.0 255.255.0.0

ARP timeout is 20 minutes.

Interface      IP Address        MAC Address         Type
-------------  --------------  -----------------  ---------------
System         10.1.1.5          00-12-21-12-21-18   Static
System         10.1.1.8          00-12-21-12-21-48   Static
System         10.1.1.9          00-05-5D-A5-32-3F   Dynamic

Total Entries: 3
```

```
Switch# show arp 10.1.0.0 255.255.0.0 static

ARP timeout is 20 minutes.

Interface     IP Address      MAC Address       Type
------------- --------------- ----------------- ---------------
System        10.0.0.0        FF-FF-FF-FF-FF-FF Local/Broadcast
System        10.90.90.90     00-12-21-12-21-11 Local
System        10.1.1.5        00-12-21-12-21-18 Static
System        10.1.1.8        00-12-21-12-21-48 Static
System        10.255.255.255  FF-FF-FF-FF-FF-FF Local/Broadcast

Total Entries: 5
```

```
Switch# show arp 0005.5DA5.323F

ARP timeout is 20 minutes.

Interface      IP Address        MAC Address         Type
-------------  ---------------  -----------------  ---------------
System         10.1.1.9          00-05-5D-A5-32-3F   Dynamic

Total Entries: 1
```

```
Switch# show arp static

ARP timeout is 20 minutes.

Interface     IP Address      MAC Address       Type
------------- --------------- ----------------- ---------------
System        10.0.0.0        FF-FF-FF-FF-FF-FF Local/Broadcast
System        10.90.90.90     00-12-21-12-21-11 Local
System        10.1.1.5        00-12-21-12-21-18 Static
System        10.1.1.8        00-12-21-12-21-48 Static
System        10.255.255.255  FF-FF-FF-FF-FF-FF Local/Broadcast

Total Entries: 5
```

```
Switch# show arp complete

ARP timeout is 20 minutes.

Interface      IP Address        MAC Address         Type
-------------  ---------------  -----------------  ---------------
System         10.1.1.9          00-05-5D-A5-32-3F   Dynamic

Total Entries: 1

Switch#
```

1-7 show arp counter

Use this command to display the number of ARP entries in the ARP cache table.

show arp counter [vrf <*string 1-12*>**]**

Syntax Description	
vrf <*string 1-12*>	Specifies the VRF that the IP resides in. If no VRF name is specified, the global instance will be used.

Default None.

Command Mode User mode or Privileged mode.

Usage Guideline Use this command to display the number of ARP entries in the ARP cache table.

Example

```
Switch# show arp counter

Total ARP Entry Counter: 3

Switch#
```

1-8 show arp timeout

Use this command to display the aging time of a dynamic ARP entry on the switch.

show arp timeout

Syntax Description None.

Default None

Command Mode User mode or Privileged mode.

Usage Guideline Use this command to display the aging time of a dynamic ARP entry on the switch.

Example To display the ARP timeout value:

```
Switch# show arp timeout

ARP timeout is 20 minutes.

Switch#
```

1-9 show ip arp

Use this command to display the Address Resolution Protocol (ARP) cache table.

show ip arp [vrf <*string 1-12*>**]**

Syntax Description	
vrf <*string 1-12*>	Specifies the VRF that the IP resides in. If no VRF name is specified, the global instance will be used.

Default None

Command Mode User mode or Privileged mode.

Usage Guideline Use this command to display the Address Resolution Protocol (ARP) cache table.

Example

```
Switch# show ip arp

ARP timeout is 20 minutes.

Interface      IP Address        MAC Address         Type
-------------  --------------  -----------------  ---------------
System         10.0.0.0        FF-FF-FF-FF-FF-FF   Local/Broadcast
System         10.90.90.90     00-12-21-12-21-11   Local
System         10.255.255.255  FF-FF-FF-FF-FF-FF   Local/Broadcast

Total Entries: 3

Switch#
```

Border Gateway Protocol (BGP) Commands

2-1 address-family ipv4

Use this command to enter the IPv4 address family mode. Use the **no** form of this command to delete the configuration of an address family.

address-family ipv4 [{unicast | vrf *VRF-NAME***}]**

no address-family ipv4 [{unicast | vrf *VRF-NAME***}]**

Syntax Description	
unicast	Specifies to enter the IPv4 unicast address family configuration mode.
vrf *VRF-NAME*	Specifies the name of the VRF instance to enter IPv4 VRF address family configuration mode.

Default None.

Command Mode Router Configuration.

Usage Guideline This command is used to enter the IPv4 address family mode. Different configuration parameters can be set in different address family mode. The IPv4 VRF address family mode is used to configure the BGP instance relation to every VRF instance. If no parameters are specified, it will enter the IPv4 unicast address family mode.

Please note that only eBGP peer is supported in the IPv4 VRF address family.

To exit from the address-family configuration mode, use the **exit-address-family** command.

Example This example shows how to enter the IPv4 unicast address family and activate peer session:

```
Switch# configure terminal
Switch(config)# router bgp 10
Switch(config-router)# address-family ipv4 unicast
Switch(config-router-af)# neighbor 5.5.5.5 activate
Switch(config-router-af)# exit-address-family
Switch(config-router)#
```

This example shows how to enter the VRF address family and create a BGP peer:

```
Switch# configure terminal
Switch(config)# router bgp 10
Switch(config-router)# address-family ipv4 vrf VPN-A
Switch(config-router-af)# neighbor 5.5.5.5 remote-as 20
Switch(config-router-af)# exit-address-family
Switch(config-router)#
```

2-2 address-family vpnv4

This command is used to enter the IPv4 VPN address family mode. Use the **no** form of this command to delete the configuration of the VPNv4 address family.

address-family vpnv4

no address-family vpnv4

Syntax Description None.

Default None.

Command Mode Router Configuration.

Usage Guideline This command is used to enter the IPv4 VPN address family mode. The BGP peers activated in this mode are used to exchange VPN IPv4 routing information.

Please note that only iBGP peer is supported in this address family now.

To exit from this address-family configuration mode, use the **exit-address-family** command.

Example This example shows how to enter vpnv4 address family and activate a BGP peer:

```
Switch# configure terminal
Switch(config)# router bgp 120
Switch(config-router)# address-family vpnv4
Switch(config-router-af)# neighbor 10.2.2.5 activate
Switch(config-router-af)# neighbor 10.2.2.5 send-community extended
Switch(config-router-af)# exit-address-family
Switch(config-router)#
```

2-3 aggregate-address

Use this command to configure BGP aggregate entries. Use the **no** form of this command to delete an aggregate entry.

aggregate-address *NETWORK-ADDRESS* **[summary-only] [as-set]**

no aggregate-address *NETWORK-ADDRESS*

Syntax Description	
NETWORK-ADDRESS	Specify the network address and the sub-network mask that BGP will aggregate. For example, the format of NETWORK-ADDRESS can be 10.9.18.2/8.
summary-only	(Optional) Filters all more-specific routes from updates.
as-set	(Optional) Generates autonomous system set path information.

Default None.

Command Mode Router configuration mode

Address family configuration mode (IPv4 Unicast and VRF)

Usage Guideline Aggregates are used to minimize the size of routing tables. Aggregation combines the characteristics of several different routes and advertises a single route. The **aggregate-address** command creates an aggregate entry in the BGP routing table if any more-specific BGP routes are available in the specified range. Using the **summary-only** parameter advertises the prefix only, suppressing the more-specific routes to all neighbors.

Use the **as-set** parameter to reduce the size of path information by listing each AS number only once, even if it was included in multiple paths that were aggregated. The **as-set** parameter is useful when aggregation of information results in incomplete path information.

You can verify your settings by entering **show ip bgp aggregate** command.

Example This example shows how to propagate network 172.0.0.0 and suppresses the more specific route 172.10.0.0:

```
Switch# configure terminal
Switch(config)# router bgp 65534
Switch(config-router)# aggregate-address 172.0.0.0/8 summary-only
```

2-4 bgp router-id

Use this command to configure a fixed router ID for the local Border Gateway Protocol (BGP) routing process. Use the **no** form of this command to remove the fixed router ID from the running configuration file and restore the default router ID selection.

bgp router-id *IP-ADDRESS*

no bgp router-id

Syntax Description	
IP-ADDRESS	Configures the router ID in IPv4 address format as the identifier of the local router running BGP.

Default

The local router ID is selected by the following rules when this command is disabled:

- If a loopback interface is configured, the router ID is set to the IP address of the loopback. If multiple loopback interfaces are configured, the loopback with the highest IP address is used.
- If no loopback interface is configured, the router ID is set to the highest IP address on a physical interface.

Command Mode

Router configuration.

Usage Guideline

The **bgp router-id** command is used to configure a fixed router ID for a local BGP routing process.

The address of a loopback interface is preferred to an IP address on a physical interface because the loopback interface is more effective than a fixed interface as an identifier because there is no physical link to go down.

You must specify a unique router ID within the network.

This command will reset all active BGP peering sessions.

It is recommended to configure a loopback interface, since the physical interface link may be up/down/removed for some reason.

You can verify your settings by entering the **show ip bgp parameters** command.

Example

This example shows how to change the router ID with 192.168.1.1:

```
Switch# configure terminal
Switch(config)# router bgp 65100
Switch(config-router)# bgp router-id 192.168.1.1
```

2-5 bgp aggregate-next-hop-check

This command is used to enable the checking of next hop of the BGP aggregated routes. Only the routes with the same next hop attribute can be aggregated if the BGP aggregate next hop check is enabled. Using the **no** form of this command is to disable the bgp aggregate-next-hop-check.

bgp aggregate-next-hop-check

no bgp aggregate-next-hop-check

Syntax None.

Default Disabled.

Command Mode Router configuration.

Usage Guideline This command is used to enable the checking of next hop of the BGP aggregated routes. Only the routes with the same next hop attribute can be aggregated if the BGP aggregate next hop check is enabled. Using the **no** form of this command is to disable the bgp aggregate-next-hop-check.

You can verify your settings by entering the **show ip bgp parameters** command.

Example This example shows how to configure the BGP aggregate-next-hop-check state:

```
Switch# configure terminal
Switch(config)# router bgp 100
Switch(config-router)# bgp aggregate-next-hop-check
```

2-6 bgp always-compare-med

Use this command to enable the comparison of the Multi Exit Discriminator (MED) for paths from neighbors in different autonomous systems. Use the **no** form of this command to disallow the comparison.

bgp always-compare-med

no bgp always-compare-med

Syntax None

Default This function is disabled by default.

Command Mode Router configuration mode.

Usage Guideline The MED, as stated in RFC 1771, is an optional non-transitive attribute that is a four octet non-negative integer. The value of this attribute may be used by the BGP best path selection process to discriminate among multiple exit points to a neighboring autonomous system.

The MED is one of the parameters that are considered when selecting the best path among many alternative paths. The path with a lower MED is preferred over a path with a higher MED. During the best-path selection process, MED comparison is done only among paths from the same autonomous system. The **bgp always-compare-med** command is used to change this behavior by enforcing MED comparison between all paths, regardless of the autonomous system from which the paths are received.

The **bgp deterministic-med** command can be configured to enforce deterministic comparison of the MED value between all paths received from within the same autonomous system.

You can verify your settings by entering **show ip bgp parameters** command.

Example This example shows how to configure to compare the MED from alternative paths, regardless of the autonomous system from which the paths are received:

```
Switch# configure terminal
Switch(config)# router bgp 65534
Switch(config-router)# bgp always-compare-med
```

2-7 bgp bestpath as-path ignore

Use this command to not consider the as-path factor in selection of the best path. Use the **no** form of this command to restore default behavior and configure BGP to consider the AS-path during route selection.

bgp bestpath as-path ignore

no bgp bestpath as-path ignore

Syntax None

Default AS path is considered when the best path selects.

Command Mode Router configuration mode.

Usage Guideline The following are the best path selection rules.

1.If the next hop associated with the route is unreachable, then the route is dropped.

2.Then route with the largest weight is selected.

3.If weight cannot determine, then the largest LOCAL-PREF is used to determine the preferred route.

4.If still cannot determine the preferred route, then the route with the shortest AS-PATH list is preferred.

5.If still cannot determine the preferred route, then lowest origin type is preferred.

6.If still cannot determine the preferred route, then the lowest MED is preferred.

7.If still cannot determine the preferred route, eBGP is preferred over iBGP paths.

8.Prefer the path with the lowest IGP metric to the BGP next hop.

9.Determine if multiple paths require installation in the routing table for BGP Multipath.

10.When both paths are external, prefer the path that was received first (the oldest one).

11.Prefer the route that comes from the BGP router with the lowest router ID.

12.If the originator or router ID is the same for multiple paths, prefer the path with the minimum cluster list length.

13.Prefer the path that comes from the lowest neighbor address.

You can use the commands, **bgp bestpath as-path ignore**, **bgp bestpath compare-router-id** or **bgp default local-preference** to customize the path selection process.

You can verify your settings by entering **show ip bgp parameters** command.

Example This example shows how to configure to ignore the AS-PATH for the best path for autonomous system 65534:

```
Switch# configure terminal
Switch(config)# router bgp 65534
Switch(config-router)# bgp bestpath as-path ignore
```

2-8 bgp bestpath compare-confed-aspath

To configure a BGP routing process to compare the confederation AS path length of the routes received, use this command in router configuration mode. To return the BGP routing process to the default operation, use the **no** form of this command.

bgp bestpath compare-confed-aspath

no bgp bestpath compare-confed-aspath

Syntax None

Default This function is disabled by default.

Command Mode Router configuration mode.

Usage Guideline If enabled, the BGP process will compare the confederation AS path length of the routes received. The shorter the confederation AS path length, the better the route is.

You can verify your settings by entering **show ip bgp parameters** command.

Example This example shows how to enable BGP process to compare the AS path which contains some confederation as numbers:

```
Switch# configure terminal
Switch(config)# router bgp 100
Switch(config-router)# bgp bestpath compare-confed-aspath
```

2-9 bgp bestpath compare-routerid

Use this command to compare router ID for identical eBGP paths. Use the **no** command to revert to disable this function.

bgp bestpath compare-routerid

no bgp bestpath compare-routerid

Syntax None

Default BGP receives routes with identical eBGP paths from eBGP peers and selects the first route received as the best path.

Command Mode Router configuration mode.

Usage Guideline When comparing similar routes from peers the BGP router does not consider router ID of the routes. By default, it selects the first received route. Use this command to include router ID in the selection process; similar routes are compared and the route with lowest router ID is selected. The router-id is the highest IP address on the router, with preference given to loopback addresses. Router ID can be manually set by using the **bgp router-id** command.

You can verify your settings by entering **show ip bgp parameters** command.

Example This example shows how to configure to compare router ID for identical eBGP paths for autonomous system 65534:

```
Switch# configure terminal
Switch(config)# router bgp 65534
Switch(config-router)# bgp bestpath compare-routerid
```

2-10 bgp bestpath med confed

To configure a BGP routing process to compare the Multi Exit Discriminator(MED)between paths learned form confederation peers, use the **bgp bestpath med confed** command in router configuration mode, To disable MED comparison of paths received from confederation peers, use the **no** form of this command.

bgp bestpath med confed

no bgp bestpath med confed

Syntax None

Default The default value is disabled.

Command Mode Router configuration mode.

Usage Guideline If enabled, the BGP process will compare the MED for the routes that are received from confederation peers. For routes that have an external AS in the path, the comparison does not occur.

You can verify your settings by entering **show ip bgp parameters** command.

Example In the following example, the BGP routing process is configured to compare MED values for paths learned from confederation peers:

```
Switch# configure terminal
Switch(config)# router bgp 100
Switch(config-router)# bgp bestpath med confed
```

2-11 bgp bestpath med missing-as-worst

To configure a BGP routing process to assign a value of infinity to routes that are missing the Multi Exit Discriminator (MED) attribute(making the path without a MED value the least desirable path),use this command in router configuration mode. To return the router to the default behavior (assign a value of 0 to the missing MED), causing this path as the best path to be chosen, use the **no** form of this command.

bgp bestpath med missing-as-worst

no bgp bestpath med missing-as-worst

Syntax None

Default The default value is disabled.

Command Mode Router configuration mode.

Usage Guideline If enabled, the BGP process will assign a value of infinity to routes that are missing the Multi Exit Discriminator (MED) attribute.

If disabled, the BGP process will assign a value of zero to routes that are missing the Multi Exit Discriminator (MED) attribute, causing this route to be chosen as the best path.

You can verify your settings by entering **show ip bgp parameters** command.

Example This example shows how to enable the BGP router process to consider a route with a missing MED attribute as having a value of infinity, making this path the least desirable path:

```
Switch# configure terminal
Switch(config)# router bgp 100
Switch(config-router)# bgp bestpath med missing-as-worst
```

2-12 bgp client-to-client reflection

Use this command to enable route reflection from a route reflector to clients. To disable client-to-client route reflection, use the **no** form of this command.

bgp client-to-client reflection

no bgp client-to-client reflection

Syntax None

Default The default value is enabled.

Command Mode Router configuration mode.

Usage Guideline By default, the clients of a router reflector are not required to be fully meshed and the routes from a client are reflected to other clients. However, if the clients are fully meshed, route reflection is not required. In this case, use the **no bgp client-to-client reflection** command to disable client-to-client reflection.

Use the **show ip bgp reflection** command to verify your settings.

Example The following example shows how to enable the route reflector function of the local router:

```
Switch(config)#router bgp 100
Switch(config-router)#bgp client-to-client reflection
Switch(config-router)#
```

2-13 bgp cluster-id

Use this command to set the cluster ID of the route reflector. To remove the cluster ID, use the **no** form of this command.

bgp cluster-id *CLUSTER-ID*

no bgp cluster-id

Syntax Description	
CLUSTER-ID	The cluster ID in IPv4 address format setting for the router reflector.

Default N/A.

Command Mode Router configuration mode.

Usage Guideline When a single route reflector is deployed in a cluster and the cluster ID of the route reflector is 0.0.0.0, the cluster is identified by the router ID of the route reflector. Otherwise, the cluster is identified by the cluster ID.

The **bgp cluster-id** command is used to assign a cluster ID to a route reflector. Multiple route reflectors are deployed in a cluster to increase redundancy and to avoid a single point of failure. When multiple route reflectors are configured in a cluster, they must be configured with the same cluster ID. This allows all route reflectors in the cluster to recognize updates from peers in the same cluster and reduces the number of updates that needs to be stored in BGP routing tables.

This command is only required for the reflector and not the client.

Use the **show ip bgp reflection** command to verify your settings.

Example In the following example, the local router is one of the route reflectors serving the cluster. It is configured with the cluster ID to identify the cluster:

```
Switch(config)#router bgp 100
Switch(config-router)#neighbor 172.18.0.16 route-reflector-client
Switch(config-router)#bgp cluster-id 10.0.0.2
Switch(config-router)#
```

2-14 bgp confederation identifier

This command is used to specify a BGP confederation identifier. Use the **no** form of this command to remove the confederation identifier.

bgp confederation identifier *AS-NUMBER*

no bgp confederation identifier

Syntax Description	
AS-NUMBER	Autonomous System numbers which use to specify a BGP confederation. The value is from 1 to 4294967295, but AS TRANS (23456).

Default N/A.

Command Mode Router configuration mode.

Usage Guideline A confederation can be used to reduce the internal BGP (iBGP) mesh by dividing a large single AS into multiple subs-AS. External peers interact with the confederation as if it is a single AS.

Each subs-AS is fully meshed within itself and it has connections to other sub ASs within the confederation. The next hop, Multi Exit Discriminator (MED), and local preference information is preserved throughout the confederation, allowing users to retain a single Interior Gateway Protocol (IGP) for all the autonomous systems.

Use the **show ip bgp confederation** command to verify your settings..

Example This example shows how to create a confederation in which the AS number is 20:

```
Switch(config)#router bgp 10
Switch(config-router)#bgp confederation identifier 20
Switch(config-router)#
```

2-15 bgp confederation peers

This command is used to add BGP confederation peers. Use the **no** form of this command to delete the confederation peers.

bgp confederation peers *ASPATH-LIST*

no bgp confederation peers *ASPATH-LIST*

Syntax Description	
ASPATH-LIST	Can be one or multiple AS number partitions separated by a comma. AS number: 1-4294967295, but AS TRANS (23456). Autonomous System numbers for BGP peers that will belong to the confederation.

Default None.

Command Mode Router configuration mode.

Usage Guideline The command is used to configure multiple adjacent Autonomous Systems in a confederation. The Autonomous Systems specified in this command are visible internally to the confederation. Each Autonomous System is fully meshed within itself or configures route reflector.

Use the **no bgp confederation peers** command to delete all the or part of the AS numbers early configured.

Use the **show ip bgp confederation** command to verify your settings.

Example In the following example, AS 21, 22, 23, 24, 25 are configured to belong to a single confederation under the identifier 10:

```
Switch(config)#router bgp 20
Switch(config-router)#bgp confederation identifier 10
Switch(config-router)#bgp confederation peers 21,22,23,24,25
Switch(config-router)#
```

Use the **show ip bgp confederation** command to verify your settings. You can delete part of the AS numbers if you want.

```
Switch(config-router)#no bgp confederation peers 21,22
Switch(config-router)#
```

You can also delete all the AS numbers.

```
Switch(config-router)#no bgp confederation peers 23,24,25
Switch(config-router)#
```

2-16 bgp dampening

Use this command to enable BGP route dampening or change BGP route dampening parameters. To disable BGP dampening, use the **no** form of this command.

bgp dampening [{*HALF-LIFE REUSE SUPPRESS MAX-SUPPRESS-TIME UN-REACHABILTY-HALF-TIME* **| route-map** *MAP-NAME***}]**

no bgp dampening [route-map]

Syntax Description	
HALF-LIFE	Specifies the time (in minutes) after which the penalty of the reachable routes will be down, by half.
REUSE	If the penalty for a flapping route decreases enough to fall below this value, the route is unsuppressed.
SUPPRESS	A route is suppressed when its penalty exceeds this limit.
MAX-SUPPRESS-TIME	The maximum time (in minutes) a route can be suppressed.
UN-REACHABILITY-HALF-LIFE	Specifies the time (in minutes) after which the penalty of the unreachable routes will be down; by half.
MAP-NAME	Route map name for set the dampening running configuration. The maximum length is 16 characters.

Default

BGP dampening is disabled by default.

The following values are used when this command is enabled without configuring any optional arguments:

Half-life: 15 minutes

Reuse: 750

Suppress: 2000

Max-suppress-time: 60 minutes.

Un-reachability-half-life: 15 minutes.

Command Mode

Router configuration mode.
Address family configuration mode (IPv4 Unicast, VPNv4 and VRF).

Usage Guideline

The purpose of this command is to eliminate the dampening of routes and thus to avoid unstable networks caused by flapping routes. The following describes the way it is achieved.
When a route flaps (from up to down), add the penalty by 1000.Since the penalty is smaller than the suppress value, BGP will work normally. It will send a withdraw message (an update message) to the neighbors.

The penalty of the route will decrease as time elapses. Here we assume that if it passes 7.5 minutes, then the penalty of the route is 1000-500*7.5/15=750.
If another flap occurs (the route changes from down to up) then the penalty of the route will be 1750, which is larger than the suppress value, and the route will be dampened. BGP will not send an update message for this status change.

When the penalty of the route decreases and becomes smaller than the re-use value (800), the route will not be dampened and the update message will be sent again.

Lastly, the max-suppress-time is the longest time the route may be suppressed. So, it decides the maximum penalty a route may suffer regardless of the number of times that the prefix is dampened. Here is the formula: Maximum-penalty= reuse-value*$2^{\text{max-suppress-time/half-life}}$
You can verify your settings by entering **show ip bgp dampening parameters** command.

Note: If the dampening ability is enabled and there are one or more dampened routes, the dampened routes will be released to be the normal state immediately after we disable the dampening function.

Examples

This example show how to enable BGP dampening and set the half life to 20 minutes,1200 for the reuse value,6000 for the suppress value, and 100 minutes for the maximum suppress time, 20 minutes for un-reachability-half-life:

```
Switch# configure terminal
Switch(config)# router bgp 100
Switch(config-router)# bgp dampening 20 1200 6000 100 20
```

The following example shows how to apply BGP damping to prefixes filtered by route-map mymap1:

```
Switch# configure terminal
Switch(config)# ip prefix-list pp1 permit 100.2.0.0/16
Switch(config)# route-map mymap1
Switch(config-route-map)# match ip address prefix-list pp1
Switch(config-route-map)# exit
Switch(config)# router bgp 100
Switch(config-router)# bgp dampening route-map mymap1
```

This following example shows how to configure bgp dampending under the view of address family:

```
Switch# configure terminal
Switch(config)# router bgp 100
Switch(config)# address-family ipv4
Switch(config-router-af)# bgp dampening 20 100 6000 120 20
```

2-17 bgp default local-preference

Use this command to change the default local preference value. To return the local preference value to the default setting, use the **no** form of this command.

bgp default local-preference *NUMBER*

no bgp default local-preference

Syntax Description	
NUMBER	Range of local reference is 0 to 4294967295.

Default If this command is disabled, BGP set default local preference value to100.

Command Mode Router configuration mode.

Usage Guideline The local preference attribute is a discretionary attribute that is used to apply the degree of preference to a route during the BGP best path selection process. This attribute is exchanged only between iBGP peers and is used to determine local policy. The route with the highest local preference is preferred.

You can verify your settings by entering **show ip bgp parameters** command.

Examples This example shows how to configure default value of the local preference to 200 for autonomous system 65534:

```
Switch# configure terminal
Switch(config)# router bgp 65534
Switch(config-router)# bgp default local-preference 200
```

2-18 bgp deterministic-med

Use this command to include the Multi Exit Discriminator (MED) value between all paths received from within the same autonomous system in the selection of the best route selection. Use the **no** command to prevent BGP from considering the MED attribute in comparing paths.

bgp deterministic-med

no bgp deterministic-med

Syntax Description None.

Default Disabled

Command Mode Router configuration

Usage Guideline The **bgp always-compare-med** command is used to enable the comparison of the Multi Exit Discriminator (MED) for paths from neighbors in different autonomous systems. After the **bgp always-compare-med** command is configured, all paths for the same prefix that are received from different neighbors, which are in the same autonomous system, will be grouped together and sorted by the ascending MED value (received-only paths are ignored and not grouped or sorted).

The best path selection algorithm will then pick the best paths using the existing rules; the comparison is made on a peer neighbor autonomous system basis and then global basis. The grouping and sorting of paths occurs immediately after this command is entered. For correct results, all routers in the local autonomous system must have this command enabled (or disabled).

The **bgp deterministic-med** command can be configured to enforce deterministic comparison of the MED value between all paths received from within the same autonomous system.

You can verify your settings by entering **show ip bgp parameters** command.

Examples This example shows how to configure to enable compare MED value for autonomous system 65534:

```
Switch# configure terminal
Switch(config)# router bgp 65534
Switch(config-router)# bgp deterministic-med
```

2-19 bgp enforce-first-as

Use this command to enforce the first AS for the eBGP routes. To disable this feature, use the **no** form of this command.

bgp enforce-first-as

no bgp enforce-first-as

Syntax Description None

Default Disabled

Command Mode Router configuration mode.

Usage Guideline This command specifies that any updates received from an external neighbor that do not have the neighbor's configured Autonomous System at the beginning of the AS-PATH attribute in the received update must be denied. Enabling this feature adds to the security of the BGP network by not allowing traffic from unauthorized systems.

You can verify your settings by entering **show ip bgp parameters** command.

Examples This example shows how to enable the security of the BGP network for autonomous system 65534. All incoming updates from eBGP peers are examined to ensure that the first AS number in the AS-PATH attribute is the local AS number of the transmitting peer:

```
Switch# configure terminal
Switch(config)# router bgp 65534
Switch(config-router)# bgp enforce-first-as
```

2-20 bgp fast-external-fallover

To configure a Border Gateway Protocol (BGP) routing process to immediately reset external BGP peering sessions if the link used to reach these peers goes down, use this command in router configuration mode. To disable BGP fast external fallover, use the **no** form of this command.

bgp fast-external-fallover

no bgp fast-external-fallover

Syntax Description None

Default Enabled

Command Mode Router configuration

Usage Guideline The **bgp fast-external-fallover** command is used to disable or enable fast external fallover for BGP peering sessions with directly connected external peers. The session is immediately reset if link(interface admin state is disable or the interface which carry the session is not existed) goes down. Only directly connected peering sessions are supported.

If BGP fast external fallover is disabled, the BGP routing process will wait until the default hold timer expires (3 keepalives) to reset the peering session.

You can verify your settings by entering **show ip bgp parameters** command.

Examples In the following example, the BGP fast external fallover feature is disabled. If the link through which this session is carried flaps, the connection will not be reset:

```
Switch# configure terminal
Switch(config)# router bgp 65534
Switch(config-router)# no bgp fast-external-fallover
```

2-21 bgp default ipv4-unicast

Use this command to enable the IPv4 unicast address family as the default address family for BGP peer session establishment. The **no** form of the command disable default IPv4 unicast address family for BGP peer session establishment.

bgp default ipv4-unicast

no bgp default ipv4-unicast

Syntax Description None.

Default Enabled.

Command Mode Router configuration.

Usage Guideline The **bgp default ipv4-unicast** command is used to enable the automatic establish BGP peer connection and exchange of IPv4 unicast address family prefixes. If the **no bgp default ipv4-unicast** command is executed, the neighbor activate address family configuration command must be executed in each IPv4 address family session before prefix exchange will occur.
The **no bgp default ipv4-unicast** command is often executed in PE routers when exchanging VPN IPv4 routes.

You can verify your settings by entering the **show ip bgp parameters** command.

Example This example shows how to disable default IPv4 unicast address family for BGP peer session establishment.

```
Switch# configure terminal
Switch(config)# router bgp 10
Switch(config-router)# no bgp default ipv4-unicast
Switch(config-router)# exit
Switch(config)#
```

2-22 clear ip bgp

To reset Border Gateway Protocol (BGP) connections using hard or soft reconfiguration, use this command in privileged mode.

clear ip bgp {all | *AS-NUMBER* | *IP-ADDRESS***} [soft [{in [prefix-filter] | out}]]**

Syntax Description	
all	(Optional) Specifies the reset of all sessions except those in the VRF address family.
AS-NUMBER	Specifies that sessions with BGP peers in the specified autonomous system will be reset. Range for 2-byte numbers is 1 to 65535. Range for 4-byte numbers is 1 to 4294967295.
IP-ADDRESS	Specifies that only the identified BGP neighbor will be reset. The value for this argument is an IPv4 address.
in	(Optional) Initiates inbound reconfiguration. If neither the in nor out keywords are specified, both inbound and outbound sessions are reset.
prefix-filter	(Optional) Clears the existing outbound route filter (ORF) prefix list to trigger a new route refresh or soft reconfiguration, which updates the ORF prefix list.
out	(Optional) Initiates inbound or outbound reconfiguration. If neither the in nor out keywords are specified, both inbound and outbound sessions are reset.
soft	(Optional) Initiates a soft reset. Does not tear down the session.

Default None

Command Mode Privileged mode.

Usage Guideline This command can be used to initiate a hard reset or soft reconfiguration of BGP neighbor sessions.

If a hard reset is applied to the inbound session, the inbound session will be torn down and the local inbound routing table and the remote outbound routing table will be cleared.

If a soft reset is applied to the inbound session, the session will not be rebuilt but the local inbound routing table will be cleared and needs to be rebuilt.

If a soft reconfiguration inbound is enabled, then the routing table can be rebuilt based on the stored route updates information. If a soft reconfiguration inbound is disabled, then the local router will send the route refresh request to the neighbor to ask for the route refresh.

When the inbound session is soft reset with the prefix filter option, and the capability orf prefix-list is enabled in the send direction, then the local BGP will send ‘clear the routing table’, and notify the remote neighbor for the prefix filter.

This is a way to notify the neighbor of the prefix filter whenever a change is made to the prefix filter.

Examples

In the following example, a soft reconfiguration is initiated for the inbound session with the neighbor 10.100.0.1, and the outbound session is unaffected:

```
Switch# clear ip bgp 10.100.0.1 soft in
Switch#
```

In the following example, the route refresh capability is enabled on the BGP neighbor routers. The existing outbound route filter (ORF) prefix list from peer 172.16.10.2 is cleared, The new route refresh which updates the ORF prefix list is triggered.

```
Switch# clear ip bgp 172.16.10.2 soft in prefix-filter
Switch#
```

In the following example, a hard reset is initiated for sessions with all routers in the autonomous system numbered 35700:

```
Switch# clear ip bgp 35700
Switch#
```

2-23 clear ip bgp vrf

To reset BGP connections using hard or soft reset for IPv4 VRF address family sessions.

clear ip bgp vrf *VRF-NAME* **{all |** *IP-ADDRESS* **|** *AS-NUMBER***} [soft [{in [prefix-filter] | out}]]**

Syntax Description	
VRF-NAME	Specifies the name of VRF.
all	Specifies to reset all BGP sessions in IPv4 VRF address family.
IP-ADDRESS	Specifies to only reset the BGP neighbor with the IP address in the VRF address family.
AS-NUMBER	Specifies to only reset the BGP neighbor with the AS number in the VRF address family.
in	(Optional) Specifies inbound reset. If neither the in nor out is specified, both inbound and outbound sessions are reset.
prefix-filter	(Optional) Clears the existing outbound route filter (ORF) prefix list to trigger a new route refresh or soft reconfiguration, which updates the ORF prefix list.
out	(Optional) Specifies outbound reset. If neither the in nor out is specified, both inbound and outbound sessions are reset.
soft	(Optional) Specifies a soft reset. The session is not torn down.

Default None.

Command Mode Privileged mode.

Usage Guideline This command can be used to initiate a hard reset or soft reset of BGP neighbor sessions.

If a hard reset is applied to the inbound session, the inbound session will be torn down and the local inbound routing table and the remote outbound routing table will be cleared.

If a soft reset is applied to the inbound session, the session will not be rebuilt but the local inbound routing table will be cleared and needs to be rebuilt.

If a soft reset inbound is enabled, then the routing table can be rebuilt based on the stored route updates information. If a soft reset inbound is disabled, then the local router will send the route refresh request to the neighbor to ask for the route refresh.

When the inbound session is soft reset with the prefix filter option, and the capability orf prefix-list is enabled in the send direction, then the local BGP will send ‘clear the routing table’, and notify the remote neighbor for the prefix filter.

This command can only take effect for the sessions in VRF address family.

Examples

In the following example, a soft reset is initiated for the inbound session for all neighbors those have been created in the view of vrf and the outbound session is unaffected:

```
Switch# clear ip bgp vrf VPN-A all soft in
Switch#
```

2-24 clear ip bgp vpnv4

To reset BGP connections using hard or soft reset for IPv4 VPN address family sessions.

clear ip bgp vpnv4 unicast {all | *IP-ADDRESS* **} [soft [{in [prefix-filter] | out}]]**

Syntax Description	
all	Specifies to reset all BGP sessions in the VPN address family.
IP-ADDRESS	Specifies to only reset the BGP neighbor with the IP address.
in	(Optional) Specifies inbound reset. If neither the in nor out is specified, both inbound and outbound sessions are reset.
prefix-filter	(Optional) Clears the existing outbound route filter (ORF) prefix list to trigger a new route refresh or soft reconfiguration, which updates the ORF prefix list.
out	(Optional) Specifies outbound reset. If neither the in nor out is specified, both inbound and outbound sessions are reset.
soft	(Optional) Specifies a soft reset. The session is not torn down.

Default None.

Command Mode Privileged mode.

Usage Guideline This command can be used to initiate a hard reset or soft reset of BGP neighbor sessions.

If a hard reset is applied to the inbound session, the inbound session will be torn down and the local inbound routing table and the remote outbound routing table will be cleared.

If a soft reset is applied to the inbound session, the session will not be rebuilt but the local inbound routing table will be cleared and needs to be rebuilt.

If a soft reset inbound is enabled, then the routing table can be rebuilt based on the stored route updates information. If a soft reset inbound is disabled, then the local router will send the route refresh request to the neighbor to ask for the route refresh.

When the inbound session is soft reset with the prefix filter option, and the capability orf prefix-list is enabled in the send direction, then the local BGP will send ‘clear the routing table’, and notify the remote neighbor for the prefix filter.

The hard reset of this command takes the same effect with the hard reset of clear ip bgp command. The soft reset here is for VPNv4 address family of the neighbors.

Examples

In the following example, a soft reconfiguration for VPNv4 address family is initiated for the inbound session for all neighbors which have been created outside VRF address family, and the outbound session is unaffected:

```
Switch# clear ip bgp vpnv4 unicast all soft in
Switch#
```

2-25 clear ip bgp dampening

To clear BGP route dampening information and to restore suppressed routes, use this command in privileged mode.

clear ip bgp dampening [{*NETWORK-ADDRESS* **|** *IP-ADDRESS***}]**

Syntax Description	
NETWORK-ADDRESS	(Optional) IPv4 address of the network or neighbor to clear dampening information.
IP-ADDRESS	(Optional) IPv4 address.

Default None.

Command Mode Privileged mode.

Usage Guideline The **clear ip bgp dampening** is used to clear stored route dampening information. If no keywords or arguments are entered, route dampening information for the entire routing table is cleared.

Examples The following example clears route dampening information of 192.168.10.0/24 and restores suppressed routes.

```
Switch# clear ip bgp dampening 192.168.10.0/24
Switch#
```

2-26 clear ip bgp dampening vrf

To clear BGP route dampening information of VRF instance and to restore suppressed routes.

clear ip bgp dampening vrf *VRF-NAME* **[{***NETWORK-ADDRESS* **|** *IP-ADDRESS***}]**

Syntax Description	
VRF-NAME	Specifies the name of VRF.
NETWORK-ADDRESS	(Optional) Specifies to only clear dampening information of the route matching the network address.
IP-ADDRESS	(Optional) Specifies to only clear dampening information of the route matching the IP address.
N/A	Specifies to clear dampening information of all routes.

Default None.

Command Mode Privileged mode.

Usage Guideline The **clear ip bgp dampening vrf** command is used to clear stored route dampening information. If no keyword is specified, the dampening information of all routes in the VRF instance will be cleared.

Examples The following example clears route dampening information of 192.168.10.0/24 and restores suppressed routes in VRF VPN-A.

```
Switch# clear ip bgp dampening vrf VPN-A 192.168.10.0/24
Switch#
```

2-27 clear ip bgp dampening ipv4 unicast

To clear BGP route dampening information and to restore suppressed routes of IPv4 unicast address family sessions.

clear ip bgp dampening ipv4 unicast [{*NETWORK-ADDRESS* **|** *IP-ADDRESS***}]**

Syntax Description	
NETWORK-ADDRESS	(Optional) Specifies to only clear dampening information of the route matching the network address.
IP-ADDRESS	(Optional) Specifies to only clear dampening information of the route matching the IP address.
N/A	Specifies to clear dampening information of all routes.

Default None.

Command Mode Privileged mode.

Usage Guideline The **clear ip bgp dampening ipv4 unicast** command is used to clear stored route dampening information of IPv4 unicast address family sessions. If no keyword is specified, route dampening information of all routes in IPv4 unicast address family will be cleared.

Examples The following example clears route dampening information of 192.168.10.0/24 and restores suppressed routes in IPv4 unicast address family.

```
Switch# clear ip bgp dampening ipv4 unicast 192.168.10.0/24
Switch#
```

2-28 clear ip bgp flap-statistics vrf

To clear BGP route dampening flap statistics of IPv4 VRF address family sessions.

clear ip bgp flap-statistics vrf *VRF-NAME* **[{***IP-ADDRESS* **|** *NETWORK-ADDRESS***}]**

Syntax Description	
VRF-NAME	Specifies the name of VRF.
NETWORK-ADDRESS	(Optional) Specifies to only clear dampening flap statistics of the route match the network address.
IP-ADDRESS	(Optional) Specifies to only clear dampening flap statistics of the route match the IP address.

Default None.

Command Mode Privileged mode.

Usage Guideline This command is used to clear the accumulated penalties for routes that have been received on a router which has BGP dampening enabled of IPv4 VRF address family sessions. If **no** keyword is specified, flap statistics of all routes in IPv4 VRF address family will be cleared.

Examples This example shows how to clear the route dampening flap statistics of network 192.168.1.0/24 which in IPv4 VRF address family:

```
Switch# clear ip bgp flap-statistics vrf VPN-A 192.168.1.0/24
Switch#
```

2-29 clear ip bgp flap-statistics ipv4 unicast

To clear BGP route dampening flap statistics, use this command in privileged mode.

clear ip bgp flap-statistics ipv4 unicast [{*IP-ADDRESS* **|** *NETWORK-ADDRESS***}]**

Syntax Description	
NETWORK-ADDRESS	(Optional) Specifies to only clear dampening flap statistics of the route match the network address.
IP-ADDRESS	(Optional) Specifies to only clear dampening flap statistics of the route match the IP address.
N/A	Specify to clear dampening flap statistics of all routes.

Default None.

Command Mode Privileged mode.

Usage Guideline This command is used to clear the accumulated penalties for routes that have been received on a router which has BGP dampening enabled of IPv4 unicast address family sessions. If **no** keyword is specified, flap statistics of all routes in IPv4 unicast address family will be cleared.

Examples This example shows how to clear the route dampening flap statistics of network 192.168.1.0/24 which in IPv4 unicast address family:

```
Switch# clear ip bgp flap-statistics ipv4 unicast 192.168.1.0/24
Switch#
```

2-30 clear ip bgp external

To reset external Border Gateway Protocol (eBGP) peering sessions using hard or soft reconfiguration, use this command in privileged mode.

clear ip bgp external [soft [{in [prefix-filter] | out}]]

Syntax Description	
in	(Optional) Initiates inbound reconfiguration. If neither the in nor out keywords are specified, both inbound and outbound sessions are reset.
prefix-filter	(Optional) Clears the existing outbound route filter (ORF) prefix list to trigger a new route refresh or soft reconfiguration, which updates the ORF prefix list.
out	(Optional) Initiates inbound or outbound reconfiguration. If neither the in nor out keywords are specified, both inbound and outbound sessions are reset.
soft	(Optional) Initiates a soft reset. Does not tear down the session.

Default None.

Command Mode Privileged mode.

Usage Guideline The **clear ip bgp external** command can be used to initiate a hard reset or soft reconfiguration of eBGP neighbor sessions.

If a hard reset is applied to the inbound session, the inbound session will be torn down and the local inbound routing table and the remote outbound routing table will be cleared.

If a soft reset is applied to the inbound session, the session will not be rebuilt but the local inbound routing table will be cleared and needs to be rebuilt.

If a soft reconfiguration inbound is enabled, then the routing table can be rebuilt based on the stored route updates information. If a soft reconfiguration inbound is disabled, then the local router will send the route refresh request to the neighbor to ask for the route refresh.

When the inbound session is soft reset with the prefix filter option, and the capability orf prefix-list is enabled in the send direction, then the local BGP will send ‘clear the routing table’, and notify the remote neighbor for the prefix filter.

This is a way to notify the neighbor of the prefix filter whenever a change is made to the prefix filter.

Examples

The following example, a soft reconfiguration is configured for all inbound eBGP peering sessions:

```
Switch# clear ip bgp external soft in
Switch#
```

The following example will send prefix filter to neighbor and let neighbor re-advertisement BGP route base on new prefix filter. The **neighbor capability orf prefix-list** in the send direction need be configured, and that the local filter list in the inbound direction for the peer need be set.

```
Switch(config)#router bgp 100
Switch(config-router)#neighbor 172.16.10.1 remote-as 200
Switch(config-router)#neighbor 172.16.10.1 capability orf prefix-list send
Switch(config-router)#neighbor 172.16.10.1 filter-list myacl in
Switch(config-router)#end
Switch#clear ip bgp external soft in prefix-filter
Switch#
```

2-31 clear ip bgp flap-statistics

To clear BGP route dampening flap statistics, use this command in privileged mode.

clear ip bgp flap-statistics [{*IP-ADDRESS* **|** *NETWORK-ADDRESS***}]**

Syntax Description	
IP-ADDRESS	Specifies an IPv4 address to clear the dampening flap statistics.
NETWORK-ADDRESS	Specifies an IPv4 network to clear the dampening flap statistics.

Default None.

Command Mode Privileged mode.

Usage Guideline This command is used to clear the accumulated penalties for routes that have been received on a router which has BGP dampening enabled. If no arguments or keywords are specified, flap statistics are cleared all routes.

Examples This example shows how to clear the route dampening flap statistics of network 192.168.1.0/24:

```
Switch# clear ip bgp flap-statistics 192.168.1.0/24
Switch#
```

2-32 clear ip bgp peer-group

To reset Border Gateway Protocol (BGP) connections using hard or soft reconfiguration for all the members of a BGP peer group, use this command in privileged mode.

clear ip bgp peer-group [{vrf *VRF-NAME* **| vpnv4 }]***PEER-GROUP-NAME* **[soft [{in [prefix-filter] | out}]]**

Syntax Description	
PEER-GROUP-NAME	Peer group name. The maximum length is 16 characters.

vrf *VRF_NAME*	(Optional) Specifies a VRF name. The length of VRF-NAME is 12 characters.
vpnv4	(Optional) Specifies to reset the sessions of VPNv4 address family.
soft	(Optional) Initiates a soft reset. Does not tear down the session. If the soft keyword is not specified, all the sessions of the members of the peer group are reset.
in	(Optional) Initiates soft resetting for the inbound routing information.
prefix-filter	(Optional) Clears the existing outbound route filter (ORF) prefix list to trigger a new route refresh or soft reconfiguration, which updates the ORF prefix list.
out	(Optional) Initiates soft resetting for the outbound routing information.

Default None

Command Mode Privileged mode

Usage Guideline This command is used to initiate a hard reset or a soft reset for a set of connections. A hard reset tears down and rebuilds all the sessions for the members of the specified peer group and clears and rebuilds the local routing table. A soft reset only clears and rebuilds the local routing table.

To the soft reset, if **neighbor soft-reconfiguration inbound** is configured, the routing table can be rebuilt based on the stored route updates information, and if it doesn't, the local router will send the route refresh message to the neighbors to ask for the routes.

When the inbound session is soft reset with the **prefix-filter** option, and the **neighbor capability orf prefix-list** in the send direction is configured, the local BGP will send "clear the routing table", and notify the remote neighbor for the prefix filter.

When using the **clear ip bgp peer-group** *PEER-GROUP-NAM* command without soft parameter, BGP connection will be torn down, so the following log message will be generated.

[BGP(2):] BGP connection is normally closed (Peer:<ipaddress>)

Where the <ipaddress> is the address of the peer. After a while, the connection will be rebuilt, and the following log message will be generated.

[BGP(1):] BGP connection is successfully established Peer:<ipaddress>

Where the <ipaddress> is the address of the peer.

This is a way to notify the neighbor of the prefix filter whenever a change is made to the prefix filter.

Example

In the following example, all members of the BGP peer group named INTERNAL are reset:

```
Switch# clear ip bgp peer-group INTERNAL
Switch#
```

In the following example, a soft reconfiguration is initiated for both the inbound and outbound session with members of the peer group INTERNAL:

```
Switch# clear ip bgp peer-group INTERNAL soft
Switch#
```

When using the parameter **soft** with either **in** or **out**, the soft reconfiguration is only initiated for the inbound or outbound session.

Assume that the **neighbor capability orf prefix-list** in the send direction is configured, and that the local filter list in the inbound direction for the peer group is changed, using this command with parameters **soft in prefix-filter** to notify all the neighbors in the peer group.

```
Switch# clear ip bgp peer-group INTERNAL soft in prefix-filter
Switch#
```

2-33 debug ip bgp

Use this command to turn on BGP debug function. Use the **no** form of this command to turn off BGP debug function.

debug ip bgp

no debug ip bgp

Syntax Description None.

Default By default BGP debug function is turned off.

Command Mode Privileged mode

Usage Guideline Use this command to turn on BGP debug function while the global debug function has been turned on before.

Examples This example turns on BGP debug function:

```
Switch# debug ip bgp
Switch#
```

2-34 debug ip bgp fsm-event

Use this command to turn on BGP FSM event debug switch. Use the **no** form of this command to turn off BGP FSM event debug switch.

debug ip bgp fsm-event

no debug ip bgp fsm-event

Syntax Description None.

Default By default BGP FSM event debug switch is turned off.

Command Mode Privileged mode.

Usage Guideline Use this command to turn on BGP FSM event debug switch. When BGP FSM event happens, debug information will be print if BGP debug function is turned on.

Use the command **debug ip bgp** to turn on BGP debug function.

Examples This example turns on BGP FSM event debug switch:

```
Switch# debug ip bgp fsm-event
Switch#
10.1.1.4-Outgoing [FSM] AS-Origination Timer Expiry
33.33.33.33-Outgoing [FSM] Routeadv Timer Expiry
10.1.1.3-Outgoing [FSM] Routeadv Timer Expiry
```

2-35 debug ip bgp packet

Use this command to turn on BGP packet debug switch. Use the **no** form of this command to turn off BGP packet debug switch.

debug ip bgp packet {receive | send}

no debug ip bgp packet {receive | send}

Syntax Description	
receive	Turn on BGP received packet debug switch.
send	Turn on BGP sent packet debug switch.

Default By default BGP packet debug switch is turned off.

Command Mode Privileged mode.

Usage Guideline Use this command to turn on BGP packet debug switch. When BGP protocol packets are received or transmitted, debug information will be print if BGP debug function is turned on.

Use the command **debug ip bgp** to turn on BGP debug function.

Examples This example turns on BGP received packet debug switch:

```
Switch# debug ip bgp packet receive
Switch#
BGP:Peer:<100.1.1.2>,RCV UPDATE,withdraw,NLRI:<88.1.1.0/24>,<88.1.2.0/
24>,<88.1.3.0/24>,<88.1.4.0/24>,<88.1.5.0/24>
100.1.1.2-Outgoing [DECODE] Update: Withdrawn Len(20)
100.1.1.2-Outgoing [RIB] Withdraw: Prefix 88.1.1.0
BGP:Peer:<10.1.1.3>,RCV KEEPAVLIVE
10.1.1.3-Outgoing [DECODE] KAlive: Received!
BGP:Peer:<100.1.1.2>,RCV UPDATE,attr:<Orign:i,As-path:(null),Next-
hop:100.1.1.2>,NLRI:<88.1.1.0/24>,<88.1.2.0/24>,<88.1.3.0/24>,<88.1.4.0/
24>,<88.1.5.0/24>
100.1.1.2-Outgoing [DECODE] Update: NLRI Len(20)
100.1.1.2-Outgoing [RIB] Update: Received Prefix 88.1.1.0
```

2-36 debug ip bgp route-map

Use this command to turn on BGP route map debug switch. Use the **no** form of this command to turn off BGP route map debug switch.

debug ip bgp route-map

no debug ip bgp route-map

Syntax Description None.

Default By default BGP route map debug switch is turned off.

Command Mode Privileged mode.

Usage Guideline Use this command to turn on BGP route map debug switch. When route map is matching BGP route information, debug information will be print if BGP debug function is turned on.

Use the command **debug ip bgp** to turn on BGP debug function.

Examples This example turns on BGP route map debug switch:

```
Switch# debug ip bgp route-map
Switch#
Route-Map:<rmap-1>, Apply Suppressed Route, Neighbor <100.1.1.4, AFI/SAFI
1/1>, Prefix:<67.1.1.0/24> <Permit>
Route-Map:<rmap-2>, Apply Received route, Neighbor <100.1.1.2, AFI/SAFI 1/
1>,Prefix: <88.1.1.0/24> <Deny>
```

2-37 debug ip bgp prefix-list

Use this command to turn on BGP IP prefix list debug switch. Use the no form of this command to turn off BGP IP prefix list debug switch.

debug ip bgp prefix-list

no debug ip bgp prefix-list

Syntax Description None.

Default By default BGP IP prefix list debug switch is turned off.

Command Mode Privileged mode.

Usage Guideline Use this command to turn on BGP IP prefix list debug switch. When IP prefix list is matching BGP information, debug information will be print if BGP debug function is turned on.

Use the command **debug ip bgp** to turn on BGP debug function.

Examples This example turns on BGP IP prefix list debug switch:

```
Switch# debug ip bgp prefix-list
Switch#
Prefix-List:<prelist-1>, Apply Received route, Neighbor <100.1.1.2, AFI/
SAFI 1/1>, Prefix:<88.1.1.0/24> <Permit>
Prefix-List: ORF Apply Sent route, Neighbor <100.1.1.4, AFI/SAFI 1/1>,
Prefix:<88.1.1.0/24> <Deny>
Prefix-List:<prelist-1>, Apply Received route, Neighbor <100.1.1.2, AFI/
SAFI 1/1>, Prefix:<88.1.2.0/24> <Deny>
Prefix-List: ORF Apply Sent route, Neighbor <100.1.1.4, AFI/SAFI 1/1>,
Prefix:<67.1.1.0/24> <Permit>
Prefix-List: ORF Apply Sent route, Neighbor <100.1.1.4, AFI/SAFI 1/1>,
Prefix:<67.1.2.0/24> <Deny>
```

2-38 debug ip bgp show global

Use this command to show internal detail information about BGP.

debug ip bgp show global [{vrf *VRF-NAME* **| vpnv4}]**

Syntax Description	
vrf *VRF-NAME*	(Optional) Specifies a VRF name. The length of VRF-NAME is 12 characters.
vpnv4	Displays global parameters that in address family of VPN version 4.

Default None.

Command Mode Privileged mode.

Usage Guideline Use this command to check internal status and detail information of BGP. If there is no parameter when execute this command, that means show the IPv4 global information; If the parameter is vrf and following a specified vrf name that means show the specified vrf global information while the parameter is VPN version 4 that is to show the VPN version 4 address family global information.

Examples This example displays detail internal information about IPv4 address family BGP:

```
Switch# debug ip bgp show global

Following is the information for global debugging:

AS Number                                 : 1
Router ID                                 : 10.2.2.2
Cluster ID                                : 30.1.1.1
Confed ID                                 : 10
Confederation Peers                       : 65510 65511
Fast External Fallover                    : Disabled
Dampening Ability                         : Enable
Client to Client Ability                  : Enable
Cluster Peers                             :
1.1.1.2 group1
Aggregate Next_Hop_Check                  : Disabled
Default Local Preference                  : 100
Default HoldTime                          : 180
Default Keepalive                         : 60
Scan Time                                 : 60

BGP Active Flags:
BGP_CFLAG_COMPARE_ROUTER_ID
BGP_CFLAG_ASPATH_IGNORE

BGP Active AF-Flags   :  None
Note:  The address family is IPv4

BGP Active Redist-Flags:
Note: The address family is IPv4
Switch#
```

This example is to show the vrf named vrf-1 related global information:

```
Switch# debug ip bgp show global vrf vrf-1

Following is the information for global debugging:

AS Number                          : 100
Router ID                          : 20.20.20.20
Cluster ID                         : 0.0.0.0
Confed ID                          : 0
Confederation Peers                :
Fast External Fallover             : Enabled
Dampening Ability                  : Disabled
Client to Client Ability           : Enable
Cluster Peers:

Aggregate Next_Hop_Check           : Disabled
Default Local Preference           : 100
Default Holdtime                   : 180
Default Keepalive                  : 60
Scan Time                          : 60

BGP Active Flags:
BGP_CFLAG_COMPARE_ROUTER_ID
BGP_CFLAG_ASPATH_IGNORE

BGP Active AF-Flags   :  None
Note: The address family is IPv4 Unicast for VRF

BGP Active Redist-Flags:
Note: The address family is IPv4 for VRF

Switch#
```

This example is to show the VPNV4 address family global information:

```
Switch# debug ip bgp show global vpnv4

Following is the information for global debugging:
---------------------------------------------------

AS Number                          : 100
Router ID                          : 20.20.20.20
Cluster ID                         : 0.0.0.0
Confed ID                          : 0
Confederation Peers                :
Fast External Fallover             : Enabled
Dampening Ability                  : Disabled
Client to Client Ability           : Enable
Cluster Peers:

Aggregate Next_Hop_Check           : Disabled
Default Local Preference           : 100
Default Holdtime                   : 180
Default Keepalive                  : 60
Scan Time                          : 60

BGP Active Flags:
BGP_CFLAG_COMPARE_ROUTER_ID
BGP_CFLAG_ASPATH_IGNORE

BGP Active AF-Flags   :  None
Note:  The address family is VPNv4

BGP Active Redist-Flags:
Note: The address family is VPN

Switch#
```

2-39 debug ip bgp show neighbors

Use this command to show internal detail information about BGP neighbors.

debug ip bgp show neighbors [{vrf *VRF-NAME* **| vpnv4}]**

Syntax Description	
vrf *VRF-NAME*	(Optional) Specifies a VRF name. The length of VRF-NAME is 12 characters.
vpnv4	Displays neighbor parameters that in address family of vpnv4.

Default None.

Command Mode Privileged mode.

Usage Guideline Use this command to check internal status and detail information of BGP neighbors. If there is no parameter follow this command that means show neighbors which created in address family of ipv4 while parameter of vrf show neighbors which created in vrf view and vpnv4 is meant to show neighbors which active in address family of VPNV4.

Examples This example displays internal detail information about BGP neighbors:

```
Switch# debug ip bgp show neighbors

BGP neighbor: 10.1.1.3 (Internel Peer)
-----------------------------------------------
Session State : Enabled
Session Activity : Enabled
Peer Group : my
Remote AS : 1
Local AS : 1
Remote Router ID : 182.148.0.3
BGP State : Established (UP for 00:21:48)
Hold Time (Configured) : 180 Seconds
Hold Time  (Current Used) : 90 Seconds
Keepalive Interval (Configured) : 60 Seconds
Keepalive Interval (Current Used) : 30 Seconds
Advertisement Interval (Configured) : 0 Seconds
Advertisement Interval (Current Used) : 5 Seconds
AS Origination Interval (Configured) : 0 Seconds
AS Origination Interval (Current Used) : 15 Seconds
Connect Retry Interval (Configured) : 0 Seconds
Connect Retry Interval (Current Used) : 0 Seconds
EBGP Multihop : 255
Weight : 0
Update Source : loopback1
Next Hop Self : Disabled
Remove Private As : Disabled
Allowas In : Disabled
Address Family IPv4 Unicast
IPv4 Unicast : Advertised and Received
Soft Reconfiguration Inbound : Disabled
Community Sent to this Neighbor : None
Default Originate : Disabled
Outbound Route Filter (ORF) type (64) Prefix list:
        Send Mode : Disabled
        Receive Mode : Disabled
Pass Word: (null)
Prefix Count: 0
Send Prefix Count: 1
Prefix Max Count: 12000
Prefix Warning Threshold: 75
Prefix Max Warning: Disabled

Switch#
```

2-40 debug ip bgp show peer-group

Use this command to show internal detail information about BGP peer group.

debug ip bgp show peer-group [{vrf *VRF-NAME* **| vpnv4}]**

Syntax Description	
vrf *VRF-NAME*	(Optional) Specifies a VRF name. The length of VRF-NAME is 12 characters.
vpnv4	Displays peer group parameters that in address family of vpnv4.

Default None.

Command Mode Privileged mode.

Usage Guideline Use this command to check internal status and detail information of BGP peer group.

Examples This example displays internal detail information about BGP peer group:

```
Switch# debug ip bgp show peer-group

BGP Peer Group :local1
-------------------------------------------------------
Session State : Enabled
Session Activity : Enabled
Members : 10.1.1.3
Remote AS : Not Set
Holdtime Interval : 180 seconds
Keepalive Interval : 60 seconds
Advertisement Interval : 0 seconds
AS Origination Interval : 0 Seconds
Connect Retry Interval : 0 Seconds
EBGP Multihop : 255
Weight : 0
Update Source : loopback1
Next Hop Self : Disabled
Remove Private As : Disabled
Allowas In : Disabled
Soft Reconfiguration Inbound : Disabled
Community Sent to this Neighbor : None
Default Originate : Disabled
Capability ORF Prefix List : None
Pass Word: (null)
Prefix Max Count: 12000
Prefix Warning Threshold: 75
Prefix Max Warning: Disabled

Switch#
```

2-41 debug ip bgp show network

Use this command to show internal detail information about BGP network.

debug ip bgp show network [vrf *VRF-NAME*]

Syntax Description	
vrf *VRF-NAME*	(Optional) Specifies a VRF name. The length of VRF-NAME is 12 characters.

Default None.

Command Mode Privileged mode.

Usage Guideline Use this command to check internal status and detail information of BGP nework. If there is no other words following this command that is to show the IPv4 address family parameters about network while the VRF specified the vrf related networks to show.

Examples This example displays internal detail information about BGP network of address family of IPv4:

```
Switch# debug ip bgp show network

Network             Route Map
-------------       -----------
192.168.0.0/16      -
172.16.0.0/16       map1

Total Entries :2

Switch#
```

This example displays internal detail information about BGP network of specified vrf:

```
Switch# debug ip bgp show network vrf vrf-1

Network             Route Map
-------------       -----------
172.16.0.0/16       map1

Total Entries :1

Switch#
```

2-42 debug ip bgp show aggregate

Use this command to show internal detail information about BGP route aggregation.

debug ip bgp show aggregate [vrf *VRF-NAME*]

Syntax Description	
vrf *VRF-NAME*	(Optional) Specifies a VRF name. The length of VRF-NAME is 12 characters.

Default None.

Command Mode Privileged mode.

Usage Guideline Use this command to check internal status and detail information of BGP route aggregation. If there is no parameter following this command that is to show the aggregate information in address of IPv4 and parameter of VRF is to show the specified vrf aggregate information.

Examples This example displays internal detail information about BGP route aggregation:

```
Switch# debug ip bgp show aggregate

Network             Summary Only   As Set    Suppress Count
-------------       ------------   ------    --------------
1.0.0.0/8           NO             NO        0

Total Entries :1

Switch#
```

This example is to show the internal detail information about BGP route aggregate:

```
Switch# debug ip bgp show aggregate vrf vrf-1

Network             Summary Only   As Set    Suppress Count
-------------       ------------   ------    --------------
50.0.0.0/8          NO             NO        0
60.0.0.0/8          NO             NO        0

Total Entries :2
```

2-43 debug ip bgp show damp

Use this command to show internal detail information about BGP route damping.

debug ip bgp show damp [vrf *VRF-NAME***]**

Syntax Description	
vrf *VRF-NAME*	(Optional) Specifies a VRF name. The length of VRF-NAME is 12 characters.

Default None.

Command Mode Privileged mode.

Usage Guideline Use this command to check internal status and detailed information of BGP route damping. If no parameter is specified, this command will display IPv4 address family dampening information and VRF will display specified VRF related dampening information.

Examples This example displays internal detail information about BGP route damping of address family of IPv4:

```
Switch# debug ip bgp show damp

Route Map                          : NULL
Reach Half Life Time is            : 900 seconds
Reuse Value                        : 750
Suppress Value                     : 2000
Max Suppress Time                  : 3600 seconds
Unreach Half Life Time is          : 900 seconds
Reuse Index Size                   : 1024
Reuse List Size                    : 512
Reuse Offset                       : 279


Current dampened routes:
Damp Hinfo: 484d9be8
 index ptr event     penalty    binfo     rn
  f5 484d9be8   1    1392  484d9ad8   484d9a90
  f5 484d9b98   1    1392  484d9a00   484d99b8
  f5 484d8080   1    1392  484d9928   484d98e0
  f5 484d7fe8   1    1392  484d9808   484d9738
 Damp Reuse List Info:
reuse_index index  ptr penalty    flap   start_time  t_updated
suppress_time evt
Damp reuse Hinfo: 484d9be8
     245     1 484d9be8    5010          6        428            448 437  1
     245     2 484d9b98    5010          6        428            448 437  1
     245     3 484d8080    5010          6        428            448 437  1
     245     4 484d7fe8    5010          6        428            448 437  1


show BGP Damp  no reuse list info: 0
index ptr penalty flap  start_time  t_updated  suppress_time evt

Output truncated...
```

This example is to show the vrf vrf-1 related bgp dampening information:

```
Switch# debug ip bgp show damp vrf vrf-1

Route Map                           : NULL
Reach Half Life Time is             : 900 seconds
Reuse Value                         : 750
Suppress Value                      : 2000
Max Suppress Time                   : 3600 seconds
Unreach Half Life Time is           : 900 seconds
Reuse Index Size                    : 1024
Reuse List Size                     : 512
Reuse Offset                        : 1


Current dampened routes:

 Damp Reuse List Info:
reuse_index index  ptr penalty    flap   start_time  t_updated
suppress_time evt


show BGP Damp  no reuse list info: 0
index ptr penalty flap  start_time  t_updated  suppress_time evt

BGP Damp Decay List Info:
decay array size is 90.
Index  value
-----------
1      1
2      0.969663
3      0.940247
4      0.911722
5      0.884064
6      0.857244
7      0.831238
8      0.806021
9      0.781569
```

2-44 debug ip bgp show interface

Use this command to show internal detail information about BGP interface.

debug ip bgp show interface

Syntax Description None.

Default None.

Command Mode Privileged mode.

Usage Guideline Use this command to check internal status and detail information of BGP interface.

Examples This example displays internal detail information about BGP interface:

```
Switch# debug ip bgp show interface

Interface Information:
Name          index   network             Flags    Status      VRF
------        -----   ---------           -----    ------ ------------
System        0001    90.1.1.10/16        5        Up     None
n105          0002    105.1.1.10/16       5        Up     None
n107          0003    107.1.1.10/16       5        Up     vrf-2
n108          0004    108.1.1.10/16       5        Up     vrf-2
n109          0005    109.1.1.10/16       5        Up     vrf-2
n110          0006    110.1.1.10/16       5        Up     vrf-1
n124          0007    124.1.1.10/16       5        Down   None
n200          0008    200.1.1.10/16       5        Down   vrf-1
n201          0009    201.1.1.10/16       5        Down   vrf-2
n202          0010    0.0.0.0/0           5        Down   vrf-1
n200-2        0011    200.1.1.10/16       5        Down   vrf-2
loopback1     0267    10.10.10.10/32      d        Up     None

Switch#
```

2-45 debug ip bgp show timer

Use this command to show internal detail information about BGP timer.

debug ip bgp show timer

Syntax Description None.

Default None.

Command Mode Privileged mode.

Usage Guideline Use this command to check internal status and detail information of BGP timer.

Examples This example displays internal detail information about BGP timer:

```
Switch# debug ip bgp show timer

BGP timer Link:
 node           time        func
 --------    ------      --------
 4805071c       1     80c8f7d0
 48050700       1     80c8fa58
 48108db4       1     80c7d8b8
 4814a0bc       1     80c7d8b8
 4815748c       1     80c7d8b8
 481576d8       2     80ca6344
 48109000       2     80ca6344
 4814a308       2     80ca6344
 481576f4       2     80ca6528
 4810901c       2     80ca6528
 4814a324       2     80ca6528
 4816d470       2     80c9eb90
 4815e21c       2     80ca10f0
 481ba804       6     80c9ed04
 481aadf0       8     80c9ee78
 4816d454       9     80c9ed04
 481aae28      10     80c9eb90
 481aae0c      11     80c9ed04
 481ba7e8      12     80c9ee78
 4818231c      13     80c9ed04
 48182338      23     80c9eb90
 48182300      26     80c9ee78
 4805071c      31     80c8f7d0
 481576bc      32     80ca7264
 48108fe4      32     80ca7264
 4816d438      32     80c9ee78
 481ba7cc      66     80ca0cc4
 481822e4      73     80ca0cc4
 481aadd4      87     80ca0cc4
 4815e238     123     80ca0f0c
 4816d41c     128     80ca0cc4

Switch#
```

2-46 debug ip bgp show redistribution

Use this command to show internal detail information about BGP route redistribution.

debug ip bgp show redistribution [vrf *VRF-NAME*]

Syntax Description	
vrf *VRF-NAME*	(Optional) Specifies a VRF name. The length of VRF-NAME is 12 characters.

Default None.

Command Mode Privileged mode.

Usage Guideline Use this command to check internal status and detail information of BGP route redistribution. If there is no parameter following this command that is to show the IP V4 address family parameters about redistribution and VRF is to show the specified VRF related redistribution parameters.

Examples This example displays internal detail information about BGP route redistribution:

```
Switch# debug ip bgp show redistribution

Redistributed routes summary:
Network              Type      Next_hop
-------              ----     -------------
81.0.0.0/8          RIP      110.1.1.9
101.0.0.0/8         RIP      110.1.1.9
200.1.0.0/24        RIP      110.1.1.9

Total Entries: 3

Redist list information:
No redist list exist!

Switch#
```

2-47 debug ip bgp show as-path-access-list

Use this command to show internal detail information about BGP path access list.

debug ip bgp show as-path-access-list

Syntax Description None.

Default None.

Command Mode Privileged mode.

Usage Guideline Use this command to check internal status and detail information of BGP path access list.

Examples This example displays internal detail information about BGP path access list:

```
Switch# debug ip bgp show as-path-access-list

BGP AS Path Access List 1
deny (_64[6-9][0-9][0-9]_|_65[0-9][0-9][0-9]_)
permit 33

Total Entries: 1

Switch#
```

2-48 debug ip bgp show community-list

Use this command to show internal detail information about BGP community list.

debug ip bgp show community-list

Syntax Description None.

Default None.

Command Mode Privileged mode.

Usage Guideline Use this command to check internal status and detail information of BGP community list.

Examples This example displays internal detail information about BGP community list:

```
Switch# debug ip bgp show community-list

Community list:list1  standard
    permit   5000:100

Switch#
```

2-49 exit-address-family

Use this command to exit from the address family configuration mode and enter the router configuration mode.

exit-address-family

Syntax Description None.

Default None.

Command Mode Address family configuration (IPv4 Unicast, VPNv4 and VRF).

Usage Guideline None.

Example The following example show how to exit from the VPNv4 address family mode and enter the router configuration mode.

```
Switch(config-router)# address-family vpnv4
Switch(config-router-af)# neighbor 172.18.1.1 activate
Switch(config-router-af)# exit-address-family
Switch(config-router)#
```

2-50 ip as-path access-list

Use this command to define a BGP Autonomous System (AS) path access list or add an AS path access list entry to an existing AS path access list. Use the **no** form of this command to delete the access list or an entry of the AS path access list.

ip as-path access-list *ACCESS-LIST-NAME* **[{ permit | deny }** *REGEXP***]**

no ip as-path access-list *ACCESS-LIST-NAME* **[{ permit | deny }** *REGEXP***]**

Syntax Description	
ACCESS-LIST-NAME	Specifies the name of the access list. The maximum length is 16 characters.
permit	Permits access to the matching conditions.
deny	Denies access to the matching conditions.
REGEXP	Specifies a regular expression to match the BGP AS paths. The maximum length is 80 characters.

Default None

Command Mode Global configuration

Usage Guideline Use this command to configure an Autonomous System path access list. An Autonomous System path access list can be applied to inbound, outbound or both routes exchanging of a BGP peer session. If the regular expression matches the specified string represented the AS path of the route, the permit or deny condition applies.
Multiple entries can be applied to a list name.

Use the **show ip as-path access-list** command to verify your settings.

Example The following example defines an as-path access-list named *mylist* to deny routes with only AS number 65535:

```
Switch(config)#ip as-path access-list mylist deny ^65535$
Switch(config)#
```

The following example show how to delete an entry in an as-path access-list early configured:

```
Switch(config)#no ip as-path access-list mylist deny ^65535$
Switch(config)#
```

After that, the as-path access-list *mylist* has no entry, but it still exists.

The following example show how to delete an as-path access-list no matter whether it has entries or not:

```
Switch(config)#no ip as-path access-list mylist
Switch(config)#
```

2-51 ip community-list

Use this command to create a community list or add a community list entry to an existing community list. Use the **no** form of this command to delete the community list or one of its entries.

Standard Community Lists:

ip community-list standard *COMMUNITY-LIST-NAME* **[{ permit | deny }** *COMMUNITY***]**

no ip community-list standard *COMMUNITY-LIST-NAME* **[{ permit | deny }** *COMMUNITY***]**

Expanded Community Lists:

ip community-list expanded *COMMUNITY-LIST-NAME* **[{ permit | deny }** *REGEXP***]**

no ip community-list expanded *COMMUNITY-LIST-NAME* **[{ permit | deny }** *REGEXP***]**

Syntax Description

COMMUNITY-LIST-NAME	Specifies the community list-name. It can accept up to 16 characters. The syntax is general string that does not allow space.
permit	Permit access to the community list.
deny	Deny access to the community list.
COMMUNITY	Community is a 32-bit integer. It can be a user-specified number represented by AA:NN, where AA (AS number) is the upper part of the word and NN (community number, user-specified) is the lower part of the word It can also be one of the following reserved community: **internet :** Specifies routes are advertised to all peers (internal and external). **local-AS:** Specifies routes not to be advertised to external BGP peers. **no-advertise:** Specifies routes not to be advertised to other BGP peers. **no-export:** Specifies routes not to be advertised outside of Autonomous System boundary.
REGEXP	Configures a regular expression that is used to specify a pattern to match against an input string. Regular expressions can be used only with expanded community lists. The maximum length is 80 characters.

Default

BGP community exchange is disabled by default. It is enabled on a per-neighbor basis with the **neighbor send-community** command.

The **Internet** community is applied to all routes or prefixes by default, until any other community value is configured with this command or the set community command.

Command Mode Global configuration mode

Usage Guideline Use the community-lists to specify BGP community attributes. The community attribute is used for implementing policy routing. It is an optional, transitive attribute and facilitates transfer of local policies through different autonomous systems. It includes community values that are 32 bits long. All names of the standard community list and expended community list must not be the same.

This command can be applied multiple times. BGP community attributes exchanged between BGP peers are controlled by the neighbor send-community command.

If permit rules exist in a community list, routes with community that does not match any rule in the list will be denied. If there are no rules or only deny rules to be configured in the community list, all routes will be denied.

Use the **show ip community-list** command to verify your settings.

Example The following example defines a standard community list named *mycom* with an entry.

```
Switch(config)# ip community-list standard mycom deny no-export 20:30
Switch(config)#
```

The following example show how to delete an entry in a community list early configured:

```
Switch(config)#no ip community-list standard mycom deny no-export 20:30
Switch(config)#
```

After that, the community list mycom has no entry, but it still exists.
The following example show how to delete a community list no matter whether it has entries or not:

```
Switch(config)# no ip community-list standard mycom
Switch(config)#
```

The following example creates an expanded community list named myexpcom with an entry.

```
Switch(config)# ip community-list expanded myexpcom permit _20[0-9]
Switch(config)#
```

2-52 ip extcommunity-list

Use this command to create an extended community list or add an extended community entry to an existing extended community list for VPN route filtering. Use the **no** form of this command to delete the extended community list or remove one of its entries.

Standard IP Extended Community Lists:

ip extcommunity-list standard *EXTCOMMUNITY-LIST-NAME* **[{ permit | deny }** *EXTCOMMUNITY***]**

no ip extcommunity-list standard *EXTCOMMUNITY-LIST-NAME* **[{ permit | deny }** *EXTCOMMUNITY***]**

Expanded IP Extended Community Lists:

ip extcommunity-list expanded *EXTCOMMUNITY-LIST-NAME* **[{ permit | deny }** *REGEXP***]**

no ip extcommunity-list expanded *EXTCOMMUNITY-LIST-NAME* **[{ permit | deny }** *REGEXP***]**

Syntax Description	
EXTCOMMUNITY-LIST-NAME	Specifies the extended community list-name. It can accept up to 16 characters. The syntax is general string that does not allow space.
permit	(Optional) Specify the extended community to accept.
deny	(Optional) Specifies the extended community to reject.
EXTCOMMUNITY	(Optional) Consists of a set of rt VALUE or soo VALUE. It can accept 12 VALUEs totally for one entry. There are two different types for the rt value or soo value: IP address: number: The IP address should be a global IP address that is assigned to the user and the number is assigned from a numbering space that is administered by the user. The number can be 1-65535. AS Number: number: The AS Number should be a public AS Number (Both 2-bytes AS number and 4-bytes AS number works) that is assigned to the user and the number is assigned from a numbering space that is administered by the user. The number can be 1-4294967295 for 2-bytes AS number and 1-65535 for 4-bytes AS number.
REGEXP	(Optional) Configures a regular expression that is used to specify a pattern to match against an input string. Regular expressions can be used only with expanded community lists. The maximum length is 80 characters.

Default BGP extended community exchange is disabled by default. It is enabled on a per-neighbor basis with the **neighbor send-community** command.

Command Mode Global configuration.

Usage Guideline

The extended community attribute is used for implementing policy routing. It is an optional, transitive attribute and facilitates transfer of local policies through different autonomous systems. All names of the standard extcommunity list and expended extcommunity list must not be the same.

This command can be applied multiple times. BGP extended community attributes exchanged between BGP peers are controlled by the **neighbor send-community** command.

If permit rules exist in an extended community list, routes with extended community that does not match any rule in the list will be denied. If there are no rules or only deny rules to be configured in the extended community list, all routes will be denied.

Use the **show ip extcommunity-list** command to verify your settings.

Example

The following example defines a standard extended community list named myecom with an entry.

```
Switch(config)# ip extcommunity-list standard myecom permit rt 1:1 soo
1.1.1.1:1
Switch(config)#
```

The following example show how to delete an entry in an extended community list early configured:

```
Switch(config)#no ip extcommunity-list standard myecom permit rt 1:1 soo
1.1.1.1:1

Switch(config)#
```

After that, the community list myecom has no entry, but it still exists.

The following example show how to delete an extended community list no matter whether it has entries or not:

```
Switch(config)# no ip extcommunity-list standard myecom
Switch(config)#
```

The following example creates an expanded extended community list named myexpcom with an entry.

```
Switch(config)# ip extcommunity-list expanded myexpcom permit _20[0-9]
Switch(config)#
```

2-53 neighbor activate

Use this command to enable the exchange of information with a Border Gateway Protocol (BGP) neighbor. Use the **no** form of this command to disable the exchange of information with a BGP neighbor.

neighbor { *IP-ADDRESS* **|** *PEER-GROUP-NAME***} activate**

no neighbor { *IP-ADDRESS* **|** *PEER-GROUP-NAME* **} activate**

Syntax Description	
IP-ADDRESS	Specifies IP address of BGP peer.
PEER-GROUP-NAME	Name of a Border Gateway Protocol (BGP) peer group. The maximum length is 16 characters.

Default

The exchange of addresses with BGP neighbors is enabled for the IPv4 unicast address family and is disabled for the VPNv4 address family if the default IPv4 unicast is enabled.

The exchange of addresses with BGP neighbors is disabled for both the IPv4 unicast address family and VPNv4 address family if the default IPv4 unicast is disabled.

Command Mode

Router configuration mode.

Address family configuration mode (IPv4 Unicast, VPNv4 and VRF).

Usage Guideline

If you specify a BGP peer group by using the *PEER-GROUP-NAME* argument, all the members of the peer group will inherit the characteristic configured with this command. It is not allowed to disable the active of a peer group.
When using the **no** form of this command, the exchange of addresses with BGP neighbor is disabled for the IPv4 address family, and the connection will be torn down, so the following log message will be generated:

[BGP(2):] BGP connection is normally closed (Peer:<ipaddress>)

where the <ipaddress> is the address of the peer.

Use the **show ip bgp neighbors** or **show ip bgp peer-group** command to verify your settings.

Example

The following example shows how to disable address exchange for neighbor 10.4.4.4:

```
Switch(config)#router bgp 65100
Switch(config-router)#neighbor 10.4.4.4 remote-as 65101
Switch(config-router)#no neighbor 10.4.4.4 activate
Switch(config-router)#
```

2-54 neighbor advertisement-interval

Use this command to set the minimum interval between sending Border Gateway Protocol (BGP) routing updates. Use the **no** command to return to the default configuration.

neighbor { *IP-ADDRESS* **|** *PEER-GROUP-NAME***} advertisement-interval** *SECONDS*

no neighbor { *IP-ADDRESS* **|** *PEER-GROUP-NAME* **} advertisement-interval**

Syntax Description	
IP-ADDRESS	Specifies IP address of BGP peer.
PEER-GROUP-NAME	Name of a Border Gateway Protocol (BGP) peer group. The maximum length is 16 characters.
SECONDS	The interval, in seconds, between the sending of UPDATE messages. The range is from 0 to 600. If this value is set to zero, the update or withdrawn message will be sent immediately.

Default By default, it is 30 seconds for external peers and 5 seconds for internal peers.

Command Mode Router configuration mode.

Address family configuration mode (VRF).

Usage Guideline If you specify a BGP peer group by using the *PEER-GROUP-NAME* argument, all the members of the peer group will inherit the characteristic configured with this command.

Use the **show ip bgp neighbors** or **show ip bgp peer-group** command to verify your settings.

Example The following example sets the minimum time interval between sending BGP routing updates to 15 seconds:

```
Switch(config)#router bgp 65100
Switch(config-router)#neighbor 10.4.4.4 remote-as 65101
Switch(config-router)#neighbor 10.4.4.4 advertisement-interval 15
Switch(config-router)#
```

2-55 neighbor allowas-in

Use this command to enable routers to allow its own AS appearing in the received BGP update packets. To disable duplicate AS number, use the **no** form of this command.

neighbor { *IP-ADDRESS* **|** *PEER-GROUP-NAME***} allowas-in [***NUMBER***]**

no neighbor { *IP-ADDRESS* **|** *PEER-GROUP-NAME* **} allowas-in**

Syntax Description	
IP-ADDRESS	Specifies IP address of BGP peer.
PEER-GROUP-NAME	Name of a Border Gateway Protocol (BGP) peer group. The maximum length is 16 characters.
NUMBER	(Optional) Specifies the maximum number of local AS to allow appearing in the AS-path attribute of the update packets. The value is from 1 to 10. If no number is supplied, the default value of 3 times is used.

Default Disabled

Command Mode Router configuration.

Address family configuration (IPv4 Unicast, VPNv4 and VRF).

Usage Guideline The BGP router will do AS path loop checks for the received BGP update packets. If the BGP router's own AS appears in the AS path list, it is identified as a loop and the packets will be discarded. If the allowas-in setting is enabled, the BGP router's own AS is allowed in the AS path list.

Use the **show ip bgp neighbors** or **show ip bgp peer-group** command to verify your settings.

Example The following example shows how to set the number of times of the local router's own AS to allow appearing in the update packets received from the neighbor 100.16.5.4 to 5:

```
Switch(config)#router bgp 65100
Switch(config-router)#neighbor 100.16.5.4 remote-as 65101
Switch(config-router)#neighbor 100.16.5.4 allowas-in 5
Switch(config-router)#
```

The following example can set the **allowas-in** to 3 without the *NUMBER* parameter:

```
Switch(config)#router bgp 65100
Switch(config-router)#neighbor 100.16.5.4 remote-as 65101
Switch(config-router)#neighbor 100.16.5.4 allowas-in
Switch(config-router)#
```

2-56 neighbor as-override

Use this command to enable to override the AS number of a site with the provider's AS number on a PE router. Use the **no** form of the command to disable this function.

neighbor {*IP-ADDRESS* **|** *PEER-GROUP-NAME***} as-override**

no neighbor {*IP-ADDRESS* **|** PEER-GROUP-NAME**} as-override**

Syntax Description	
IP-ADDRESS	Specifies IP address of the peer.
PEER-GROUP-NAME	Specify the name of the peer group.

Default Disabled.

Command Mode Address family configuration (VRF).

Usage Guideline The command is used to prevent routing loops between routers within a VPN.

In the VPN, the most typical application lies in that the two CE ends have the same AS number. Normally, these two CE routers can't receive the other from the other party, because the BGP protocol will not receive the route information with the same AS number in AS path attribute as the AS of BGP instance itself. After the above command is configured on the PE router, you can let the PE replace the AS number of the CE to AS number of PE self, so that the CE from the other end can receive the route information. Only set this function for the EBGP peer.

Use the **show ip bgp neighbors** or **show ip bgp peer-group** command to verify your settings.

Example This example shows how to enable AS override flag of BGP peer 3.3.3.3 in VRF vpn1.

```
Switch# configure terminal
Switch# router bgp 10
Switch(config-router)# address-family ipv4 vrf vpn1
Switch(config-router-af)# neighbor 3.3.3.3 remote-as 20
Switch(config-router-af)# neighbor 3.3.3.3 as-override
```

2-57 neighbor capability orf prefix-list

Use this command to advertise outbound router filter (ORF) capabilities to a peer or a peer group. Use the **no** form of this command to disable ORF capabilities.

neighbor { *IP-ADDRESS* **|** *PEER-GROUP-NAME***} capability orf prefix-list {receive | send | both}**

no neighbor { *IP-ADDRESS* **|** *PEER-GROUP-NAME* **} capability orf prefix-list {receive | send | both}**

Syntax Description	
IP-ADDRESS	Specifies IP address of BGP peer.
PEER-GROUP-NAME	Name of a Border Gateway Protocol (BGP) peer group. The maximum length is 16 characters.
receive	Enables the ORF capability in receive mode.
send	Enables the ORF capability in send mode.
both	Enables the ORF capabilities in both receive and send modes.

Default No ORF capabilities are advertised to a peer router.

Command Mode Router configuration.

Address family configuration (IPv4 Unicast, VPNv4 and VRF).

Usage Guideline The BGP Outbound Route Filter (ORF) Capability allows one BGP router to install its configured inbound prefix list filter on to the remote BGP router. This is used for reducing the amount of unwanted routing updates from the remote peer.

When using this command, BGP connection will be torn down, so the following log message will be generated.

[BGP(2):] BGP connection is normally closed (Peer:<ipaddress>)

Where the <ipaddress> is the address of the peer. After a while, the connection will be rebuilt, and the following log message will be generated.

[BGP(1):] BGP connection is successfully established Peer:<ipaddress>

Where the <ipaddress> is the address of the peer.

Use the **show ip bgp neighbors** or **show ip bgp peer-group** command to verify your settings.

Example The following example shows how to configure the router to advertise ORF.

Assume there are two routers, R1 (10.90.90.90) and R2 (10.1.1.1). R2 has two BGP routes, 172.18.1.0/24 and 172.19.1.0/24. R1 only want to receive 172.18.0.0/16, and then it can notify to R2 its willingness though ORF.

On router R1, configure an ip prefix-list named *myorf* firstly:

```
R1# configure terminal
R1(config)# ip prefix-list myorf permit 172.18.0.0/16 le 32
R1(config)#
```

Then, set routing policy to R2, and advertise the ORF to R2:

```
R1(config)#router bgp 10
R1(config-router)#neighbor 10.1.1.1 remote-as 1
R1(config-router)# neighbor 10.1.1.1 prefix-list myorf in
R1(config-router)#neighbor 10.1.1.1 capability orf prefix-list send
R1(config-router)#
```

On router R2, advertise its ORF capability in receive direction to R1.

```
R2(config)#router bgp 1
R2(config-router)#neighbor 10.90.90.90 remote-as 10
R2(config-router)#neighbor 10.90.90.90 capability orf prefix-list receive
R2(config-router)#
```

2-58 neighbor default-originate

To allow a BGP speaker (the local router) to send the default route 0.0.0.0 to a neighbor for use as a default route, use this command in router configuration mode. To send no route as a default, use the **no** form of this command.

neighbor {*IP-ADDRESS* **|** *PEER-GROUP-NAME***} default-originate [route-map** *MAP-NAME***]**

no neighbor {*IP-ADDRESS* **|** *PEER-GROUP-NAME***} default-originate**

Syntax Description	
IP-ADDRESS	Specifies IP address of BGP peer.
PEER-GROUP-NAME	Name of a Border Gateway Protocol (BGP) peer group. The maximum length is 16 characters.
MAP-NAME	(Optional) Name of the route map. The length is up to 16 characters. The route map allows route 0.0.0.0 to be injected conditionally.

Default No default route is sent to the neighbor.

Command Mode Router configuration.

Address family configuration (IPv4 Unicast and VRF).

Usage Guideline This command allows a BGP speaker (the local router) to send the default route 0.0.0.0/0 to a specified neighbor to use as its default route. If route map is specified, the default route will be injected if the route map contains a match IP address statement.

Use the **show ip bgp neighbors** or **show ip bgp peer-group** command to verify your settings.

Example The following example show how to advertisement BGP default route to neighbor 172.16.2.3 unconditionally:

```
Switch(config)# router bgp 10
Switch(config-router)# neighbor 172.16.2.3 remote-as 20
Switch(config-router)# neighbor 172.16.2.3 default-originate
```

The following example show how to advertisement BGP default route to neighbor 172.16.22.32 and set weight to 2000.

Create a route-map name as mymap and set entry:

```
Switch(config)# route-map mymap permit 1
Switch(config-route-map)# set weight 2000
Switch(config-route-map)#exit
```

Configure BGP neighbor to use route-map mymap as default originate filter:

```
Switch(config)# router bgp 1
Switch(config-router)# neighbor 172.16.22.32 remote-as 2
Switch(config-router)# neighbor 172.16.22.32 default-originate route-map
mymap
Switch(config-router)#exit
```

2-59 neighbor description

Use this command to associate a description with a neighbor or a peer group. Use the **no** form of this command to remove the description.

neighbor { *IP-ADDRESS* **|** *PEER-GROUP-NAME* **} description** *DESC*

no neighbor { *IP-ADDRESS* **|** *PEER-GROUP-NAME* **} description**

Syntax Description	
IP-ADDRESS	Specifies IP address of BGP peer.
PEER-GROUP-NAME	Name of a Border Gateway Protocol (BGP) peer group. The maximum length is 16 characters.
DESC	Specifies a descriptive string for the neighbor. The maximum length is 80 characters. The syntax is general string that allows space.

Default There is no description.

Command Mode Router configuration.

Address family configuration (VRF).

Usage Guideline If you specify a BGP peer group by using the *PEER-GROUP-NAME* argument, all the members of the peer group will inherit the characteristic (description) configured with this command.

Use the **show ip bgp neighbors** or **show ip bgp peer-group** command to verify your settings.

Example The following example shows how to configure a description for the neighbor 172.16.10.10:

```
Switch(config)#router bgp 65100
Switch(config-router)#neighbor 172.16.10.10 remote-as 65101
Switch(config-router)#neighbor 172.16.10.10 description ABC in China
Switch(config-router)#
```

2-60 neighbor ebgp-multihop

This command is used to set the TTL of the BGP connections to external peers or peer-groups that are not directly connected. Use the **no** form of this command to return to the default.

neighbor { *IP-ADDRESS* **|** *PEER-GROUP-NAME* **} ebgp-multihop [***NUMBER***]**

no neighbor { *IP-ADDRESS* **|** *PEER-GROUP-NAME* **} ebgp-multihop**

Syntax Description	
IP-ADDRESS	Specifies IP address of BGP peer.
PEER-GROUP-NAME	Name of a Border Gateway Protocol (BGP) peer group. The maximum length is 16 characters.
NUMBER	(Optional) Value of TTL, range from 1 to 255. If it is not specified, the value is 255.

Default By default, the hop value for EBGP neighbor is 1.

Command Mode Router configuration.

Address family configuration (VRF).

Usage Guideline If you specify a BGP peer group by using the PEER-GROUP-NAME argument, all the members of the peer group will inherit the characteristic configured with this command

Use the **show ip bgp neighbors** or **show ip bgp peer-group** command to verify your settings.

Example The following example shows how to set the value of **ebgp-multihop** in order to connect to the neighbor 172.16.10.10, which resides on a network that is not directly connected:

```
Switch(config)#router bgp 65100
Switch(config-router)#neighbor 172.16.10.10 remote-as 65101
Switch(config-router)# neighbor 172.16.10.10 ebgp-multihop 5
Switch(config-router)#
```

The following example can set the **ebgp-multihop** to 255 without the *NUMBER* parameter:

```
Switch(config)#router bgp 65100
Switch(config-router)#neighbor 172.16.10.10 remote-as 65101
Switch(config-router)# neighbor 172.16.10.10 ebgp-multihop
Switch(config-router)#
```

2-61 neighbor filter-list

Use this command to set up a BGP filter. Use the **no** command to disable this function.

neighbor { *IP-ADDRESS* **|** *PEER-GROUP-NAME* **} filter-list** *ACCESS-LIST-NAME* **{in|out}**

no neighbor { *IP-ADDRESS* **|** *PEER-GROUP-NAME* **} filter-list {in|out}**

Syntax Description	
IP-ADDRESS	Specifies IP address of BGP peer.
PEER-GROUP-NAME	Name of a Border Gateway Protocol (BGP) peer group. The maximum length is 16 characters.
ACCESS-LIST-NAME	The name of an autonomous system path access list. You define this access list with the **ip as-path access-list** command.
in	Filter list is applied to incoming advertisements from that neighbor.
out	Filter list is applied to outgoing advertisements to that neighbor.

Default No filter is used.

Command Mode Router configuration.

Address family configuration (IPv4 Unicast, VPNv4 and VRF).

Usage Guideline This command specifies an access list filter on updates based on the BGP autonomous system paths. Each filter is an as-path access list based on regular expressions.

If the filter list doesn't exist, it will permit all. And if the filter list does exist but has no filter entry, it means deny any.

Each neighbor can only have one inbound and one outbound access list.

Use the **show ip bgp neighbors** or **show ip bgp peer-group** command to verify your settings.

Example The following example shows how to configure the BGP neighbor 172.16.1.1 not to sent advertisements about any path through or from the adjacent autonomous system 123:

Firstly, create an ip as-path access-list named *myacl*:

```
Switch# configure terminal
Switch(config)#ip as-path access-list myacl deny _123_
Switch(config)#ip as-path access-list myacl deny ^123$
Switch(config)#ip as-path access-list myacl permit .*
Switch(config)#
```

Then, set the routing policy to neighbor 172.16.1.1:

```
Switch(config)#router bgp 65100
Switch(config-router)#neighbor 192.168.6.6 remote-as 123
Switch(config-router)#neighbor 172.16.1.1 remote-as 65200
Switch(config-router)#neighbor 172.16.1.1 filter-list myacl out
Switch(config-router)#
```

2-62 neighbor maximum-prefix

Use this command to control how many prefixes can be received from a neighbor. Use the **no** form of this command to return to the default value.

neighbor {*IP-ADDRESS* **|** *PEER-GROUP-NAME***} maximum-prefix** *MAXIMUM* **[***THRESHOLD***] [warning-only]**

no neighbor {*IP-ADDRESS* **|** *PEER-GROUP-NAME***} maximum-prefix**

Syntax Description	
IP-ADDRESS	Specifies IP address of BGP peer.
PEER-GROUP-NAME	Name of a Border Gateway Protocol (BGP) peer group. The maximum length is 16 characters.
MAXIMUM	Maximum number of prefixes allowed from the specified neighbor. The number of prefixes that can be configured is limited only by the available system resources on a router.
THRESHOLD	(Optional) Integer specifying at what percentage of the maximum-prefix limit the router starts to generate a warning message. The range is from 1 to 100; the default is 75.
warning-only	(optional) Allows the router to generate a sys-log message when the maximum-prefix limit is exceeded, instead of terminating the peering session.

Default

The default maximum number of prefix is determined by project. For example, the default MAXIMUM value is12000 in project DGS3620.

Peering sessions are disabled when the maximum number of prefixes is exceeded.

THRESHOLD: 75 percent

Command Mode

Router configuration.

Address family configuration (IPv4 Unicast, VPNv4 and VRF).

Usage Guideline

When the number of received prefixes exceeds the maximum number configured, BGP disables the peering session (by default). You can use the **clear ip bgp** command to reestablish the session. If the **warning-only** keyword is configured, BGP sends only a log message and continues to peer with the sender.

Use the **show ip bgp neighbors** or **show ip bgp peer-group** command to verify your settings.

Example

In the following example, the maximum prefixes that will be received from the 192.168.1.1 neighbor are set to 10000.

```
Switch(config)#router bgp 40000
Switch(config-router)#neighbor 192.168.1.1 remote-as 30000
Switch(config-router)#neighbor 192.168.1.1 maximum-prefix 10000
Switch(config-router)#
```

The following example set the maximum prefixes to 10000, and set the local router to generate a log message instead of terminate the session when the maximum-prefix limit is exceeded:

```
Switch(config)#router bgp 40000
Switch(config-router)#neighbor 192.168.1.1 remote-as 30000
Switch(config-router)#neighbor 192.168.1.1 maximum-prefix 10000 warning-
only
Switch(config-router)#
```

2-63 neighbor next-hop-self

Use this command to configure the router as the next hop for a BGP-speaking peer or a peer group. To disable this feature, use the **no** form of this command.

neighbor {*IP-ADDRESS* **|** *PEER-GROUP-NAME***} next-hop-self**

no neighbor {*IP-ADDRESS* **|** *PEER-GROUP-NAME***} next-hop-self**

Syntax Description	
IP-ADDRESS	Specifies IP address of BGP peer.
PEER-GROUP-NAME	Name of a Border Gateway Protocol (BGP) peer group. The maximum length is 16 characters.

Default This command is disabled by default.

Command Mode Router configuration.

Address family configuration (IPv4 Unicast, VPNv4 and VRF).

Usage Guideline This command is useful in unmeshed networks (such as Frame Relay or X.25) where BGP neighbors may not have direct access to all other neighbors on the same IP subnet.

If a neighbor belongs to a peer group, you can only configure the **next-hop-self** from the peer group.

Use the **show ip bgp neighbors** or **show ip bgp peer-group** command to verify your settings.

Example The following example forces all updates destined for 10.108.1.1 to advertise this router as the next hop:

```
Switch(config)#router bgp 40000
Switch(config-router)#neighbor 10.108.1.1 remote-as 30000
Switch(config-router)#neighbor 10.108.1.1 next-hop-self
Switch(config-router)#
```

2-64 neighbor password

Use this command to enable Message Digest 5 (MD5) authentication and set the password on a TCP connection between two BGP peers. To disable this function, use the **no** form of this command.

neighbor {*IP-ADDRESS* **|** *PEER-GROUP-NAME***} password** *PASSWORD*

no neighbor {*IP-ADDRESS* **|** *PEER-GROUP-NAME***} password**

Syntax Description	
IP-ADDRESS	Specifies IP address of BGP peer.
PEER-GROUP-NAME	Name of a Border Gateway Protocol (BGP) peer group. The maximum length is 16 characters.
PASSWORD	Case-sensitive password of up to 25 characters. Set the MD5 authentication password when the TCP connection between BGP neighbors is established.

Default Disabled

Command Mode Router configuration.

Address family configuration (VRF).

Usage Guideline This command is used to configure the password for a BGP neighbor or BGP peer group. The password setting will cause TCP connections between the peers to restart with MD5 authentication. The same password need be configured between peers, otherwise the TCP connection will fail. A password can use special characters, such as ~!@#$%^&*()-_=+|\}]{[“':;/><.,?, The maximum length of the password is 25 characters.

When using this command, BGP connection will be torn down, so the following log message will be generated.

[BGP(2):] BGP connection is normally closed (Peer:<ipaddress>)

Where the <ipaddress> is the address of the peer. After a while, the connection will be rebuilt if both the BGP speakers are configured the same password, and the following log message will be generated.

[BGP(1):] BGP connection is successfully established Peer:<ipaddress>

Where the <ipaddress> is the address of the peer.

Use the **show ip bgp neighbors** or **show ip bgp peer-group** command to verify your settings.

Example The following example shows how to set the password of the BGP neighbor 10.2.2.2 to “abc”:

```
Switch(config)#router bgp 40000
Switch(config-router)#neighbor 10.2.2.2 remote-as 30000
Switch(config-router)#neighbor 10.2.2.2 password abc
Switch(config-router)#
```

2-65 neighbor peer-group (add group member)

Use this command to add a neighbor in a peer group. Use the **no** command to remove a neighbor in a peer group.

neighbor *IP-ADDRESS* **peer-group** *PEER-GROUP-NAME*

no neighbor *IP-ADDRESS* **peer-group** *PEER-GROUP-NAME*

Syntax Description	
IP-ADDRESS	Specifies IP address of BGP peer.
PEER-GROUP-NAME	Name of a Border Gateway Protocol (BGP) peer group. The maximum length is 16 characters.

Default None.

Command Mode Router configuration.

Address family configuration (IPv4 Unicast, VPNv4 and VRF).

Usage Guideline The neighbor at the specified IP address inherits all the configuration of the peer group. The members of a peer group must all be internal or external. If all the members of the BGP peer group are external, they are allowed to have different AS numbers.

There are two kinds of peer groups. For one kind, the remote AS is not set. Members must be created with **remote-as** parameter before adding to the peer group. After a neighbor is added to the peer group, there is no influence to its remote AS if we then configure the peer group's remote AS. For the other kind, the peer group has been set a remote AS number. A neighbor can be added to the peer group with no remote AS. In this situation, it inherits the peer group's remote AS automatically, and its remote AS changes with the changing of peer group's remote AS.

If a BGP peer belongs to a peer group, some attributes or actions can only be configured from the peer group. The following is a list of them:

capability-of-prefix-list
next-hop-self
route-reflector-client
send-community
soft-reconfiguration-inbound
remove-private-as
allowas-in
holdtime
keepalive
unsuppress-map
filter-list for out direction
route-map for out direction
prefix-list for out direction

as-override
soo

On the contrary, some attributes or actions are allowed to be configured from both the peer group and the member. If they are configured from the member, the setting will overwrite the setting configured from the peer group.

Other attributes that can be set from an individual peer are as follows:

description,
filter-list for in direction,
route-map for in direction,
prefix-list for in direction,
ebgp-multihop,
shutdown,
activate,
weight.
default-originate.
update-source.

As for the above attributes, setting the attribute of a peer group will automatically affect the setting for individual peers in the peer group.

If a BGP neighbor has already been the established state before using this command, BGP connection will be torn down, so the following log message will be generated.

[BGP(2):] BGP connection is normally closed (Peer:<ipaddress>)

Where the <ipaddress> is the address of the peer. After a while, the connection will be rebuilt, and the following log message will be generated.

[BGP(1):] BGP connection is successfully established Peer:<ipaddress>

Where the <ipaddress> is the address of the peer.

Use the **show ip bgp peer-group** command to verify your settings.

Example

The following example show how to add an existing peer 172.16.1.1 to a peer group named *DLINK.*

```
Switch(config)#router bgp 40000
Switch(config-router)#neighbor DLINK peer-group
Switch(config-router)#neighbor 172.16.1.1 remote-as 30000
Switch(config-router)#neighbor 172.16.1.1 peer-group DLINK
Switch(config-router)#
```

The following example show how to add a new peer 172.16.1.2 to the peer group *DLINK*, in which case the peer group must be configured the remote-as first.

```
Switch(config)#router bgp 40000
Switch(config-router)#neighbor DLINK peer-group
Switch(config-router)#neighbor DLINK remote-as 30000
Switch(config-router)#neighbor 172.16.1.2 peer-group DLINK
Switch(config-router)#
```

2-66 neighbor peer-group (create group)

Use this command to create a peer group. Use the **no** form of this command to delete a peer group

neighbor *PEER-GROUP-NAME* **peer-group**

no neighbor *PEER-GROUP-NAME* **peer-group**

Syntax Description	
PEER-GROUP-NAME	Name of a Border Gateway Protocol (BGP) peer group. The maximum length is 16 characters.

Default No default peer group

Command Mode Router configuration.

Address family configuration (VRF).

Usage Guideline Use this command to gather a set of neighbors for simplifying configuration. The remote AS must specified by using the **neighbor** *PEER-GROUP-NAME* **remote-as** *AS-NUMBER* command.

Use the **show ip bgp peer-group** command to verify your settings.

Example This example shows how to create a peer group named *DLINK-GROUP*.

```
Switch(config)#router bgp 65100
Switch(config-router)#neighbor DLINK-GROUP peer-group
```

2-67 neighbor prefix-list

Use this command to set a routing policy to a specified peer or a peer group based on the prefix list. To remove a prefix list, use the **no** form of this command.

neighbor {*IP-ADDRESS* **|** *PEER-GROUP-NAME***} prefix-list** *PREFIX-LIST-NAME* **{in | out}**

no neighbor { *IP-ADDRESS* **|** *PEER-GROUP-NAME* **} prefix-list {in | out}**

Syntax Description	
IP-ADDRESS	Specifies IP address of BGP peer.
PEER-GROUP-NAME	Name of a Border Gateway Protocol (BGP) peer group. The maximum length is 16 characters.
PREFIX-LIST-NAME	Name of a prefix list. The length is up to 16 characters.
in	Filter list is applied to incoming advertisements from that neighbor.
out	Filter list is applied to outgoing advertisements to that neighbor.

Default All external and advertised address prefixes are distributed to BGP neighbor.

Command Mode Router configuration.

Address family configuration (IPv4 Unicast, VPNv4 and VRF).

Usage Guideline The command is used to configure the filter related setting for a BGP neighbor or a peer group based on the prefix list.

If the prefix list doesn't exist or the prefix list does exist but has no filter entry defined, it will permit all.

Use the **show ip bgp neighbors** or **show ip bgp peer-group** command to verify your settings.

Example The following example shows how to configure the BGP neighbor 172.18.1.1 to apply the prefix list named myprefix to incoming advertisements:

Firstly, create an ip prefix-list named *myprefix*:

```
Switch# configure terminal
Switch(config)# ip prefix-list myprefix permit 172.20.0.0/16 le 32
Switch(config)#
```

Then, set the routing policy to neighbor 172.18.1.1:

```
Switch(config)#router bgp 65100
Switch(config-router)#neighbor 172.18.1.1 remote-as 65200
Switch(config-router)#neighbor 172.18.1.1 prefix-list myprefix in
Switch(config-router)#
```

2-68 neighbor remote-as

Use this command to create a BGP neighbor with its remote AS or configure the remote AS of a peer group. Use the **no** form of this command to delete a neighbor or a peer group.

neighbor { *IP-ADDRESS* **|** *PEER-GROUP-NAME***} remote-as** *AS-NUMBER*

no neighbor { *IP-ADDRESS* **|** *PEER-GROUP-NAME***} remote-as**

Syntax Description	
IP-ADDRESS	Specifies IP address of BGP peer.
PEER-GROUP-NAME	Name of a Border Gateway Protocol (BGP) peer group. The maximum length is 16 characters.
AS-NUMBER	The number of autonomous system to which the neighbor belongs. Range for 2-byte numbers is 1 to 65535. Range for 4-byte numbers is 1 to 4294967295.

Default There are no BGP neighbor peers.

Command Mode Router configuration.

Address family configuration (VRF).

Usage Guideline If you specify a BGP peer group, all the members of the peer group will inherit the characteristic configured with this command. When using the **no** form of this command with *PEER-GROUP* parameter, all the members that are generated with no indicated AS number will be deleted.

Use the **show ip bgp neighbors** or **show ip bgp peer-group** command to verify your settings.

Example This example shows how to create a neighbor 10.10.10.2 with remote AS 10.

```
Switch(config)#router bgp 65100
Switch(config-router)#neighbor 10.10.10.2 remote-as 10
Switch(config-router)#
```

2-69 neighbor remove-private-as

Use this command to remove private autonomous system numbers from the autonomous system path attribute in the updates sent to the specified neighbor or the members of the specified peer group. To disable this function, use the **no** form of this command.

neighbor { *IP-ADDRESS* **|** *PEER-GROUP-NAME* **} remove-private-as**

no neighbor { *IP-ADDRESS* **|** *PEER-GROUP-NAME* **} remove-private-as**

Syntax Description	
IP-ADDRESS	Specifies IP address of BGP peer.
PEER-GROUP-NAME	Name of a Border Gateway Protocol (BGP) peer group. The maximum length is 16 characters.

Default Disabled

Command Mode Router configuration.

Address family configuration (IPv4 Unicast and VRF).

Usage Guideline This command is available for external BGP (eBGP) neighbors only.

When an update is passed to the external neighbor, if the autonomous system path includes private autonomous system numbers, the software will drop the private autonomous system numbers except the following conditions:

If the autonomous system path includes both private and public autonomous system numbers, the software considers this to be a configuration error and does not remove the private autonomous system numbers.

If the autonomous system path contains the autonomous system number of the eBGP neighbor, the private autonomous system numbers will not be removed.

If this command is used with confederation, it will work as long as the private autonomous system numbers follow the confederation portion of the autonomous path.
The private autonomous system values are 64512 to 65535.

Use the **show ip bgp neighbors** or **show ip bgp peer-group** command to verify your settings.

Example The following example shows a configuration that will remove the private autonomous system number from the updates sent to 172.16.1.1. The AS path attribute of the updates advertised by 10.10.10.10 through autonomous system 100 will just contain “10” (as seen by autonomous system 20):

```
switch(config)#router bgp 10
switch(config-router)#neighbor 10.10.10.10 remote-as 65530
switch(config-router)#neighbor 172.16.1.1 remote-as 20
switch(config-router)#neighbor 172.16.1.1 remove-private-as
Switch(config-rotuer)#
```

2-70 neighbor route-map

Use this command to apply a route map to incoming or outgoing routes. Use the **no** command to remove the route map.

neighbor { *IP-ADDRESS* **|** *PEER-GROUP-NAME* **} route-map** *MAP-NAME* **{ in | out}**

no neighbor { *IP-ADDRESS* **|** *PEER-GROUP-NAME* **} route-map { in | out}**

Syntax Description	
IP-ADDRESS	Specifies IP address of BGP peer.
PEER-GROUP-NAME	Name of a Border Gateway Protocol (BGP) peer group. The maximum length is 16 characters.
MAP-NAME	Name of the route map. The length is up to 16 characters.
in	Applies the route-map to the incoming routes.
out	Applies the route-map to the outgoing routes.

Default None

Command Mode Router configuration.

Address family configuration (IPv4 Unicast, VPNv4 and VRF).

Usage Guideline The command is used to configure the route map related setting for a BGP neighbor or a peer group.

If a route map is configured relating to a BGP neighbor but the route map doesn't exist, it means deny any. If the route map exists but has no filter entry defined, it will permit all.

Use the **show ip bgp neighbors** or **show ip bgp peer-group** command to verify your settings.

Example The following example applies a route map named *internal-map* to a BGP outgoing updates to 172.16.1.1:

Firstly, create a route-map named *internal-map*:

```
Switch(config)#route-map internal-map
Switch(config-route-map)#set local-preference 100
Switch(config-route-map)#exit
Switch(config)#
```

Then, set the routing policy to neighbor 172.16.1.1:

```
Switch(config)#router bgp 10
Switch(config-router)#neighbor 172.16.1.1 remote-as 10
Switch(config-router)#neighbor 172.16.1.1 route-map internal-map out
Switch(config-router)#
```

2-71 neighbor route-reflector-client

This command is used to configure the local BGP as a route reflector and specify a neighbor or a peer group as its client. Use the **no** form of this command to remove the client.

neighbor { *IP-ADDRESS* **|** *PEER-GROUP-NAME* **} route-reflector-client**

no neighbor { *IP-ADDRESS* **|** *PEER-GROUP-NAME* **} route-reflector-client**

Syntax Description	
IP-ADDRESS	Specifies IP address of BGP peer.
PEER-GROUP-NAME	Name of a Border Gateway Protocol (BGP) peer group. The maximum length is 16 characters.

Default

No route reflector client set.

Command Mode

Router configuration.

Address family configuration (IPv4 Unicast and VPNv4).

Usage Guideline

When the route reflector client is defined and the router reflection is enabled by the command **bgp client-to-client reflection**, the BGP router will act as the route reflector. The reflector and its clients form a cluster. In a cluster, all the members must be an iBGP connection with the reflector and vice versa. The reflector is the representative of the cluster. For the reflector, the iBGP connection is established by the **neighbor remote-as** command and the corresponding neighbor must be specified as the client by this command. For the client, the iBGP connection is established by the **neighbor remote-as** command.

When the router is in reflection mode, the router will exchange information with client neighbors in the reflection way and with the remaining neighbors in the ordinary way. When the router is in non-reflection mode, the router will exchange information with all the neighbors in the non-reflection way.

An AS can have multiple clusters, and a cluster can have more than one reflector for redundancy purposes.

Use the **show ip bgp neighbors** or **show ip bgp peer-group** command to verify your settings.

Example

The following example shows how to add a neighbor as the route reflector client:.

```
Switch(config)#router bgp 5
Switch(config-router)#neighbor 10.10.10.2 remote-as 5
Switch(config-router)#neighbor 10.10.10.2 route-reflector-client
Switch(config-router)#
```

2-72 neighbor send-community

Use this command to specify that community attribute should be sent to a BGP neighbor or all the members of a peer group. Use the **no** form of this command to remove the entry.

neighbor {*IP-ADDRESS* **|** *PEER-GROUP-NAME***} send-community [{both | standard | extended}]**

no neighbor {*IP-ADDRESS* **|** *PEER-GROUP-NAME***} send-community [{both | standard | extended}]**

Syntax Description	
IP-ADDRESS	Specifies IP address of BGP peer.
PEER-GROUP-NAME	Name of a Border Gateway Protocol (BGP) peer group. The maximum length is 16 characters.
both	(Optional) Specifies that both standard and extended communities will be sent.
standard	(Optional) Specifies that only standard communities will be sent.
extended	(Optional) Specifies that only extended communities will be sent.

Default None

Command Mode Router configuration.

Address family configuration (IPv4 Unicast, VPNv4 and VRF).

Usage Guideline If you specify a BGP peer group by using the *PEER-GROUP-NAME*, all the members of the peer group will inherit the characteristic configured with this command.

Only the **standard** communities will be sent if no optional parameter is specified.

Use the **show ip bgp neighbors** or **show ip bgp peer-group** command to verify your settings.

Example The following example sets the send-community with standard:

```
Switch(config)#router bgp 65100
Switch(config-router)#neighbor 10.4.4.4 remote-as 65200
Switch(config-router)#neighbor 10.4.4.4 send-community standard
Switch(config-router)#
```

2-73 neighbor shutdown

Use this command to disable a neighbor or a peer group. Use the **no** form of this command to re-enable a neighbor or a peer group.

neighbor { *IP-ADDRESS* **|** *PEER-GROUP-NAME***} shutdown**

no neighbor { *IP-ADDRESS* **|** *PEER-GROUP-NAME***} shutdown**

Syntax Description	
IP-ADDRESS	Specifies IP address of BGP peer.
PEER-GROUP-NAME	Name of a Border Gateway Protocol (BGP) peer group. The maximum length is 16 characters.

Default The peers or peer groups do not shut down.

Command Mode Router configuration.

Address family configuration (VRF).

Usage Guideline You can use this command to terminate any active session for the specified neighbor or peer group. After this command is executed, all the routing information associated with the neighbor or peer group are cleared, but the configured information still exist. In the case of a peer group, a large number of peering sessions could be terminated suddenly.

Use the **show ip bgp neighbors** or **show ip bgp peer-group** command to verify your settings.

Example The following example shows how to disable any active session for the neighbor 172.16.10.10:

```
Switch(config)#router bgp 65100
Switch(config-router)#neighbor 172.16.10.10 shutdown
Switch(config-rotuer)#
```

2-74 neighbor soft-reconfiguration inbound

This command is used to start storing the route updates received from the specified neighbor or peer group. To not store received updates, use the **no** form of this command.

neighbor { *IP-ADDRESS* **|** *PEER-GROUP-NAME***} soft-reconfiguration inbound**

no neighbor { *IP-ADDRESS* **|** *PEER-GROUP-NAME***} soft-reconfiguration inbound**

Syntax Description	
IP-ADDRESS	Specifies IP address of BGP peer.
PEER-GROUP-NAME	Name of a Border Gateway Protocol (BGP) peer group. The maximum length is 16 characters.

Default Disabled.

Command Mode Router configuration.

Address family configuration (IPv4 Unicast and VRF).

Usage Guideline If the setting is enabled, the route updates received from the specified neighbor or peer group will be stored. In this case, the routing table can be rebuilt based on the stored route updates after the soft reset for inbound sessions. Otherwise, both BGP peers must support the soft route refresh capability, which is advertised in the OPEN message sent when the peers establish a TCP session, and in order to rebuild the routing table, the local router need to send the ROUTE REFRESH message to the neighbor to ask for the route information.

Use the **show ip bgp neighbors** or **show ip bgp peer-group** command to verify your settings.

Example The following example enables inbound soft reconfiguration for the neighbor 172.16.10.1. All the updates received form this neighbor will be stored unmodified, regardless of the inbound policy.

```
Switch(config)#router bgp 65100
Switch(config-router)#neighbor 172.16.10.1 remote-as 65200
Switch(config-router)#neighbor 172.16.10.1 soft-reconfiguration inbound
Switch(config-router)#
```

2-75 neighbor soo

Use this command to configure the Site of Origin (SoO) value of a peer or a peer group. Use the **no** form of this command to remove the Site of Origin value configured.

neighbor {*IP-ADDRESS* **|** *PEER-GROUP-NAME***} soo** *SOO-VALUE*

no neighbor {*IP-ADDRESS* **|** *PEER-GROUP-NAME***} soo**

Syntax Description	
IP-ADDRESS	Specifies IP address of the peer.
PEER-GROUP-NAME	Specifies the name of the peer group.
SOO-VALUE	The Site of Origin attribute will be encoded as a Route Origin Extended Community. There are two different types for the attribute: IP address: number: The IP address should be a global IP address that is assigned to the user and the number is assigned from a numbering space that is administered by the user. The number can be 1-65535. AS Number: number: The AS Number should be a public AS Number (Both 2-bytes AS number and 4-bytes AS number works) that is assigned to the user and the number is assigned from a numbering space that is administered by the user. The number can be between 1 and 4294967295 for the 4-bytes, AS number and between 1 and 65535 for the 2-bytes AS number.

Default No Site of Origin attribute configured by default.

Command Mode Address family configuration (VRF).

Usage Guideline Use this command to set the SoO value for a BGP neighbor or a peer group.
The SoO extended community is BGP extended communities attribute that is used to identify routes that have originated from a site so that the re-advertisement of that prefix back to the source site can be prevented. The SoO extended community uniquely identifies the site from which a router has learned a route. BGP can use the SoO value associated with a route to prevent routing loops.
Use the **show ip bgp neighbors** or the **show ip bgp peer-group** command to verify your settings.

Example This example shows how to set the site of origin value of BGP peer 3.3.3.3 in VRF vpn1.

```
Switch# configure terminal
Switch# router bgp 10
Switch(config-router)# address-family ipv4 vrf vpn1
Switch(config-router-af)# neighbor 3.3.3.3 remote-as 20
Switch(config-router-af)# neighbor 3.3.3.3 soo 10:100
Switch(config-router-af)# exit-address-family
```

2-76 neighbor timers

Use this command to set the timers for a specific BGP peer or a peer group. Use the **no** form of this command to return to the default value of the global setting.

neighbor { *IP-ADDRESS* **|** *PEER-GROUP-NAME***} timers** *KEEP-ALIVE HOLD-TIME*

no neighbor { *IP-ADDRESS* **|** *PEER-GROUP-NAME***} timers**

Syntax Description	
IP-ADDRESS	Specifies IP address of BGP peer.
PEER-GROUP-NAME	Name of a Border Gateway Protocol (BGP) peer group. The maximum length is 16 characters.
KEEP-ALIVE	Frequency (in seconds) with which the software sends keepalive messages to its peer. The default is 60 seconds. The range is from 0 to 65535.
HOLD-TIME	Interval (in seconds) after not receiving a keepalive message that the software declares a peer dead. The default is 180 seconds. The range is from 0 to 65535.

Default

KEEPALIVE: 60 seconds

HOLDTIME: 180 seconds

Command Mode

Router configuration.

Address family configuration (VRF).

Usage Guideline

KEEP-ALIVE specifies the interval at which a keepalive message is sent to its peers. The system will declare a peer as dead if not receiving a keepalive message until the hold time.

If the **holdtime** is zero, the hold time will never expire. If the **keepalive** is set to zero, the keepalive message will never be sent out

It is recommended that the **holdtime** value is three times than the **keepalive** timer.

The timers configured for a specific neighbor or peer group override the timers configured for all BGP neighbors using the **timers bgp** command.

Use the **show ip bgp neighbors** or **show ip bgp peer-group** command to verify your settings.

Example

The following example shows how to configure the KEEP-ALIVE timer to 120 seconds and HOLDTIME timer to 360 seconds for the neighbor 172.16.10.10:

```
Switch(config)#router bgp 65100
Switch(config-router)#neighbor 172.16.10.10 remote-as 65300
Switch(config-router)#neighbor 172.16.10.10 timers 120 360
Switch(config-router)#
```

2-77 neighbor unsuppress-map

This command is used to selectively advertise routes previously suppressed by the **aggregate-address** command. Use the **no** form of this command to remove the route map.

neighbor { *IP-ADDRESS* **|** *PEER-GROUP-NAME***} unsuppress-map** *MAP-NAME*

no neighbor { *IP-ADDRESS* **|** *PEER-GROUP-NAME***} unsuppress-map**

Syntax Description	
IP-ADDRESS	Specifies IP address of BGP peer.
PEER-GROUP-NAME	Name of a Border Gateway Protocol (BGP) peer group. The maximum length is 16 characters.
MAP-NAME	Name of the route-map of up to 32 characters.

Default No routes are unsuppressed.

Command Mode Router configuration.

Address family configuration (IPv4 Unicast, VPNv4 and VRF).

Usage Guideline When a route map is applied by this command, the suppressed route which matches the permit rule will be unsuppressed.

If a route map is configured relating to a BGP neighbor but the route map doesn't exist, it means deny any. If the route map exists but has no filter entry defined, it will permit all.

Use the **show ip bgp neighbors** or **show ip bgp peer-group** command to verify your settings.

Example The following example shows the routes specified by a route map named *internal-map* being unsuppressed for neighbor 172.16.10.10:

```
Switch(config)#router bgp 65100
Switch(config-router)#neighbor 172.16.10.10 unsuppress-map internal-map
Switch(config-router)#
```

2-78 neighbor update-source

Use this command to allow BGP sessions to use any operational interface for TCP connections. Use the **no** form of this command to restore the interface assignment to the closest interface.

neighbor { *IP-ADDRESS* **|** *PEER-GROUP-NAME***} update-source** *INTERFACE-TYPE INTERFACE-NUMBER*

no neighbor { *IP-ADDRESS* **|** *PEER-GROUP-NAME***} update-source**

Syntax Description	
IP-ADDRESS	Specifies IP address of BGP peer.
PEER-GROUP-NAME	Name of a Border Gateway Protocol (BGP) peer group. The maximum length is 16 characters.
INTERFACE-TYPE	The type of the interface. The supporting types include vlan interface and loopback interface.
INTERFACE-NUMBER	The number of the interface. The interface number's range is from 1 to 8 for loopback interface and from 1 to 4094 for vlan interface.

Default Disabled.

Command Mode Router configuration.

Address family configuration (VRF).

Usage Guideline Use this command in conjunction with any specified interface on the router. The use of loopback interface eliminates a dependency and BGP does not have to rely on the availability of a particular interface for making TCP connections. After this command configured success, BGP neighbor's session will be rebuilt.

Use the **show ip bgp neighbors** or **show ip bgp peer-group** command to verify your settings.

Example The following example sets the update-source interface of neighbor 172.16.10.10 to interface loopback 3:

```
Switch(config)#router bgp 65100
Switch(config-router)#neighbor 172.16.10.10 update-source loopback 3
Switch(config-router)#
```

2-79 neighbor weight

Use this command to specify the weight to be associated with a specific neighbor. To remove a weight assignment, use the **no** form of this command.

neighbor {*IP-ADDRESS* **|** *PEER-GROUP-NAME***} weight** *NUMBER*

no neighbor {*IP-ADDRESS* **|** *PEER-GROUP-NAME***} weight**

Syntax Description	
IP-ADDRESS	Specifies IP address of BGP peer.
PEER-GROUP-NAME	Name of a Border Gateway Protocol (BGP) peer group. The maximum length is 16 characters.
NUMBER	Weight to assign. Acceptable values are from 0 to 65535.

Default Routes learned from another BGP peer have a default weight of 0 and routes sourced by the local router have a default weight of 32768.

Command Mode Router configuration.

Address family configuration (VRF).

Usage Guideline The weight specified by this command determine the weight to be associated the routes learned from the specified neighbor.

Use the **show ip bgp neighbors** or **show ip bgp peer-group** command to verify your settings.

Example The following example sets the weight of the neighbor 10.4.4.4 to 10000:

```
Switch(config)#router bgp 65100
Switch(config-router)#neighbor 10.4.4.4 remote-as 65200
Switch(config-router)#neighbor 10.4.4.4 weight 10000
Switch(config-router)#
```

2-80 network (BGP)

Use this command to configure the networks to be advertised by the Border Gateway Protocol (BGP) process. To remove an entry from the routing table, use the **no** form of this command.

network *NETWORK-ADDRESS* **[route-map** *MAP-NAME***]**

no network *NETWORK-ADDRESS* **[route-map]**

Syntax Description	
NETWORK-ADDRESS	Specify the network address and the sub-network mask that BGP will advertise. For example, the format of NETWORK-ADDRESS can be 10.9.18.2/8
route-map *MAP-NAME*	(Optional) Specify the name of a configured route map. The route map should be examined to filter the networks to be advertised. If not specified, all networks are advertised.

Default

None.

Command Mode

Router configuration.

Address family configuration (IPv4 Unicast and VRF).

Usage Guideline

BGP networks can be learned from connected routes, from dynamic routing, and from static route sources.

Use this command to specify a network as local to this autonomous system and adds it to the BGP routing table. For exterior protocols the **network** command controls which networks are advertised. Interior protocols use the **network** command to determine where to send updates.
The maximum number of supported network entries is project dependent.
The BGP will advertise a network entry if the router has the route information for this entry if synchronize state is enabled.

You can verify your settings by entering the **show ip bgp network** command in privileged mode.

Examples

The following example sets up network 10.108.0.0 to be included in the BGP updates.

```
Switch# configure terminal
Switch(config)# router bgp 65100
Switch(config-router)# network 10.108.0.0/16
```

The following example sets up network 133.10.25.0/24 to be included in the BGP updates and use route-map mymap1 to set the weight of routes to 2000.

```
Switch# configure terminal
Switch(config)# route-map mymap1 permit 1
Switch(config-route-map)# set weight 2000
Switch config-route-map # exit
Switch(config)# router bgp 65100
Switch(config-router)# network 133.10.25.0/24 route-map mymap1
```

2-81 redistribute

This command is used to redistribute routing information from other routing protocols to BGP. Use the **no** form of this command to disable this function.

redistribute {local | static | rip | ospf {all | internal | external | type_1 | type_2 | inter+e1 | inter+e2}} [metric *NUMBER* **| route-map** *MAP-NAME***]**

no redistribute {local | static | rip | ospf} [metric | route-map]

Syntax Description	
local	To redistribute local routes to BGP.
static	To redistribute static routes to BGP.
rip	To redistribute RIP routes to BGP.
ospf	To redistribute OSPF routes to BGP. **all** - To redistribute both OSPF AS-internal and OSPF AS-external routes to BGP. **internal** - To redistribute only the OSPF AS-internal routes. **external** - To redistribute only the OSPF AS-external routes, including type-1 and type-2 routes. **type_1** - To redistribute only the OSPF AS-external type-1 routes. **type_2** - To redistribute only the OSPF AS-external type-2 routes. **inter+e1** - To redistribute only the OSPF AS-external type-1 and OSPF AS-internal routes. **inter+e2** - To redistribute only the OSPF AS-external type-2 and OSPF AS-internal routes.
NUMBER	(Optional) Specify the BGP metric value for the redistributed routes.Enter the metric value used here. This value must be between 0 and 4294967295.
MAP-NAME	(Optional) Specifies a route map which will be used as the criteria to determine whether to redistribute specific routes. Enter the route map name used here. This name can be up to 16 characters long.

Default Disabled.

Command Mode Router configuration.
Address family configuration (IPv4 Unicast and VRF).

Usage Guideline When a switch supports multiple routing protocols, the coordination between these protocols becomes an important task. This command is used for redistribute prefixes from other routing protocols to BGP.

You can verify your settings by entering **show ip bgp redistribute** command.

Examples

This example shows how to redistribute rip route to bgp and use the optional parameters to modify the routes:

```
Switch# configure terminal
Switch(config)# router bgp 65534
Switch(config-router)# redistribute rip metric 2000 route-map my-may
```

2-82 route-preference

Use this command to set BGP route preference. Use the **no** form of this command to restore the default value of bgp route preference.

route-preference {ibgp|ebgp} *VALUE*

no route-preference

Syntax Description	
VALUE	Preference of bgp route. The value range is 1-999.

Default The default route-preference for EBGP is 70 and IBGP is 130.

Command Mode Router configuration.
Address family configuration (VRF).

Usage Guideline This command is to set the route-preference for BGP route. BGP route contains two types one is IBGP and the other is EBGP. When two or more route protocol have learned one same route, the route-preference will be used to decided which one should be added into ip route table. Of course, for one route the smaller the route-preference, the better the route is.

Users can verify the settings by entering the **show ip route-preference** command in Privileged mode.

Examples This example shows how to configure ibgp route-preference for autonomous system 200:

```
Switch# configure terminal
Switch(config)# router bgp 200
Switch(config-router)#route-preference ibgp 150
```

2-83 router bgp

Use this command to enable (configure) BGP routing process. Use the **no** form of this command to remove a BGP routing process.

router bgp *AS-NUMBER*

no router bgp *AS-NUMBER*

Syntax Description	
AS-NUMBER	Specifies the number of an autonomous system that identifies the router to other BGP routers. Range for 2-byte numbers is 1 to 65535. Range for 4-byte numbers is 1 to 4294967295.

Default No BGP routing process is enabled by default.

Command Mode Global configuration mode.

Usage Guideline Each public autonomous system that directly connects to the Internet is assigned a unique number that identifies both the BGP routing process and the autonomous system (a number from 1 to 64511). Private autonomous system numbers are in the range from 64512 to 65534 (65535 is reserved for special use).

The AS Number size is defined as 2 bytes in RFC1771 and RFC4271.

But the AS Number can be expanded to 4 bytes to support much AS number.[RFC4893] To support 4-byte AS number, the AS number range is supported from 1 to 4294967295.

Private autonomous system numbers can be used for internal routing domains but must be translated for traffic that is routed out to the Internet. BGP should not be configured to advertise private autonomous system numbers to external networks. Use this command to enter router configuration mode for the specified routing process.

Examples This example shows how to configure a BGP process for autonomous system 200:

```
Switch# configure terminal
Switch(config)# router bgp 200
Switch(config-router)#
```

2-84 show ip as-path access-list

To display configured as-path access-lists, use this command in user or privileged mode.

show ip as-path access-list [*ACCESS-LIST-NAME***]**

Syntax Description	
ACCESS-LIST-NAME	(Optional) Specifies the access list to be displayed. The length is up to 16 characters.

Default None

Command Mode Privileged mode.

Usage Guideline This command can be used without any arguments or keywords. If no arguments are specified, this command will display all as-path access-lists. However, the as-path access-list name is specified when entering the **show ip as-path access-list** command. This option can be useful for filtering the output of this command and verifying a single named as-path access-list.

Example This example shows how to display the content of IP AS path access-list:

```
Switch# show ip as-path access-list

 BGP AS Path Access List: a1
          permit        ^300$
          deny          ^200$

          Total Filter Entries: 2

 BGP AS Path Access List: a2
          permit        3*0$
          deny          20

          Total Filter Entries: 2

 BGP AS Path Access List: a3
          permit        1

          Total Filter Entries: 1

Total AS Path Access List Number: 3

Switch#
```

show ip as-path access-list Field Description:

Field	Description
BGP AS Path Access List	Indicates the name of the BGP AS path access list.
permit	Indicates that the packets will be accepted if there AS-PATH attribute match the regular expression specified.
deny	Indicates that the packets will be rejected if there AS-PATH attribute match the regular expression specified.
Total Filter Entries	Indicates the total number of entries of a specifically AS path access list.
Total AS Path Access List Number	Indicates the total number of the AS path access lists.

2-85 show ip bgp

To display entries in the Border Gateway Protocol (BGP) routing table, use this command in privileged mode.

show ip bgp [{*IP-ADDRESS* **|** *NETWORK-ADDRESS* **[longer-prefixes]}]**

Syntax Description	
IP-ADDRESS	(Optional) IP address entered to filter the output to display only a particular host or network in the BGP routing table.
NETWORK-ADDRESS	(Optional) Specify the network address and the sub-network mask, for example: 120.25.0.0/16
longer-prefixes	(Optional) Displays the specified route and all more specific routes.

Default None

Command Mode Privileged mode

Usage Guideline The **show ip bgp** command is used to display the contents of the BGP routing table. When one bgp route's as path information filed carried more than 160 characters, this command will not show the totally information, and the command of **show ip bgp** *NETWORK-ADDRESS* can show the full information of this route especially the as path.

Examples The following example shows the BGP routing table:

```
Switch# show ip bgp

BGP Local Router ID is 10.90.90.10
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal
Origin codes: i - IGP, e - EGP, ? – incomplete

IP Address/Netmask       Gateway        Metric       LocPrf   Weight  Path

*>   10.0.0.0/8           0.0.0.0          1                    32768    ?
```

The following example shows the BGP routing which network address is 172.18.0.0/16 and includes longer prefixes:

```
Switch# show ip bgp 172.18.0.0/16 longer-prefixes

BGP Local Router ID is 10.90.90.10
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal
Origin codes: i - IGP, e - EGP, ? – incomplete


IP Address/Netmask   Gateway         Metric        LocPrf   Weight  Path

*>   172.18.0.0/16   10.90.1.1       1                      32768  100 200 ?
*>   172.18.2.0/24   10.90.1.1       1                     32768  100 200 ?
*>   172.18.3.0/24   10.90.1.1       1                     32768  100 200 ?
```

When one route's as path field more than 160 characters, Using this command can only show 160 characters of the as path field:

```
Switch# show ip bgp

BGP Local Router ID is 10.90.90.10
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal
Origin codes: i - IGP, e - EGP, ? – incomplete


IP Address/Netmask  Gateway     Metric   LocPrf   Weight   Path

*>   66.1.1.0/16     65.1.1.2    1                32768    (400)100 200 300
500 501 502 503 504 505 506 507 508 509 510 511 512 513 514 515 516 517 518
519 520 521 522 523 524 525 526 527 528 529 530 531 532 533 534 535 536 53
1000 i
*>   63.1.5.0/16     65.1.1.2    1                32768    (400)100 200 300
500 501 502 503 504 505 506 507 508 509 510 511 512 513 514 515 516 517 518
519 520 521 522 523 524 525 526 527 528 529 530 531 532 533 534 535 536 53
1000 i
*>   72.18.3.0/16    65.1.1.2    1                32768    (400)100 200 300
500 501 502 503 504 505 506 507 508 509 510 511 512 513 514 515 516 517 518
519 520 521 522 523 524 525 526 527 528 529 530 531 532 533 534 535 536 53
1000 i
```

If you show some of these route using command of show ip bgp NETWORK-ADDRESS, you will get the totally information of these route:

```
Switch# show ip bgp 66.1.1.0/24

BGP routing table entry for 66.1.1.0/24
Paths:(1 available, best #1, table: Default_IP_Routing_Table.)
Advertised to non peer-group peer: 76.1.1.10
Advertised to peer-groups:group1,group2

As path is: (400) 100 200 300 500 501 502 503 504 505 506 507 508 509 510 511
512 513 514 515 516 517 518 519 520 521 522 523 524 525 526 527 528 529 530
531 532 533 534 535 536 53 1000 600 601 602 603 604 605 606 607 609 750 751
752 757 758 759 780 1005 1007 2000 2008 1010 2010 953 959

Next hop is:65.1.1.2 (metric 1) from 65.1.1.102 (177.221.0.3)
Origin IGP, Imetric 1, localpref 4294967295, weight 30000, confed-external,
best
```

show ip bgp Field Description

Field	Description
BGP Local Router ID	The router identifier of the local BGP router.
Status codes	Status of the table entry displayed at the beginning of each line. It can be one or more of the following values: s—The table entry is suppressed. d—The table entry is damped. h—The table entry is damped and has been withdrawn by the neighbor. *—The table entry is valid. >—The table entry is the best entry to use for that network. i—The table entry was learned via an internal BGP (iBGP) session.
Origin codes	Origin of the table entry displayed at the end of each line. It can be one of the following values: i—Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. e—Entry originated from an Exterior Gateway Protocol (EGP). ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
IP Address/ Netmask	IP prefix with its mask length of the entry.
Gateway	IP address of the next router that is used when forwarding a packet to the destination network. An entry of 0.0.0.0 indicates that the router has some non-BGP routes to this network.

Metric	If shown, this is the value of the inter-autonomous system metric. This field is frequently not used.
LocPrf	Local preference value as set with the **set local-preference** route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network.

2-86 show ip bgp aggregate

To display aggregate entry in BGP (Border Gateway Protocol) database, use this command in user or privileged mode.

show ip bgp aggregate [vrf *VRF-NAME*] [*NETWORK-ADDRESS*]

Syntax Description	
vrf *VRF-NAME*	(Optional) Specifies a VRF name. The length of the VRF-NAME is 12 characters.
NETWORK-ADDRESS	(Optional) Specify the network address and the sub-network mask, for example: 120.25.0.0/16

Default None

Command Mode Privileged mode.

Usage Guideline This command is used to display aggregate entries created.

Examples This example output from the **show ip bgp aggregate** command in privileged mode.

```
Switch#show ip bgp aggregate 10.0.0.0/8

Network Address           Options
------------------       -------------------
100.0.0.0/8                 -
200.0.0.0/10               summary-only

Total Aggregate Address Number:  2
```

show ip bgp aggregate Field Description

Field	Description
Network Address	IP prefix with its mask length of the entry.
Options	May be as-set or summary-only.
Total Aggregate Address Number	The aggregate network number.

2-87 show ip bgp all

To display entries in the BGP routing table of IPv4 VPN address family and VRF related routing information.

show ip bgp all [{*NETWORK-ADDRESS* **| label}]**

Syntax Description	
NETWORK-ADDRESS	(Optional) Specifies to display the routes match the network address.
label	(Optional) Specifies to display the BGP private labels of the routes, which are assigned from MPLS.

Default None.

Command Mode Privileged mode.

Usage Guideline The **show ip bgp all** command is used for show route information in IPv4 VPN address family and routes in VRF.

Examples The following example shows the BGP routing table in IPv4 VPN address family:

```
Switch# show ip bgp all

 BGP Local Router ID is 30.1.1.2
 Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal
 Origin codes: i - IGP, e - EGP, ? - incomplete

IP Address/Netmask       Gateway        Metric       LocPrf   Weight  Path
Route Distinguisher: 1:1 (default for vrf VPN-A)
*>i  88.1.1.0/24         30.1.1.5       0            100      0       10 i
Route Distinguisher: 1:1 (VPN route(s))
*>i  88.1.1.0/24         30.1.1.5       0            100      0       10 i
Route Distinguisher: 2:2 (default for vrf VPN-B)
*>i  77.1.1.0/24         30.1.1.5       0            100      0       11 i
Route Distinguisher: 2:2 (VPN route(s))
*>i  77.1.1.0/24         30.1.1.5       0            100      0       11 i

Switch#
```

The following example displays the BGP private labels of all routes.

```
Switch#show ip bgp all label

 BGP Local Router ID is 30.1.1.2
 Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal
 Origin codes: i - IGP, e - EGP, ? - incomplete

   Network              From           In Label/Out Label

Route Distinguisher: 1000:10 (default for VRF vrf-1)
*> 0.0.0.0/0           Self Peer            1000/no
*> 84.10.40.0/24       Self Peer            1000/no
*> 84.10.50.0/24       Self Peer            1000/no
*> 111.0.0.0/8         Self Peer            1000/no
*> 128.0.0.0/24        Self Peer            1000/no
*> 191.255.255.0/24    Self Peer            1000/no
*> 192.0.0.0/24        Self Peer            1000/no
*> 200.1.0.0/24        Self Peer            1000/no
*> 223.255.255.0/24    Self Peer            1000/no
Route Distinguisher: 1000:12 (VPN route(s))
*> 41.1.0.0/16         12.12.12.12          no/1000
Route Distinguisher: 2000:10 (default for VRF vrf-2)
*> 107.1.0.0/16        Self Peer            1001/no
*> 108.1.0.0/16        Self Peer            1001/no
*> 109.1.0.0/16        Self Peer            1001/no
*> 128.0.0.0/24        Self Peer            1001/no
*> 191.255.255.0/24    Self Peer            1001/no
*> 192.0.0.0/24        Self Peer            1001/no
*> 200.1.0.0/16        Self Peer            1001/no
*> 201.1.0.0/16        Self Peer            1001/no

Switch#
```

Field	Description
BGP Local Router ID	Local Router IDThe router identifier of the local BGP router.

Status codes	Status of the table entry displayed at the beginning of each line. It can be one or more of the following values: s—The table entry is suppressed. d—The table entry is damped. h—The table entry is damped and has been withdrawn by the neighbor. *—The table entry is valid. >—The table entry is the best entry to use for that network. i—The table entry was learned via an internal BGP (iBGP) session.
Origin codes	Origin of the table entry displayed at the end of each line. It can be one of the following values: i—Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a network router configuration command. e—Entry originated from an Exterior Gateway Protocol (EGP). ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
IP Address/ Netmask	IP prefix with its mask length of the entry.
Gateway	IP address of the next router that is used when forwarding a packet to the destination network. An entry of 0.0.0.0 indicates that the router has some non-BGP routes to this network.
Metric	If shown, this is the value of the inter-autonomous system metric. This field is frequently not used.
LocPrf	Local preference value as set with the set local-preference route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Route Distinguisher	Specify the route distinguisher of the following routes.
default for vrf	Specify the VRF which The route distinguisher is default for.
VPN route(s)	Specify that the following routes are learned from PEs.
Path	Autonomous system paths to the destination network.
From	Specify the origin of this prefix.
In label	Specify the label which would be assigned to other routes that origin from other PE.
Out label	Specify the label which get form other PE neighbor.
Self Peer	Specify that the route is originated from local.
no	Specify this prefix does not have label of this direction.

2-88 show ip bgp rd

To display entries in the BGP routing table in IPv4 VPN address family with the specified Route Distinguisher.

show ip bgp rd *ASN:NN* **[{***NETWORK-ADDRESS* **| label }]**

Syntax Description	
ASN:NN	Specifies the Route Distinguisher
NETWORK-ADDRESS	(Optional) Specifies to display the route match the network address.
label	(Optional) Specifies to display the BGP private labels of the routes, which are assigned from MPLS.

Default None.

Command Mode Privileged mode.

Usage Guideline The **show ip bgp rd** command is used to display BGP route information in a VPNv4 address family and VRF address family based on Route Distinguisher.

Examples The following example shows the BGP routing table in VRF address family based on Route Distinguisher:

```
Switch# show ip bgp rd 1:1

 BGP Local Router ID is 30.1.1.2
 Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal
 Origin codes: i - IGP, e - EGP, ? - incomplete

IP Address/Netmask       Gateway        Metric       LocPrf   Weight  Path

Route Distinguisher: 1:1 (default for vrf VPN-A)
*>i  88.1.1.0/24        30.1.1.5         0          100        0      10  i

Switch#
```

The following example displays the BGP private labels of a specified RD.

```
Switch#show ip bgp rd 1:1 label

 BGP Local Router ID is 11.11.11.11
 Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal
 Origin codes: i - IGP, e - EGP, ? - incomplete

   Network              From           In Label/Out Label

Route Distinguisher: 1:1 (default for VRF my)
*> 88.1.2.0/24          100.1.1.2      1000/no
*> 88.1.5.0/24          100.1.1.2      1000/no
*> 89.1.1.0/24          10.1.1.3       no/16
*> 89.1.2.0/24          10.1.1.3       no/17
*> 99.1.1.0/24          Self Peer      1000/no
Route Distinguisher: 1:1 (VPN route(s))
*> 89.1.1.0/24          10.1.1.3       no/16
*> 89.1.2.0/24          10.1.1.3       no/17

Switch#
```

Field	Description
BGP Local Router ID	Local Router IDThe router identifier of the local BGP router.
Status codes	Status of the table entry displayed at the beginning of each line. It can be one or more of the following values: s—The table entry is suppressed. d—The table entry is damped. h—The table entry is damped and has been withdrawn by the neighbor. *—The table entry is valid. >—The table entry is the best entry to use for that network. i—The table entry was learned via an internal BGP (iBGP) session.

Origin codes	Origin of the table entry displayed at the end of each line. It can be one of the following values: i—Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a network router configuration command. e—Entry originated from an Exterior Gateway Protocol (EGP). ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
IP Address/ Netmask	IP prefix with its mask length of the entry.
Gateway	IP address of the next router that is used when forwarding a packet to the destination network. An entry of 0.0.0.0 indicates that the router has some non-BGP routes to this network.
Metric	If shown, this is the value of the inter-autonomous system metric. This field is frequently not used.
LocPrf	Local preference value as set with the set local-preference route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Route Distinguisher	Specify the route distinguisher of the following routes.
default for vrf	Specify the VRF which The route distinguisher is default for.
VPN route(s)	Specify that the following routes are learned from PEs.
Path	Autonomous system paths to the destination network.
From	Specify the origin of this prefix.
In label	Specify the label which would be assigned to other routes that origin from other PE.
Out label	Specify the label which get form other PE neighbor.
Self Peer	Specify that the route is originated from local.
no	Specify this prefix does not have label of this direction.

2-89 show ip bgp vrf

To display entries in the BGP routing table in VRF address family.

show ip bgp vrf *VRF-NAME* **[{***NETWORK-ADDRESS* **| label }]**

Syntax Description	
VRF-NAME	(Optional)Specifies the name of VRF.
NETWORK-ADDRESS	(Optional) Specifies to display the route match the network address.
label	(Optional) Specifies to display the BGP private labels of the routes, which are assigned from MPLS.

Default None.

Command Mode Privileged mode.

Usage Guideline The **show ip bgp vrf** command is used to display the BGP routing information inVRF address family.

Examples The following example shows the BGP routing table of IPv4 VRF address family:

```
Switch# show ip bgp vrf VPN-A

 BGP Local Router ID is 30.1.1.2
 Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal
 Origin codes: i - IGP, e - EGP, ? - incomplete

IP Address/Netmask       Gateway        Metric       LocPrf   Weight  Path

Route Distinguisher: 1:1 (default for vrf VPN-A)
*>i  88.1.1.0/24        30.1.1.5         0          100        0      10  i

Switch#
```

The following example displays the BGP private labes of routes of a specified VRF.

```
Switch#show ip bgp vrf VPN-B label

 BGP Local Router ID is 11.11.11.11
 Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal
 Origin codes: i - IGP, e - EGP, ? - incomplete

   Network              From           In Label/Out Label

Route Distinguisher: 1:1 (default for VRF VPN-B)
*> 11.0.0.0/16          Self Peer      1000/no
*> 89.1.1.0/24          10.1.1.3       no/16
*> 99.1.1.0/24          Self Peer      1000/no

Switch#.
```

Field	Description
BGP Local Router ID	Local Router IDThe router identifier of the local BGP router.
Status codes	Status of the table entry displayed at the beginning of each line. It can be one or more of the following values: s—The table entry is suppressed. d—The table entry is damped. h—The table entry is damped and has been withdrawn by the neighbor. *—The table entry is valid. >—The table entry is the best entry to use for that network. i—The table entry was learned via an internal BGP (iBGP) session.
Origin codes	Origin of the table entry displayed at the end of each line. It can be one of the following values: i—Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a network router configuration command. e—Entry originated from an Exterior Gateway Protocol (EGP). ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.

IP Address/ Netmask	IP prefix with its mask length of the entry.
Gateway	IP address of the next router that is used when forwarding a packet to the destination network. An entry of 0.0.0.0 indicates that the router has some non-BGP routes to this network.
Metric	If shown, this is the value of the inter-autonomous system metric. This field is frequently not used.
LocPrf	Local preference value as set with the set local-preference route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Route Distinguisher	Specify the route distinguisher of the following routes.
default for vrf	Specify the VRF which The route distinguisher is default for.
VPN route(s)	Specify that the following routes are learned from PEs.
Path	Autonomous system paths to the destination network.
From	Specify the origin of this prefix.
In label	Specify the label which would be assigned to other routes that origin from other PE.
Out label	Specify the label which get form other PE neighbor.
Self Peer	Specify that the route is originated from local.
no	Specify this prefix does not have label of this direction.

2-90 show ip bgp redistribute

This command is used to display the route redistribution configuration of BGP.

show ip bgp redistribute [vrf *VRF-NAME***]**

Syntax Description	
vrf *VRF-NAME*	(Optional) Specifies the name of VRF to display the route redistribution configuration in IPv4 VRF address family.
N/A	Display the route redistribution configuration in IPv4 unicast address family.

Default None.

Command Mode Privileged mode

Usage Guideline Use this command to check the route redistribution configuaration about BGP.

Example This example shows how to display the redistribution configuration of BGP:

```
Switch#show ip bgp redistribute

 Route Redistribution Settings

Source    Destination   Type      Metric       RouteMapName
Protocol  Protocol
--------  ------------  --------  ------       ------------

LOCAL     BGP           All       0            N/A

Total Entries : 1
```

This example shows how to display the redistribution configuration of BGP of IP VRF address family:

```
Switch#show ip bgp redistribute vrf VPN-A

 Route Redistribution Settings

Source    Destination   Type      Metric       RouteMapName
Protocol  Protocol
--------  ------------  --------  ------       ------------

Redistribute For VRF VPN-A

LOCAL     BGP           All       0            N/A

Total Entries : 1

Switch#
```

Field	Description
Route	Information of redistribute between bgp and some other protocols.
Source Protocol	The source protocol of the redistribute operation.
Destination Protocol	The destination protocol of the redistribute operation. Of course, it always is BGP.
Type	Specifies which part of route to be redistributed to bgp.
Metric	Specifies the BGP metric value for the redistributed routes.
RouteMapName	Specifies a route map which will be used as the criteria to determine whether to redistribute specific routes.
Total Entries	The numbers of protocols which have do redistribute operation between bgp and the protocol itself.
vrf	Indicates the name of the VRF if the redistribute has been done within a VRF.

2-91 show ip bgp cidr-only

To display routes with classless inter-domain routing (CIDR), use this command in privileged mode.

show ip bgp cidr-only

Syntax Description None.

Default None.

Usage Guideline This command is used to display BGP routes with classless inter-domain routing (CIDR).

Command Mode Privileged mode

Examples This example output from the **show ip bgp cidr-only** command in privileged mode.

```
Switch# show ip bgp cidr-only

BGP Local Router ID is 10.0.40.1
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal
Origin codes: i - IGP, e - EGP, ? – incomplete

IP Address/Netmask       Gateway         Metric      LocPrf    Weight  Path
*>  10.10.10.0/23        172.16.10.1     0                     300     10 i
*>  10.10.20.0/23        172.16.10.1     0                     300     10 i
*   10.20.10.0/22        172.16.10.1     0                     300     10 i
*dh 30.10.1.1/23         172.3.3.2       100         50        200     20 i
```

show ip bgp cidr-only Field Description

Field	Description
BGP Local Router ID	The router identifier of the local BGP router.
Status codes	Status of the table entry displayed at the beginning of each line. It can be one or more of the following values: s—The table entry is suppressed. d—The table entry is damped. h—The table entry is damped and has been withdrawn by the neighbor. *—The table entry is valid. >—The table entry is the best entry to use for that network. i—The table entry was learned via an internal BGP (iBGP) session.

Origin codes	Origin of the table entry displayed at the end of each line. It can be one of the following values: i—Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. e—Entry originated from an Exterior Gateway Protocol (EGP). ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
IP Address/ Netmask	IP prefix with its mask length of the entry.
Gateway	IP address of the next router that is used when forwarding a packet to the destination network. An entry of 0.0.0.0 indicates that the router has some non-BGP routes to this network.
Metric	If shown, this is the value of the inter-autonomous system metric. This field is frequently not used.
LocPrf	Local preference value as set with the **set local-preference** route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network.

2-92 show ip bgp community

Use this command to display routes which are matching the community.

show ip bgp community *COMMUNITY* **[exact-match]**

Syntax Description	
COMMUNITY	A community is in the form of <as-number> : <udn-number> or any of the following predefined values: **internet**, **no-export, local-as**, **no-advertise**. A community string can be formed by multiple communities, separated by a comma. An example of a community string is 200:1024, 300:1025, 400:1026.
exact-match	(Optional) If specified, communities need to match exactly. If not specified, then there are two cases: If internet is contained in the community list, then all routes will match. If not, then the community needs to be a subset of route's community to match.

Default None

Command Mode Privileged mode

Usage Guideline Use this command to display the routes which match the community specified.

When using this command with **exact-match** parameter, only the routes which community attribute exactly match will be displayed.

Example This example output from the show ip bgp community command in privileged mode.

```
Switch# show ip bgp community local-as

 BGP Local Router ID is 10.90.90.90
 Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal
 Origin codes: i - IGP, e - EGP, ? - incomplete

IP Address/Netmask     Gateway       Metric    LocPrf     Weight     Path

*>10.10.10.0/24        172.16.10.1   0                    300        10i
*>10.10.20.0/24        172.16.10.1   0                    300        10i
*>10.20.10.0/24        172.16.10.1   0                    300        10i

Switch#
```

show ip bgp community Field Description

Field	Description
BGP Local Router ID	The router identifier of the local BGP router.
Status codes	Status of the table entry displayed at the beginning of each line. It can be one or more of the following values: s—The table entry is suppressed. d—The table entry is damped. h—The table entry is damped and has been withdrawn by the neighbor. *—The table entry is valid. >—The table entry is the best entry to use for that network. i—The table entry was learned via an internal BGP (iBGP) session.
Origin codes	Origin of the table entry displayed at the end of each line. It can be one of the following values: i—Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. e—Entry originated from an Exterior Gateway Protocol (EGP). ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
IP Address/ Netmask	IP prefix with its mask length of the entry.
Gateway	IP address of the next router that is used when forwarding a packet to the destination network. An entry of 0.0.0.0 indicates that the router has some non-BGP routes to this network.
Metric	If shown, this is the value of the inter-autonomous system metric. This field is frequently not used.
LocPrf	Local preference value as set with the **set local-preference** route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network.

2-93 show ip bgp community-list

Use the show ip bgp community-list command to display routes that are permitted by the Border Gateway Protocol (BGP) community list,

show ip bgp community-list *COMMUNITY-LIST-NAME* **[exact-match]**

Syntax Description	
COMMUNITY-LIST-NAME	Community list name. The maximum length is 16 characters.
exact-match	(Optional) Displays only routes that have an exact match.

Default None

Command Mode Privileged mode

Usage Guideline This command requires you to specify an argument when used. The **exact-match** keyword is optional.

Example The following is sample output of the **show ip bgp community-list** command:

```
Switch#show ip bgp community-list MarketingComm

 BGP Local Router ID is 10.90.90.90
 Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal
 Origin codes: i - IGP, e - EGP, ? - incomplete

IP Address/Netmask     Gateway      Metric     LocPrf   Weight  Path

* 10.3.0.0/16          10.0.22.1    0          100      0       1800 1239 ?
* 10.6.0.0/16          10.0.22.1    0          100      0       1800 690 ?
* 10.7.0.0/16          10.0.22.1    0          100      0       1800 701 ?

Switch#
```

show ip bgp community-list Field Description

Field	Description
BGP Local Router ID	The router identifier of the local BGP router.

Status codes	Status of the table entry displayed at the beginning of each line. It can be one or more of the following values: s—The table entry is suppressed. d—The table entry is damped. h—The table entry is damped and has been withdrawn by the neighbor. *—The table entry is valid. >—The table entry is the best entry to use for that network. i—The table entry was learned via an internal BGP (iBGP) session.
Origin codes	Origin of the table entry displayed at the end of each line. It can be one of the following values: i—Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. e—Entry originated from an Exterior Gateway Protocol (EGP). ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
IP Address/ Netmask	IP prefix with its mask length of the entry.
Gateway	IP address of the next router that is used when forwarding a packet to the destination network. An entry of 0.0.0.0 indicates that the router has some non-BGP routes to this network.
Metric	If shown, this is the value of the inter-autonomous system metric. This field is frequently not used.
LocPrf	Local preference value as set with the **set local-preference** route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network.

2-94 show ip bgp confederation

This command is used to display the confederation configuration of BGP.

show ip bgp confederation

Syntax Description None

Default None

Command Mode Privileged mode

Usage Guideline Use this command to display the detail of the confederation configured.

Example The following example show current setting of confederation:

```
Switch# show ip bgp confederation

BGP AS Number                 : 65501
Confederation Identifier      : 10
Confederation Peer            : 65502, 65503
Neighbor List:
 IP Address             Remote AS Number
 ---------------       --------------------
 10.1.1.1               65501
 172.18.1.1             65503
 192.168.1.1            65502
Switch#
```

show ip bgp confederation Field Description

Field	Description
BGP AS Number	Indicates the AS number of the local BGP.
Confederation Identifier	Indicates the confederation Identifier of the local BGP.
Confederation Peer	Indicates the sub-AS numbers in the same confederation.
Neighbor List	List all the neighbors in the local BGP router.
IP Address	Indicates the IP address of the neighbors.
Remote AS Number	AS number of the neighbor.

2-95 show ip bgp dampening dampened-paths

Use this command in privileged mode to display routes that dampened by BGP.

show ip bgp dampening dampened-paths [vrf *VRF-NAME***]**

Syntax Description	
vrf *VRF-NAME*	(Optional) Specifies the VRF name. The length of the VRF-NAME is 12 characters.

Default None.

Command Mode Privileged mode.

Usage Guideline Use this command to show dampened entries in the BGP routing table.

Examples This example shows how to display the dampened routes using the **show ip bgp dampening dampened- paths** command in privileged mode.

```
Switch# show ip bgp dampening dampened-paths

BGP Local Router ID is 172.29.232.182
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network            From                  Reuse       Path
*d 10.0.0.0/8       172.16.232.177          00:18:4     100 ?
*d 10.2.0.0/16      172.16.232.177          00:28:5     100 ?
```

show ip bgp dampening dampened-paths Field Description

Field	Description
BGP Local Router ID	The router identifier of the local BGP router.
Status codes	Status of the table entry displayed at the beginning of each line. It can be one or more of the following values: s—The table entry is suppressed. d—The table entry is damped. h—The table entry is damped and has been withdrawn by the neighbor. *—The table entry is valid. >—The table entry is the best entry to use for that network. i—The table entry was learned via an internal BGP (iBGP) session.

Origin codes	Origin of the table entry displayed at the end of each line. It can be one of the following values: i—Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. e—Entry originated from an Exterior Gateway Protocol (EGP). ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
Network	IP prefix with its mask length of the entry.
From	The peer's router-id of bgp.
Reuse	The time which should be expensed before bgp reuse this route.
Path	Autonomous system paths to the destination network.

2-96 show ip bgp dampening parameters

To display bgp dampening configurations, use this command in privileged mode.

show ip bgp dampening parameters [vrf *VRF-NAME***]**

Syntax Description	
vrf *VRF-NAME*	(Optional) Specifies the VRF name. The length of the VRF-NAME is 12 characters.

Default None.

Command Mode Privileged mode

Usage Guideline Use this command to show dampening parameters of BGP.

Examples The following example is to show the dampening configuration information by using the **show ip bgp dampening parameters** command in privileged mode.

```
Switch# show ip bgp dampening parameters

BGP Dampening Parameter for IPv4 Unicast
----------------------------------------
BGP Dampening State             : Disabled

BGP Dampening Route Map         :
Half-life Time                  : 15 mins
Reuse Value                     : 750
Suppress Value                  : 2000
MAX Suppress Time               : 60 mins
Unreachable route's Half-life   : 15 mins
```

show ip bgp dampening parameters Field Description.

Field	Description
BGP Dampening State	Specifies the BGP dampening function's state.
BGP Dampening Route Map	The route map here is to set the dampening.
Half-Life Time	I Specifies the time (in minute) after which the penalty of the reachable routes will be down, by half. The default setting is 15 minutes.
Reuse Value	If the penalty for a flapping route decreases enough to fall below this value, the route is unsuppressed. The default setting is 750
Suppress Value	A route is suppressed when its penalty exceeds this limit. The default setting is 2000.
MAX Suppress Time	Maximum time (in minutes) a route can be suppressed. The default setting is 45 minutes.

Unreachable route's Half-life	Specifies the time (in minute) after which the penalty of the unreachable routes will be down, by half. The default setting is 15 minutes.

2-97 show ip bgp dampening flap-statistics

To display BGP flap statistics, use this command in privileged mode.

show ip bgp dampening flap-statistics [vrf *VRF-NAME***]**

Syntax Description	
vrf *VRF-NAME*	(Optional) Specifies the VRF name. The length of the VRF-NAME is 12 characters.

Command Mode Privileged mode

Usage Guideline Use this command to show flap entries in the BGP routing table.

Examples To display the flap entries in the BGP routing table, use the **show ip bgp dampening flap-statistics** command in privileged mode.

```
Switch# show ip bgp dampening flap-statistics


BGP Local Router ID is 10.90.90.10
Status codes: s suppressed, d damped, h history, * valid, > best, i –
internal
Origin codes: i - IGP, e - EGP, ? – incomplete

   Network              From            Flaps    Duration    Reuse     Path
*d 10.0.0.0/8         172.29.232.177    4        00:13:31    00:18:10   100i
*d 10.2.0.0/16        172.29.232.177    4        00:02:45    00:28:20   100i
```

show ip bgp dampening flap-statistics Field Description

Field	Description
BGP Local Router ID	The router identifier of the local BGP router.
Status codes	Status of the table entry displayed at the beginning of each line. It can be one or more of the following values: s—The table entry is suppressed. d—The table entry is damped. h—The table entry is damped and has been withdrawn by the neighbor. *—The table entry is valid. >—The table entry is the best entry to use for that network. i—The table entry was learned via an internal BGP (iBGP) session.

Origin codes	Origin of the table entry displayed at the end of each line. It can be one of the following values: i—Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. e—Entry originated from an Exterior Gateway Protocol (EGP). ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
Network	IP prefix with its mask length of the entry dampened.
From	The IP address of the peer advertised this route.
Reuse	Time after which the route will be made available. Format is HH:MM:SS.
Path	Autonomous system paths of route that is being dampened.
Flaps	Number of times that the route has flapped.
Duration	Time since the router noticed the first flap. Format is HH:MM:SS.

2-98 show ip bgp filter-list

To display routes that conform to a specified filter list, use the show ip bgp filter-list command.

show ip bgp filter-list *ACCESS-LIST-NAME*

Syntax Description	
ACCESS-LIST-NAME	Specifies the AS path access list name and only the routes match the AS path access list are displayed. The maximum length is 16 characters.

Default None

Command Mode Privileged mode

Usage Guideline Use this command to display routs which are match the filter list specified.

Example This example shows how to display the BGP route filter by content of access-list, as-ACL_HQ.

```
Switch# show ip bgp filter-list as-ACL_HQ

 BGP Local Router ID is 10.90.90.90
 Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal
 Origin codes: i - IGP, e - EGP, ? - incomplete

IP Address/Netmask       Gateway        Metric       LocPrf   Weight  Path

*172.16.0.0/24            172.16.72.30   0             109      108     ?
*172.16.1.0/24            172.16.72.30   0             109      108     ?
*172.16.11.0/24           172.16.72.30   0             109      108     ?
*172.16.14.0/24           172.16.72.30   0             109      108     ?
*172.16.15.0/24           172.16.72.30   0             109      108     ?
*172.16.16.0/24           172.16.72.30   0             109      108     ?

Switch#
```

show ip bgp filter-list Field Description

Field	Description
BGP Local Router ID	The router identifier of the local BGP router.

Status codes	Status of the table entry displayed at the beginning of each line. It can be one or more of the following values: s—The table entry is suppressed. d—The table entry is damped. h—The table entry is damped and has been withdrawn by the neighbor. *—The table entry is valid. >—The table entry is the best entry to use for that network. i—The table entry was learned via an internal BGP (iBGP) session.
Origin codes	Origin of the table entry displayed at the end of each line. It can be one of the following values: i—Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. e—Entry originated from an Exterior Gateway Protocol (EGP). ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
IP Address/ Netmask	IP prefix with its mask length of the entry.
Gateway	IP address of the next router that is used when forwarding a packet to the destination network. An entry of 0.0.0.0 indicates that the router has some non-BGP routes to this network..
Metric	If shown, this is the value of the inter-autonomous system metric. This field is frequently not used.
LocPrf	Local preference value as set with the **set local-preference** route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network.

2-99 show ip bgp inconsistent-as

To displays the routes which have the same prefix and different AS path origins, use this command in privileged mode.

show ip bgp inconsistent-as

Syntax Description None

Default None

Command Mode Privileged mode

Usage Guideline This command displays the routes which have inconsistent-as originating autonomous systems.

Examples This example output from the **show ip bgp inconsistent-as** command in privileged mode.

```
Switch# show ip bgp inconsistent-as

BGP Local Router ID is 10.90.90.10
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal
Origin codes: i - IGP, e - EGP, ? – incomplete

IP Address/Netmask      Gateway      Metric    LocPrf   Weight   Path
*  172.16.1.0/24       172.16.72.30  1                   0      109 108 i
                       172.16.72.21  1                   0      110 101 i
*  172.16.11.0/24      172.16.72.30  1                   0      109 108 i
                       172.16.72.10  1                   0      104 105 i
                       172.16.72.10  1                   0      104 103 i
```

show ip bgp inconsistent-as Field Description

Field	Description
BGP Local Router ID	The router identifier of the local BGP router.

Status codes	Status of the table entry displayed at the beginning of each line. It can be one or more of the following values: s—The table entry is suppressed. d—The table entry is damped. h—The table entry is damped and has been withdrawn by the neighbor. *—The table entry is valid. >—The table entry is the best entry to use for that network. i—The table entry was learned via an internal BGP (iBGP) session.
Origin codes	Origin of the table entry displayed at the end of each line. It can be one of the following values: i—Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. e—Entry originated from an Exterior Gateway Protocol (EGP). ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
IP Address/ Netmask	IP prefix with its mask length of the entry.
Gateway	IP address of the next router that is used when forwarding a packet to the destination network. An entry of 0.0.0.0 indicates that the router has some non-BGP routes to this network.
Metric	If shown, this is the value of the inter-autonomous system metric. This field is frequently not used.
LocPrf	Local preference value as set with the **set local-preference** route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network.

2-100 show ip bgp neighbors

Use this command to display information of the BGP neighbors.

show ip bgp neighbors [{[vrf *VRF-NAME***] [***IP-ADDRESS* **[{advertised-routes | received prefix-filter | received-routes | routes | statistics}]] | all}]**

Syntax Description	
vrf *VRF-NAME*	(Optional) Specifies a VRF name. The length of the VRF-NAME is 12 characters.
IP-ADDRESS	(Optional) IP address of a neighbor. If this argument is omitted, all neighbors are displayed.
advertised-routes	(Optional) Displays the routes advertised to a BGP neighbor.
received prefix-filter	(Optional) Displays the prefix-list received from the specified neighbor.
received-routes	(Optional) Displays the received routes from neighbor. To display all the received routes from the neighbor, configure the BGP soft reconfigure first.
routes	(Optional) Displays all accepted routes learned from neighbors.
statistics	(Optional) Displays the statistical information of BGP speaker.
all	(Optional) Displays information of all BGP neighbors.

Default None

Command Mode Privileged mode

Usage Guideline Use this command to display the information of the neighbor. The information may be the dynamic parameters configured to the neighbor, routers received from or sent to the neighbor, ORF filter received from the neighbor and the statistics information about the neighbor.

Example This example shows how to display all the neighbors.

```
Switch#show ip bgp neighbors all

BGP neighbor: 10.1.1.1 (Internal Peer)
------------------------------------------------------------------
Session State                                   : Enabled
Remote AS                                       : 1
Remote Router ID                                : 0.0.0.0
BGP State                                       : Connect
Hold Time                                       : 180 Seconds
Keepalive Interval                              : 60 Seconds
Advertisement Interval                          : 5 Seconds
EBGP Multihop                                   : 255
Weight                                          : 0

Address Family IPv4 Unicast
IPv4 Unicast                                    : None
Next Hop Self                                   : Disabled
Remove Private As                               : Disabled
AllowAS In                                      : Disabled
Soft Reconfiguration Inbound                    : Disabled
Send Community                                  : None
Default Originate                               : Disabled
Outbound Route Filter (ORF) type (64) Prefix list:
        Send Mode                               : Disabled
        Receive Mode                            : Disabled
Prefix Max Count                                : 12000
Prefix Warning Threshold                        : 75
Prefix Warning Only                             : Disabled

Address Family VPNv4 Unicast
VPNv4 Unicast                                   : None
Next Hop Self                                   : Disabled
AllowAS In                                      : Disabled
Send Community                                  : None
Outbound Route Filter (ORF) type (64) Prefix list:
        Send Mode                               : Disabled
        Receive Mode                            : Disabled
Prefix Max Count                                : 12000
Prefix Warning Threshold                        : 75
Prefix Warning Only                             : Disabled
```

```
BGP neighbor: 10.5.5.5 (External Peer), vrf VPN-A
------------------------------------------------------------------
Session State                                   : Enabled
Remote AS                                       : 2
Remote Router ID                                : 0.0.0.0
BGP State                                       : Idle
Hold Time                                       : 180 Seconds
Keepalive Interval                              : 60 Seconds
Advertisement Interval                          : 30 Seconds
EBGP Multihop                                   : 1
Weight                                          : 0

Address Family IPv4 Unicast
IPv4 Unicast                                    : None
AS Override                                     : Disabled
Next Hop Self                                   : Disabled
Remove Private As                               : Disabled
AllowAS In                                      : Disabled
Soft Reconfiguration Inbound                    : Disabled
Send Community                                  : None
Default Originate                               : Disabled
Outbound Route Filter (ORF) type (64) Prefix list:
        Send Mode                               : Disabled
        Receive Mode                            : Disabled
Prefix Max Count                                : 12000
Prefix Warning Threshold                        : 75
Prefix Warning Only                             : Disabled

Total neighbor number : 2
```

show ip bgp neighbors Field Description:

Field	Description
BGP neighbor	IP address of the BGP neighbor.
Internal Peer	Indicates that the neighbor is internal.
External Peer	Indicates that the neighbor is external.
vrf	Indicates the name of the VRF if the neighbor belongs to a VRF.
Session State	Indicates whether the neighbor is shut down or not.
Remote AS	AS number of the neighbor.
Remote Router ID	The router identifier of the local BGP router.

BGP State	The Finite State Machine (FSM) of the neighbor. The value may be **Idle**, **Connect, Active**, **Opensent**, **Openconfirm** and **Established.**
UP for	Indicates how long the **Established** state last. This field only display in the **Established** state.
Hold Time	Indicates the maximum number of seconds that may elapse between the receipts of successive KEEPALIVE and/or UPDATE messages with the neighbor.
Keepalive Interval	Indicates the number of seconds between sending KEEPALIVE message with the neighbor.
Advertisement Interval	Indicates the minimum interval between sending Border Gateway Protocol (BGP) routing updates.
EBGP Multihop	Indicates the TTL of the BGP packet sent to the neighbor.
Weight	Indicates the weight that will be associated to the routes learned from the neighbor.
Update Source	Interface used for TCP connection with the neighbor.
loopback	Indicates that the update source interface is a loopback interface, followed by its number.
vlan	Indicates that the update source interface is a vlan interface, followed by its vlan id.
Next Hop Self	Indicates whether the local BGP enable the router as the next hop for the neighbor.
Remove Private As	Indicates whether the configuration of removing the private AS from the AS path attribute in the updates sent to the neighbor is enabled or not.
AllowAS In	Indicates whether the local BGP allow its own AS number appearing in the received BGP update packets from the neighbor.
Num (AllowAS in)	Indicates how many times that the local BGP allow its own AS number appearing in the received BGP update packets. This field is only display when the **AllowAS In** is enabled.
Address Family VPNv4 Unicast	Indicates that the configuration below is only for VPNv4 unicast address family.
VPNv4 Unicast	Indicates whether the local BGP enabled the exchange of information with a Border Gateway Protocol (BGP) neighbor in VPNv4 unicast address family.
None (VPNv4 Unicast)	Indicates that the local BGP does not exchange VPNv4 unicast information with the neighbor.
Advertised (VPNv4 Unicast)	Indicates that the local BGP advertise its VPNv4 unicast information to the neighbor.
Received (VPNv4 Unicast)	Indicates that the local BGP receive the VPNv4 unicast information from the neighbor.
AS Override	Indicates whether the local BGP override the AS number of the peer with its own AS number in the routes received from the peer.
Site-of-Origin	Indicates the Site-of-Origin value configured to the neighbor.
Address Family IP v4 Unicast	Indicates that the configuration below is only for IPv4 unicast address family.
IPv4 Unicast	Indicates whether the local BGP enable the exchange of information with a Border Gateway Protocol (BGP) neighbor in IPv4 unicast address family.

None (IPv4 Unicast)	Indicates that the local BGP does not exchange IPv4 unicast information with the neighbor.
Advertised (IPv4 Unicast)	Indicates that the local BGP advertise its IPv4 unicast information to the neighbor.
Received (IPv4 Unicast)	Indicates that the local BGP receive the IPv4 unicast information from the neighbor.
Soft Reconfiguration Inbound	Indicates whether the local BGP store the route updates received from neighbor
Send Community	Indicates whether the local BGP send its community attributes to the neighbor.
None (send community)	The local BGP doesn't send any community attributes to the neighbor.
Standard (send community)	The local BGP send standard community attributes to the neighbor.
Extended (send community)	The local BGP send extended community attributes to the neighbor.
Default Originate	Indicates whether the local BGP send the default route to the neighbor.
Route Map (Default Originate)	Indicates a route-map name which control in which condition the local BGP send the default route to the neighbor.
Incoming Update Prefix List	Indicates an IP prefix list name which the route updates received from the neighbor must be applied
Outgoing Update Prefix List	Indicates an IP prefix list name which the route updates sent to the neighbor must be applied.
Incoming Update Filter List	Indicates an AS path access list name which the route updates received from the neighbor must be applied
Outgoing Update Filter List	Indicates an AS path access list name which the route updates sent to the neighbor must be applied.
Route Map for Incoming Routes	Indicates a route map name which the route updates received from the neighbor must be applied
Route Map for Outgoing Routes	Indicates a route map name which the route updates sent to the neighbor must be applied.
Unsuppressed Route Map	Indicates a route map name which the routes previously suppressed by the **aggregate-address** command must be applied.

Outbound Route Filter (ORF) type (64) Prefix list	Indicates the state of the ORF prefix list.
Send Mode	Indicates whether the local BGP send ORF prefix list to the neighbor.
Receive Mode	Indicates whether the local BGP receive ORF prefix list from the neighbor.
IP Prefix List (ORF)	Name of the IP prefix list received from the neighbor. The name is made up by the IP address by the dotted decimal notation dot Address Family Identifier (AFI) dot Subsequent Address Family Identifier (SAFI).
entries (ORF)	Number of entries of the prefix list.
Seq (ORF)	Sequence number of the entry.
permit (ORF)	Indicates that routes matched the IP prefix behind will be advertised to the neighbor.
deny (ORF)	Indicates that routes matched the IP prefix behind will not be advertised to the neighbor.
le (ORF)	Less than or equal. Indicates the length of the mask.
ge (ORF)	Greater than or equal. Indicates the length of the mask.
Password	Show the password set on the TCP connection to the neighbor.
Prefix Max Count	Show the maximum number of prefixes the local BGP can accept.
Prefix Warning Threshold	Indicates in which percentage of the maximum prefixes the local BGP begin to log warning message.
Prefix Warning Only	Indicates whether the local BGP terminate the session of the neighbor after the total BGP routes reach the maximum prefixes.
Description	Show the description configured to descript the neighbor.
Total neighbor number	Indicates the total number of neighbors in the local BGP router.

The following example displays routes advertised for only the 172.16.232.178 neighbor:

```
Switch#show ip bgp neighbors 172.16.232.178 advertised-routes

 BGP Local Router ID is 10.90.90.90
 Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal
 Origin codes: i - IGP, e - EGP, ? - incomplete

IP Address/Netmask        Gateway         Metric     LocPrf   Weight  Path

*10.0.0.0/24              172.16.232.179  0          100      0       ?
*10.20.2.0/24             172.1.1.2       0                   32768   i
```

show ip bgp neighbors advertised-routes Field Description:

Field	Description
BGP Local Router ID	The router identifier of the local BGP router.
Status codes	Status of the table entry displayed at the beginning of each line. It can be one or more of the following values: s—The table entry is suppressed. d—The table entry is damped. h—The table entry is damped and has been withdrawn by the neighbor. *—The table entry is valid. >—The table entry is the best entry to use for that network. i—The table entry was learned via an internal BGP (iBGP) session.
Origin codes	Origin of the table entry displayed at the end of each line. It can be one of the following values: i—Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. e—Entry originated from an Exterior Gateway Protocol (EGP). ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
IP Address/ Netmask	IP prefix with its mask length of the entry.
Gateway	IP address of the next router that is used when forwarding a packet to the destination network. An entry of 0.0.0.0 indicates that the router has some non-BGP routes to this network.
Metric	If shown, this is the value of the inter-autonomous system metric. This field is frequently not used.
LocPrf	Local preference value as set with the **set local-preference** route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network.

The following example shows the IP prefix-filter received from the neighbor 10.1.1.1 by ORF.

```
Switch#show ip bgp neighbors 10.1.1.1 received prefix-filter
ip prefix-list 10.1.1.1.1.1: 2 entries
   seq 5 permit 8.8.8.0/24 le 32
   seq 10 permit 9.9.9.0/24 le 32

Switch#
```

show ip bgp neighbors received prefix-filter Field Description

Field	Description
IP Prefix List	Name of the IP prefix list received from the neighbor. The name is made up by the IP address by the dotted decimal notation dot Address Family Identifier (AFI) dot Subsequent Address Family Identifier (SAFI).
entries	Number of entries of the prefix list.
Seq	Sequence number of the entry.
permit	Indicates that routes matched the IP prefix behind will be advertised to the neighbor.
deny	Indicates that routes matched the IP prefix behind will not be advertised to the neighbor.
le	Less than or equal. Indicates the length of the mask.
ge	Greater than or equal. Indicates the length of the mask.

The following example displays all the unprocessed routes received only from the 10.1.1.2 neighbor. These routes are contained in the Adj-RIB-In associated with the neighbor 10.1.1.2.

```
Switch# show ip bgp neighbors 10.1.1.2 received-routes

 BGP Local Router ID is 10.90.90.90
 Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal
 Origin codes: i - IGP, e - EGP, ? - incomplete

IP Address/Netmask      Gateway         Metric        LocPrf   Weight  Path

*172.18.0.0/24          10.1.1.2        0                      0        10i
*172.18.1.0/24          10.1.1.2        0                      0        10i
*172.18.2.0/24          10.1.1.2        0                      0        10i

Switch#
```

show ip bgp neighbors received-routes Field Description

Field	Description
BGP Local Router ID	The router identifier of the local BGP router.

Status codes	Status of the table entry displayed at the beginning of each line. It can be one or more of the following values: s—The table entry is suppressed. d—The table entry is damped. h—The table entry is damped and has been withdrawn by the neighbor. *—The table entry is valid. >—The table entry is the best entry to use for that network. i—The table entry was learned via an internal BGP (iBGP) session.
Origin codes	Origin of the table entry displayed at the end of each line. It can be one of the following values: i—Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. e—Entry originated from an Exterior Gateway Protocol (EGP). ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
IP Address/ Netmask	IP prefix with its mask length of the entry.
Gateway	IP address of the next router that is used when forwarding a packet to the destination network. An entry of 0.0.0.0 indicates that the router has some non-BGP routes to this network.
Metric	If shown, this is the value of the inter-autonomous system metric. This field is frequently not used.
LocPrf	Local preference value as set with the **set local-preference** route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network.

The following example displays all the accepted routes learned only from the 10.1.1.2 neighbor. These routes are contained in the Loc-RIB. This example bases on the example above, and we configure the local policy to only allow the IP prefix 172.18.1.0/24 in.

```
Switch# show ip bgp neighbors 10.1.1.2 routes

 BGP Local Router ID is 10.90.90.90
 Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal
 Origin codes: i - IGP, e - EGP, ? - incomplete

IP Address/Netmask        Gateway         Metric     LocPrf   Weight  Path

*>172.18.1.0/24           10.1.1.2        0                  0       10 i

Switch#
```

show ip bgp neighbors routes Field Description

Field	Description
BGP Local Router ID	The router identifier of the local BGP router.
Status codes	Status of the table entry displayed at the beginning of each line. It can be one or more of the following values: s—The table entry is suppressed. d—The table entry is damped. h—The table entry is damped and has been withdrawn by the neighbor. *—The table entry is valid. >—The table entry is the best entry to use for that network. i—The table entry was learned via an internal BGP (iBGP) session.
Origin codes	Origin of the table entry displayed at the end of each line. It can be one of the following values: i—Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. e—Entry originated from an Exterior Gateway Protocol (EGP). ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
IP Address/ Netmask	IP prefix with its mask length of the entry.
Gateway	IP address of the next router that is used when forwarding a packet to the destination network. An entry of 0.0.0.0 indicates that the router has some non-BGP routes to this network..
Metric	If shown, this is the value of the inter-autonomous system metric. This field is frequently not used.
LocPrf	Local preference value as set with the **set local-preference** route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network.

The following example displays the statistical information between 10.1.1.2 and 10.10.0.2.

```
Switch#show ip bgp neighbors 10.1.1.2 statistics

BGP neighbor: 10.1.1.2 (External Peer)
-----------------------------------------------
      Accepted Prefixes               : 3
      Last read                       : 00:00:47

      Send Statistics
            Opens                     : 1
            Notifications             : 0
            Updates                   : 1
            Keepalives                : 26
            Route Refresh             : 0
            Total                     : 28

      Receive Statistics
            Opens                     : 1
            Notifications             : 0
            Updates                   : 1
            Keepalives                : 25
            Route Refresh             : 0
            Total                     : 27

      Connections Established     : 1
      Connections Dropped         : 0
      Local Host                  : 10.10.0.2
      Local Port                  : 1024
      Remote Host                 : 10.1.1.2
      Remote Port                 : 179
      Due Time for Next Start Timer     : 5 seconds
      Due Time for Next Connect Timer   : 0 seconds

Switch#
```

show ip bgp neighbors statistics Field Description

Field	Description
BGP neighbor	IP address of the BGP neighbor.
Internal Peer	Indicates that the neighbor is internal.
External Peer	Indicates that the neighbor is external.

Accepted Prefixes	Number of routes accepted by the local BGP. These routes are contained in the Loc-RIB.
Last read	Time that BGP last received a message from this neighbor. Format is HH:MM:SS.
Send Statistics	The statistics information of the outgoing packets.
Opens (send)	Number of OPEN packets sent to the neighbor.
Notifications(send)	Number of NOTIFICATIONS packets sent to the neighbor.
Updates(send)	Number of UPDATES packets sent to the neighbor.
Keepalives(send)	Number of KEEPALIVES packets sent to the neighbor.
Route Refresh(send)	Number of ROUTEREFRESH packets sent to the neighbor.
Total(send)	Total packets sent to the neighbor.
Receive Statistics	The statistics information of the incoming packets.
Opens (receive)	Number of OPEN packets received from the neighbor.
Notifications (receive)	Number of NOTIFICATIONS packets received from the neighbor.
Updates (receive)	Number of UPDATES packets received from the neighbor.
Keepalives (receive)	Number of KEEPALIVES packets received from the neighbor.
Route Refresh (receive)	Number of ROUTEREFRESH packets received from the neighbor.
Total (receive)	Total packets received from the neighbor.
Connections Established	Number of times that the local BGP establish the TCP connection with the neighbor.
Connections Dropped	Number of times that the TCP connection been dropped.
Local Host	IP address of the local BGP.
Local Port	TCP port of the local BGP.
Remote Host	IP address of the neighbor.
Remote Port	TCP port of the neighbor.
Due Time for Next Start Timer	BGP peer auto re-start timer value next time. Seconds.
Due Time for Next Connect Timer	BGP peer re-connect timer value next time when peer session connect fail. Seconds

2-101 show ip bgp network

To display networks created by Border Gateway Protocol network command, use this command in user or privileged mode.

show ip bgp network [vrf *VRF-NAME*] [*NETWORK-ADDRESS*]

Syntax Description	
vrf *VRF-NAME*	(Optional) Specifies a VRF name. The length of the VRF-NAME is 12 characters.
NETWORK-ADDRESS	The IP network address.If a specific network address is not specified, all IP addresses will be displayed.

Default None

Command Mode Privileged mode.

Usage Guideline This command displays the networks advertised by BGP.

Examples This example output from the show ip bgp network command in privileged mode.

```
Switch#show ip bgp network

Network Address          Route Map
-------------------------------------------
20.0.0.0/24              -

Total Network Number:  1
```

show ip bgp network Field Description:

Field	Description
Network Address	BGP prefix created by command of **network** *<network-address >.*
Route Map	Specify the route-map of this network to apply.
Total Network Number	The number of bgp network.

2-102 show ip bgp reflection

This command is used to display the route reflection configuration of BGP.

show ip bgp reflection [vpnv4]

Syntax Description	
vpnv4	(Optional) Display reflection information of VPNv4 address family.

Default None.

Command Mode Privileged mode.

Usage Guideline Use this command to display what you have already configured to the local BGP about the route reflection.

Example This example shows how to display the reflection configuration of BGP:

```
Switch#show ip bgp reflection

 Client to Client Reflection State    : Disabled
 Cluster ID                           : 0.0.0.0
 Route Reflector Client:
        peer group: inter (172.18.10.1)
                172.18.10.3
                172.18.10.4
                172.18.10.5

Switch#
```

show ip bgp reflection Field Description

Field	Description
Client to Client Reflection State	Indicates the state of the route client to client reflection.
Cluster ID	Indicates the cluster ID of the local route reflection.
Route Reflector Client	Clients of the local route reflector, including peer group clients list and the individual clients list by IP addresses below.
peer group	Indicates the name of the peer group with the peer group members in the parentheses separated by comma.

2-103 show ip bgp route-map

To display networks which match route-map of Border Gateway Protocol, use this command in user or privileged mode.

show ip bgp route-map *MAP-NAME*

Syntax Description	
MAP-NAME	Specify the name of a route map. The maximum length is 16 characters.

Command Mode Privileged mode.

Usage Guideline This command displays the networks according to the specified route-map.

Examples This exam output from the show ip bgp route-map command in privileged mode.

```
Switch# show ip bgp route-map my

 BGP Local Router ID is 10.90.90.90
 Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal
 Origin codes: i - IGP, e - EGP, ? - incomplete

IP Address/Netmask       Gateway         Metric        LocPrf   Weight  Path

*>   10.0.0.0/8          0.0.0.0          0          100         32768     i
```

show ip bgp route-map Field Description

Field	Description
BGP Local Router ID	The router identifier of the local BGP router.
Status codes	Status of the table entry displayed at the beginning of each line. It can be one or more of the following values: s—The table entry is suppressed. d—The table entry is damped. h—The table entry is damped and has been withdrawn by the neighbor. *—The table entry is valid. >—The table entry is the best entry to use for that network. i—The table entry was learned via an internal BGP (iBGP) session.

Origin codes	Origin of the table entry displayed at the end of each line. It can be one of the following values: i—Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. e—Entry originated from an Exterior Gateway Protocol (EGP). ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
IP Address/ Netmask	IP prefix with its mask length of the entry.
Gateway	IP address of the next router that is used when forwarding a packet to the destination network. An entry of 0.0.0.0 indicates that the router has some non-BGP routes to this network.
Metric	If shown, this is the value of the inter-autonomous system metric. This field is frequently not used.
LocPrf	Local preference value as set with the **set local-preference** route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network.

2-104 show ip bgp parameters

To display parameters of Border Gateway Protocol, use this command in user or privileged privileged mode.

show ip bgp parameters

Syntax Description None.

Default None

Command Mode Privileged mode.

Usage Guideline This command displays the parameters of BGP.

Examples This example output from the show ip bgp parameters command in privileged mode.

```
Switch#show ip bgp parameters

BGP Global State                    : Enabled
Version                             : 4
BGP Router Identifier               : 10.90.90.90
Synchronization                     : Disabled
Enforce First AS                    : Disabled
Local AS Number                     : 10
Hold Time                           : 180 Seconds
Keepalive Interval                  : 60 Seconds
Always Compare MED                  : Disabled
Deterministics MED                  : Disabled
Med Confed                          : Disabled
Default Local Preference            : 100
AS Path Ignore                      : Disabled
Compare Router ID                   : Disabled
MED Missing as Worst                : Disabled
Compare Confederation Path          : Disabled
Fast External Fallover              : Enabled
Aggregate Next Hop Check            : Disabled
Default IPv4 Unicast                : Enabled
```

show ip bgp parameters Field Description

Field	Description
BGP Global State	BGP global state, In this version, BGP always is enabled.
Version	BGP protocol version.

BGP Router Identifier	BGP process's router ID.
Synchronization	BGP synchronization state.
Enforce First AS	When the setting is enabled, any updates received from an external neighbor, that does not have the neighbor's configured Autonomous System (AS) at the beginning of the AS_PATH in the received update, will be denied.
Local AS Number	The local as number.
Hold Time	The system will declare a peer as dead if a keepalive message is received that is more than the hold time
Keepalive Interval	Frequency that a bgp send keepalive message to peer.
Always Compare MED	Enable or disable the comparison of the Multi Exit Discriminator (MED) for paths from the neighbors in different Autonomous Systems.
Deterministics MED	Enable or disable to enforce the deterministic comparison of the Multi Exit Discriminator (MED) for paths received from the neighbors within the same Autonomous System.
Med Confed	If enabled, the BGP process will compare the MED for the routes that are received from confederation peers.
Default Local Preference	Specifies the default local preference value. The default value is 100.
AS Path Ignore	If enabled, the BGP process will ignore the AS path in the path selection process. By default this value is disabled.
Compare Router ID	If enabled, the BGP process will include the router ID in the path selection process. Similar routes are compared and the route with the lowest router ID is selected. By default this value is disabled.
MED Missing as Worst	If enabled, the BGP process will assign a value of infinity to routes that are missing the Multi Exit Discriminator (MED) attribute.
Compare Confederation Path	If enabled, the BGP process will compare the confederation AS path length of the routes received. The shorter the confederation AS path length, the better the route is.
Fast External Fallover	If enable, Border Gateway Protocol (BGP) routing process will immediately reset its external BGP peer sessions if the link used to reach these peers goes down.
Aggregate Next Hop Check	Only the routes with the same next hop attribute can be aggregated if the BGP aggregate next hop check is enabled.
Default IPv4 Unicast	Indicate whether the global router configuration is default for IPv4 Unicast or not.

2-105 show ip bgp peer-group

This command is used to display information of the BGP peer group.

show ip bgp peer-group [{[vrf *VRF-NAME***] [***PEER-GROUP-NAME***] | all}]**

Syntax Description	
vrf *VRF-NAME*	(Optional) Specifies a VRF name. The length of the VRF-NAME is 12 characters.
PEER-GROUP-NAME	Name of a Border Gateway Protocol (BGP) peer group. The maximum length is 16 characters.
all	(Optional) Displays information of all BGP peer groups.

Default None

Command Mode Privileged mode

Usage Guideline Use this command to display the contents of the BGP peer group.

Example The following example displays the information of the peer group named *mygroup*.

```
Switch# show ip bgp peer-group mygroup

BGP Peer Group :mygroup
------------------------------------------------------------------------
Description                                     :
Session State                                   : Enabled
Remote AS                                       : 1
Advertisement Interval                          : 5 seconds
Keepalive Interval                              : 60 seconds
Holdtime Interval                               : 180 seconds
EBGP Multihop                                   : 255
Weight                                          : 0

Address Family IPv4 Unicast
Members                                         : None
Route Reflector Client                          : Disabled
Send Community                                  : None
Remove Private As                               : Disabled
Next Hop Self                                   : Disabled
AllowAS In                                      : Disabled
Soft Reconfiguration Inbound                    : Disabled
Default Originate                               : Disabled
Outbound Route Filter (ORF) type (64) Prefix list:
        Send Mode                               : Disabled
        Receive Mode                            : Disabled
Prefix Max Count                                : 12000
Prefix Warning Threshold                        : 75
Prefix Warning Only                             : Disabled

Address Family VPNv4 Unicast
Members                                         : None
Route Reflector Client                          : Disabled
Send Community                                  : None
Next Hop Self                                   : Disabled
AllowAS In                                      : Disabled
Outbound Route Filter (ORF) type (64) Prefix list:
        Send Mode                               : Disabled
        Receive Mode                            : Disabled
Prefix Max Count                                : 12000
Prefix Warning Threshold                        : 75
Prefix Warning Only                             : Disabled
Switch#
```

show ip bgp peer-group Field Description

Field	Description
BGP Peer Group	Name of the peer group.
Description	Show the description configured to descript the peer group
Session State	Indicates whether the peer group is shut down or not.
Members	Members of this peer group, separated by comma.
Remote AS	Remote AS number of the peer group.
Not Set (remote AS)	Indicates that this peer group doesn't assign any AS number.
Advertisement Interval	Indicates the minimum interval between sending Border Gateway Protocol (BGP) routing updates.
Keepalive Interval	Indicates the number of seconds between sending KEEPALIVE message with the members of this peer group.
Hold Time	Indicates the maximum number of seconds that may elapse between the receipts of successive KEEPALIVE and/or UPDATE messages with the members of this peer group.
EBGP Multihop	Indicates the TTL of the BGP packet sent to the members of this peer group.
Weight	Indicates the weight that will be associated to the routes learned from the members of this peer group.
Update Source	Interface used for TCP connection with the neighbor.
loopback	Indicates that the update source interface is a loopback interface, followed by its number.
vlan	Indicates that the update source interface is a vlan interface, followed by vlan id.
Next Hop Self	Indicates whether the local BGP enable the router as the next hop for the members of this peer group.
Route Reflector Client	Indicates whether this peer group is a route reflector client of the local BGP.
Send Community	Indicates whether the local BGP send its community attributes to the members of this group.
Standard (send community)	The local BGP send standard community attributes to the neighbor.
Extended (send community)	The local BGP send extended community attributes to the neighbor.
None (send community)	The local BGP doesn't send any community attributes to the neighbor.
Remove Private As	Indicates whether the configuration of removing the private AS from the AS path attribute in the updates sent to the members of this peer group is enabled or not.
AllowAS In	Indicates whether the local BGP allow its own AS number appearing in the received BGP update packets form the members of this peer group.
Num (AllowAS in)	Indicates how many times that the local BGP allow its own AS number appearing in the received BGP update packets from the members of this peer group. This field is only display when the **AllowAS In** is enabled.

Soft Reconfiguration Inbound	Indicates whether the local BGP store the route updates received from members of this peer group.
Unsuppressed Route Map	Indicates a route map name which the routes previously suppressed by the **aggregate-address** command must be applied.
Default Originate	Indicates whether the local BGP send the default route to the members of this peer group.
Incoming Update Prefix List	Indicates an IP prefix list name which the route updates received from the members of this peer group must be applied
Outgoing Update Prefix List	Indicates an IP prefix list name which the route updates sent to the members of this peer group must be applied.
Incoming Update Filter List	Indicates an AS path access list name which the route updates received from the members of this peer group must be applied
Outgoing Update Filter List	Indicates an AS path access list name which the route updates sent to the members of this peer group must be applied.
Route Map for Incoming Routes	Indicates a route map name which the route updates received from the members of this peer group must be applied
Route Map for Outgoing Routes	Indicates a route map name which the route updates sent to the members of this peer group must be applied.
Outbound Route Filter (ORF) type (64) Prefix list	Indicates the state of the ORF prefix list.
Send Mode	Indicates whether the local BGP send ORF prefix list to the members of this peer group.
Receive Mode	Indicates whether the local BGP receive ORF prefix list from the members of this peer group.
Password	Show the password set on the TCP connection to the members of this peer group.
Prefix Max Count	Show the maximum number of prefixes the local BGP can accept.
Prefix Warning Threshold	Indicates in which percentage of the maximum prefixes the local BGP begin to log warning message.
Prefix Warning Only	Indicates whether the local BGP terminate the session of the members of this peer group after the total BGP routes reach the maximum prefixes.

2-106 show ip bgp quote-regexp

To display routes which matching the regular expression, use this command in privileged mode.

show ip bgp quote-regexp *REGEXP*

Syntax Description	
REGEXP	Displays routes matching the AS path regular expression. The maximum length is 80 characters.

Default None.

Command Mode Privileged mode.

Usage Guideline This command displays the routes which matching the AS path regular expression.

Examples This example output from the show ip bgp quote-regexp command in privileged mode.

```
Switch#show ip bgp quote-regexp “100”


BGP Local Router ID is 10.90.90.10
 Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal
 Origin codes: i - IGP, e - EGP, ? – incomplete

  IP Address/Netmask   Gateway        Metric    LocPrf   Weight  Path

s  172.16.0.0/24       172.16.72.30   1                  0       100 108 ?
s  172.16.0.0/24       172.16.72.30   1                  0       100 108 ?
*  172.16.1.0/24       172.16.72.30   1                  0       100 108 ?
*  172.16.11.0/24      172.16.72.30   1                  0       100 108 ?
*  172.16.14.0/24      172.16.72.30   1                  0       100 108 ?
*  172.16.15.0/24      172.16.72.30   1                  0       100 108 ?
*  172.16.16.0/24      172.16.72.30   1                  0       100 108 ?
```

show ip bgp route-map quote-regexp Field Description

Field	Description
BGP Local Router ID	The router identifier of the local BGP router.

Status codes	Status of the table entry displayed at the beginning of each line. It can be one or more of the following values: s—The table entry is suppressed. d—The table entry is damped. h—The table entry is damped and has been withdrawn by the neighbor. *—The table entry is valid. >—The table entry is the best entry to use for that network. i—The table entry was learned via an internal BGP (iBGP) session.
Origin codes	Origin of the table entry displayed at the end of each line. It can be one of the following values: i—Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. e—Entry originated from an Exterior Gateway Protocol (EGP). ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
IP Address/ Netmask	IP prefix with its mask length of the entry.
Gateway	IP address of the next router that is used when forwarding a packet to the destination network. An entry of 0.0.0.0 indicates that the router has some non-BGP routes to this network..
Metric	If shown, this is the value of the inter-autonomous system metric. This field is frequently not used.
LocPrf	Local preference value as set with the **set local-preference** route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network.

2-107 show ip bgp summary

This command is used to display the state of all BGP neighbors connection, also includes route id, local AS number and so on.

show ip bgp summary [{vrf *VRF-NAME* **| vpnv4}]**

Syntax Description	
vrf *VRF-NAME*	(Optional) Specifies a VRF name. The length of VRF-NAME is 12 characters.
vpnv4	(Optional) Displays the summary information of VPNv4 address family.

Default None.

Command Mode Privileged mode.

Examples This example is used to display the BGP summary information:

```
Switch# show ip bgp summary

BGP Router Identifier              : 10.90.90.10
Local AS Number                    : 10
BGP AS Path Entries                : 0
BGP Community Entries              : 0

Neighbor          Ver     AS     MsgRcvd   MsgSent   Up/Down    State/PfxRcd
------------     ---     ---    -------   -------   -------    ------------
10.90.90.100       4      100      10          8       00:03:18        10

Total Number of Neighbors: 1
```

Field	Description
BGP Router Identifier	The router identifier of the local BGP router.
Local AS Number	The Autonomous system number of local bgp.
BGP AS Path Entries	AS path access-list number.
BGP Community Entries	The entries of bgp community, including standard community and expand community.
Neighbor	BGP neighbor which is created by command of **neighbor** <*IP-ADDRESS* > **remote-as** <*AS-NUMBER*>.
Ver	BGP protocol version. And now, value is 4.
AS	The peer's Autonomous system number.
MsgRcvd	The number of message which receives form this neighbor.
MsgSent	The number of message which be sent to this neighbor.
Up/Down	The length of time that the BGP session has been in the Established state, or the current status if not in the Established state.

State/PfxRcd	The current state of the BGP session, or the number of prefixes that have been received from a neighbor or peer group. When the maximum number (as set by the **neighbor maximum-prefix** command) is reached, the string “PfxRcd” appears in the entry, the neighbor is shut down, and the connection is set to Idle. An (Admin) entry with Idle status indicates that the connection has been shut down using the **neighbor shutdown** command.

2-108 show ip community-list

To display configured community lists, use this command in privileged mode.

show ip community-list [*COMMUNITY-LIST-NAME***]**

Syntax Description	
COMMUNITY-LIST-NAME	Community list name. The maximum length is 16 characters.

Default None.

Command Mode Privileged mode.

Usage Guideline This command can be used without any arguments or keywords. If no arguments are specified, this command will display all community lists. However, the community list name can be specified when entering the **show ip community-list command**. This option can be useful for filtering the output of this command and verifying a single named community list.

Example The following output is similar to the output that will be displayed when the show ip community-list command is entered in config mode:

```
Switch#show ip community-list

Community List Name:  c1
---------------------------------
   Type  : Standard
       permit  :  20:30 no-advertise local-as
       deny  :  no-export

   Total Filter Entries: 2

Community List Name:  c2
---------------------------------
   Type  : Expanded
       permit  :  .*300.*$
       deny  :  500

   Total Filter Entries: 2

Community List Name:  c3
---------------------------------
   Type  : Expanded
       permit  :  20:30

   Total Filter Entries: 1

total community-list count:3

Switch#
```

show ip community-list Field Description

Field	Description
Community List Name	Name of this community list.
Type	Type of this community list.
Standard	Indicates that this entry is an standard community list with the well-known community value **internet local-AS no-advertise** and **no-export**, or with the standard AA:NN format.
Expanded	Indicates that this entry is an expanded community list with a regular expression.
permit	Routes with community attributes match the entry will be accepted.
deny	Routes with community attributes match the entry will be rejected.

Total Filter Entries	Total number of entries of a specifically community list.
total community-list count	Total numbers of the community list.

2-109 show ip extcommunity-list

To display extened community lists configurations.

show ip extcommunity-list [*EXTCOMMUNITY-LIST-NAME***]**

Syntax Description	
EXTCOMMUNITY-LIST-NAME	(Optional) Specifies to only display one extended community list.
N/A	Display all extended community lists.

Default None.

Command Mode Privileged mode.

Usage Guideline If no keyword is specified, this command will display all extcommunity lists. The extcommunity list name can be specified and it is useful for filtering the output of this command and verifying a single named extended community list.

Example The following displays the configuration of extended community-lists.

```
Switch#show ip extcommunity-list

Extended Community List Name:  e1
-----------------------------------------------
   Type  : Expanded

       permit : _23

   Total Filter Entries: 1

Extended Community List Name:  s1
-----------------------------------------------
   Type  : Standard

       permit :RT  1:1
SoO 1.1.1.1:1

       permit :SoO 2:3 3.2.1.1:10

   Total Filter Entries: 2

Total Extended Community-list Count:2

Switch#
```

Field	Description
Extended Community List Name	Name of this extcommunity list.
Type	Type of this community list.
Standard	Indicates that this entry is an standard extcommunity list with rt or soo value.
Expanded	Indicates that this entry is an expanded extcommunity list with a regular expression.
permit	Routes with extcommunity attributes match the entry will be accepted.
deny	Routes with extcommunity attributes match the entry will be rejected.
Total Filter Entries	Total number of entries of a specifically extcommunity list.
total community-list count	Total numbers of the extcommunity list.

2-110 synchronization

To enable the synchronization between BGP and your Interior Gateway Protocol (IGP) system, use the **synchronization** command in router configuration mode. To enable the router to advertise a network route without waiting for the IGP, use the **no** form of this command.

synchronization

no synchronization

Syntax Description None.

Default This command is disabled by default.

Command Mode Router configuration mode.

Usage Guideline Usually, a BGP speaker does not advertise a route to an external neighbor unless that route is local or exists in the IGP. By default, **synchronization** between BGP and the IGP is turned off to allow the switch to advertise a network route without waiting for route validation from the IGP. This feature allows routers and access servers within an autonomous system to have the route before BGP makes it available to other autonomous systems.
Use the synchronization command if routers in the autonomous system do not speak BGP.
You can verify your settings by entering the **show ip bgp parameters** command.

Examples This example shows how to enable synchronization in AS 65121.

```
Switch# configure terminal
Switch(config)# router bgp 65121
Switch(config-router)# synchronization
Switch(config-router)#
```

2-111 timers bgp

Use this command to adjust BGP network timers. Use the **no** form of this command to restore to the default value.

timers bgp *KEEP-ALIVE HOLD-TIME*

no timers bgp

Syntax Description	
KEEP-ALIVE	Specify the frequency, in seconds, with which the software sends *KEEPALIVE* messages to its BGP peer. The range is from 0 to 65535.
HOLD-TIME	Specifies the interval, in seconds, after not receiving a KEEPALIVE message that the software declares a BGP peer dead. The range is from 0 to 65535.

Default

KEEP-ALIVE: 60 seconds.

HOLD-TIME: 180 seconds.

Command Mode

Router configuration mode.

Usage Guideline

The suggested default value for the *KEEPALIVE* is 1/3 of the *HOLDTIME*. The timers configured for a specific neighbor or peer group (by the command **neighbor timers**) override the timers configured for all BGP neighbors using the **timers bgp** command.
When the minimum acceptable *HOLD-TIME* is configured on a BGP router, a remote BGP peer session is established only if the remote peer is advertising a *HOLD-TIME* that is equal to, or greater than, the minimum acceptable *HOLD-TIME* interval. If the minimum acceptable *HOLD-TIME* interval is greater than the configured *HOLD-TIME*, the next time the remote session tries to establish, it will fail and the local router will send a notification stating "unacceptable hold time."
You can verify your settings by entering the **show ip bgp parameters** command.

Examples

This example shows how to change the *KEEPALIVE* timer to 50 seconds and the *HOLD-TIME* timer to 150 seconds:

```
Switch# configure terminal
Switch(config)# router bgp 65100
Switch(config-router)# timers bgp 50 150
```

Distance Vector Multicast Routing Protocol (DVMRP) Commands

3-1 ip dvmrp

To enable Distance Vector Multicast Routing Protocol (DVMRP) on an interface, use the **ip dvmrp** command in interface configuration mode. To disable DVMRP on the interface, use the **no** form of this command.

ip dvmrp

no ip dvmrp

Syntax Description None.

Default Disabled.

Command Mode Interface configuration mode

Usage Guideline This command enables DVMRP on the specified interface.

If you want to use DVMRP to forward multicast packets, use **ip multicast-routing** command to enable multicast global state.

To verify you configuration, use the command **show ip dvmrp interface**.

Example This command enables DVMRP on interface VLAN 1.

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ip dvmrp
```

Disable DVMRP on interface VLAN 1.

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# no ip dvmrp
```

3-2 ip dvmrp metric

Use this command to configure the metric value on current interface. To restore the default value, use **no** form of this command.

ip dvmrp metric *METRIC*

no ip dvmrp metric

Syntax Description	
METRIC	Specify the metric value of the interface. The range is 1 to 31.

Default 1

Command Mode Interface configuration mode

Usage Guideline For each source network reported, a route metric is associated with the route being reported. The metric is the sum of the interface metrics between the router originating the report and the source network. For the purposes of DVMRP, the Infinity metric is defined to be 32. This limits the breadth across the whole DVMRP network and is necessary to place an upper bound on the convergence time of the protocol.

To verify you configuration, use command **show ip dvmrp interface**.

Example Configure the DVMRP metric of VLAN 1 to 30.

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ip dvmrp metric 30
```

Configure the DVMRP metric of VLAN 2 back to default.

```
Switch# configure terminal
Switch(config)# interface vlan 2
Switch(config-if)# no ip dvmrp metric
```

3-3 show ip dvmrp interface

Use this command to display DVMRP interface information.

show ip dvmrp interface [*IFNAME***]**

Syntax Description	
IFNAME	Specify an interface name. If no interface name is specified, the command will list all interfaces' info.

Default None

Command Mode User mode or Privileged mode.

Usage Guideline This command is used to display basic DVMRP interface information.

Example The following example shows all DVMRP interfaces information.

```
Switch# show ip dvmrp interface

Interface     IP Address         Metric  Generation ID  State
------------  -----------------  ------  -------------  --------
System        10.90.90.90        1       1368947491     Enabled
ipif1         90.1.1.1           1       0              Disabled

Total Entries: 2
```

The following example shows information of interface System.

```
Switch# show ip dvmrp interface System

Interface     IP Address         Metric  Generation ID  State
------------  -----------------  ------  -------------  --------
System        10.90.90.90        1       1368947491     Enabled
```

Field	Description
Interface	Specify the interface name.
IP Address	The IP address of the interface.
Generation ID	Specify the generation ID of this interface. This value is dynamically generated by the switch, and it is used for the neighbor to detect that whether the switch has restarted or not
Metric	The metric value of the interface, which is configured by command "**ip dvmrp metric**".
State	Specify the DVMRP interface state, which is configured by command "**ip dvmrp**"

3-4 show ip dvmrp neighbor

Use this command to display DVMRP neighbor information.

show ip dvmrp neighbor [*IFNAME***]**

Syntax Description	
IFNAME	Specify an interface name. If no interface name is specified, the command will list all interfaces' info.

Default None

Command Mode User mode or Privileged mode.

Usage Guideline This command is used to display DVMRP neighbor information. If no interface name is specified, this command will display DVMRP neighbor information on all interfaces.

Example The following example shows all DVMRP neighbor information.

```
Switch# show ip dvmrp neighbor

Interface        Neighbor Address  Generation ID  Expire Time
---------------  ----------------  -------------  -----------
System           10.48.74.123      1368354259     00:00:32
ipif1            172.18.1.2        1368355860     00:00:05

Total Entries : 2
```

The following example shows neighbor information of interface System.

```
Switch# show ip dvmrp neighbor System

Interface      Neighbor Address   Generation ID  Expire Time
-------------  ----------------   -------------  -----------
System         10.90.90.2         1368355860     00:00:31

Total Entries: 1
```

Field	Description
Interface	Specify the interface name.
Neighbor Address	Specify the neighbor's address of the specified interface.
Generation ID	Specify the generation ID of the neighbor. This value is dynamically generated by the neighbor switch, and it is used for the local switch to detect that whether the neighbor has restarted or not
Expire Time	After this time, the neighbor will be aged out if no new probe message received from the neighbor.

3-5 show ip dvmrp route

This command is used to display the DVMRP route info.

show ip dvmrp route [*IPADDRESS MASK***]**

Syntax Description	
IPADDRESS	Specify IP address. Together with the parameter *MASK*, specify displaying the route info for the specified network.
MASK	The mask of the IP address. If no network is specified, all route info will be displayed.

Default None

Command Mode User mode or Privileged mode.

Usage Guideline This command is used to display route information learned by DVMRP. If no parameter added, this command will display all the route information on the switch.

Example The following example displays all the route information learned by DVMRP.

```
Switch# show ip dvmrp route

DVMRP Routing Table

Source Address    Upstream Neighbor  Metric  Learned  Interface    Expire
/Netmask
----------------- -----------------  ------  -------  ------------ ------
2.0.0.0/8         10.90.90.90        2       Dynamic  System       00:01:22
10.0.0.0/8        10.90.90.2         1       Local    System       -

Total Entries: 2
```

This example displays routing information of .10.3.3.3 255.0.0.0

```
Switch# show ip dvmrp route 10.3.3.3 255.0.0.0

DVMRP Routing Table

Source Address  Upstream Neighbor   Metric  Learned  Interface   Expire
/Netmask
--------------  ---------------    ------  -------  ----------- ------
10.0.0.0/8      10.90.90.2         1       Local    System      -

Total Entries: 1
```

Field	Description
Source Address/Netmask	Specify the network address of this entry.
Upstream Neighbor	
Metric	Specify cost to this network. This value can be modified by command "**ip dvmrp metric**".
Learned	Specify the way to of learning this route entry. "Dynamic" means this route entry is learned by DVMRP route exchanging. "Local" means this route entry is a local route.
Interface	Specify this route entry is learned by the interface.
Expire	Specify how long until the entry is removed from the DVMRP route table. "-" means this entry will never expire (because it is a local interface).

Internet Group Management Protocol (IGMP) Commands

4-1 clear ip igmp group

Use this command to clear dynamic group member information obtained from the response messages in the IGMP buffer.

clear ip igmp group [*GROUP-ADDRESS* **| interface** *IFNAME***]**

Syntax Description	
N/A	Delete all dynamic group information.
GROUP-ADDRESS	Address of the multicast group. This is a multicast IP address in four-part dotted-decimal notation.
IFNAME	Interface name.

Default None

Command Mode Global configuration mode.

Usage Guideline The IGMP buffer includes a list that contains the dynamic multicast groups that the hosts in the direct subnet join. If the device joins a group, this group will be included in this list. To delete all the dynamic group entries from the IGMP buffer, use the **clear ip igmp group** command without parameters.

Example The following example shows how to clear all entries from the IGMP cache:

```
Switch# configure terminal
Switch(config)# clear ip igmp group
```

The following example shows how to clear entries for the multicast group 224.0.255.1 from the IGMP cache:

```
Switch# configure terminal
Switch(config)# clear ip igmp group 224.0.255.1
```

This example shows how to clear the IGMP-group cache entries from a specific interface of the IGMP-group cache:

```
Switch# configure terminal
Switch(config)# clear ip igmp group interface ipif1
```

4-2 ip igmp static-group

Use this command to directly add an interface to a group. You can use this command to add an interface to a group. Use the **no** form of this command to remove the setting.

ip igmp static-group *GROUP-ADDRESS*

no ip igmp static-group *GROUP-ADDRESS*

Syntax Description	
GROUP-ADDRESS	Address of the multicast group. This is a multicast IP address in four-part dotted-decimal notation.

Default The switch is not added to the multicast group manually.

Command Mode Interface configuration mode

Usage Guideline This command directly adds an interface to a multicast group. You can use this command to add an interface to a group.

Use command **show ip igmp groups static** to verify your setting.

Example Following example is to add a host group member manually:

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ip igmp static-group 233.3.3.3
```

4-3 ip igmp last-member-query-interval

To configure the interval at which the switch sends IGMP group-specific or group-source-specific (with IGMP Version 3) query messages, use the ip igmp last-member-query-interval command in interface configuration mode. To set this interval to the default value, use the **no** form of this command.

ip igmp last-member-query-interval *SECONDS*

no ip igmp last-member-query-interval

Syntax Description	
SECONDS	The interval sending the group query message in the range1 to 25, in seconds.

Default 1 second.

Command Mode Interface configuration mode

Usage Guideline When a device receives an IGMP Version 2 (IGMPv2) or IGMP Version 3 (IGMPv3) message indicating that a host wants to leave a group, source, or channel, it sends last-member-query-count(equal to robustness-variable) group, group-specific, or source-specific IGMP query messages at intervals set by the **ip igmp last-member-query-interval** command. If no response is received after this period, the device stops forwarding for the group, source, or channel.

Use command **show ip igmp interface** to verify your setting.

Example The following example sets the interval of sending the group query message to 20 seconds on interface VLAN 1:

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ip igmp last-member-query-interval 20
```

4-4 ip igmp query-interval

Use this command to configure the query interval of an ordinary member. Use the **no** form to set the query interval of ordinary member to the default value.

ip igmp query-interval *SECONDS*

no ip igmp query-interval

Syntax Description	
SECONDS	Query interval of ordinary member, in second. The range is 1 to 31744 seconds.

Default 125 seconds

Command Mode Interface configuration mode

Usage Guideline The time to query an ordinary member can be changed by configuring the query interval of the ordinary member.

Use command **show ip igmp interface** to verify your setting.

Example Configure the query interval of ordinary member to 120 seconds on the interface VLAN 1.

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ip igmp query-interval 120
```

4-5 ip igmp query-max-response-time

Use this command to configure the maximum response interval. Use the **no** form of this command to set the maximum response interval to the default value.

ip igmp query-max-response-time *SECONDS*

no ip igmp query-max-response-time

Syntax Description	
SECONDS	The maximum response interval, in second. The range is 1 to 25 seconds.

Default 10 seconds

Command Mode Interface configuration mode

Usage Guideline This command controls the interval for the respondent to respond the query message before the device deletes the group information.

Use command **show ip igmp interface** to verify your setting.

Example Configure the maximum response interval to 20 seconds on the interface VLAN 1.

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ip igmp query-max-response-time 20
```

4-6 ip igmp robustness-variable

Use this command to change the value of the robustness variable. Use the **no** form of this command to restore it to the default value.

ip igmp robustness-variable *NUMBER*

no ip igmp robustness-variable

Syntax Description	
NUMBER	The value of robustness variable ranging 1 to 7.

Default 2

Command Mode Interface configuration mode

Usage Guideline The Robustness Variable allows tuning for the expected packet loss on a network. If a network is expected to be lossy, the Robustness Variable may be increased. IGMP is robust to (Robustness Variable - 1) packet losses.

Use command **show ip igmp interface** to verify your setting.

Example The following example sets the value of robustness variable to 3 on the interface VLAN 1:

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ip igmp robustness-variable 3
```

4-7 ip igmp version

Use this command to set the version number of IGMP to be used on the interface. Use the **no** form of this command to restore it to the default value.

ip igmp version {1 | 2 | 3}

no ip igmp version

Syntax Description	
{1 | 2 | 3}	Three version numbers, ranging 1 to 3.

Default 3.

Command Mode Interface configuration mode.

Usage Guideline Use this command to configure the IGMP version. We recommend that all devices on the subnet support the same IGMP version.

Use command **show ip igmp interface** to verify your setting.

Example The following example sets the version number to 2 on the interface VLAN 1:

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ip igmp version 2
```

4-8 ip igmp check-subscriber-source-network

Use this command to configure the flag that determines whether or not to check the subscriber's source IP when an IGMP report or leave message is received. Use the **no** form of this command to disable the check.

ip igmp check-subscriber-source-network

no ip igmp check-subscriber-source-network

Syntax Description None

Default The switch will check the subscriber source network

Command Mode Interface configuration mode

Usage Guideline When the **ip igmp check-subscriber-source-network** command is enabled on an interface, any IGMP report or leave messages received by the interface will be checked to determine whether its source IP is in the same network as the interface. If it's not in the same network for a received report or leave message, the message won't be processed by the IGMP protocol. If the check is disabled, the IGMP report or leave message with any source IP will be processed by the IGMP protocol.

Use command **show ip igmp interface** to verify your setting.

Example The following example disables the subscriber source network check on the interface VLAN 1:

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# no ip igmp check-subscriber-source-network
```

4-9 show ip igmp interface

Use this command to show the information on the interface.

show ip igmp interface [*IFNAME***]**

Syntax Description	
IFNAME	Interface name.
N/A	Show information about all the interfaces.

Default None.

Command Mode User mode or Privileged mode.

Usage Guideline This command displays the IGMP configurations and some dynamic information on the switch or on a specified IP interface.

Example The following example shows the information of all the interfaces:

```
Switch# show ip igmp interface

Interface System
Internet Address is 10.90.90.90/8
IGMP is disabled on interface
Current IGMP router version is 2
IGMP query interval is 125 seconds
IGMP querier timeout is 0 seconds
IGMP max query response time is 10 seconds
Robustness variable is 2
Last member query interval is 1 second
IGMP check subscriber source network state is enabled
IGMP snooping is globally disabled
IGMP snooping is disabled on this interface
IGMP snooping fast-leave is disabled on this interface
IGMP snooping querier is disabled on this interface

Interface ipif1
Internet Address is 1.90.90.90/8
IGMP is enabled on interface
Current IGMP router version is 3
IGMP query interval is 125 seconds
IGMP querier timeout is 45 seconds
IGMP max query response time is 10 seconds
Robustness variable is 2
Last member query interval is 1 second
IGMP check subscriber source network state is enabled
IGMP snooping is globally enabled
IGMP snooping is enabled on this interface
IGMP snooping fast-leave is disabled on this interface
IGMP snooping querier is disabled on this interface
```

Field	Description
Internet address is...	Internet address of the interface and subnet mask being applied to the interface, as specified with the **ip address** command.
IGMP is disabled on interface	Indicates whether IGMP is active on the interface. The IGMP state will be automatically enabled when any multicast routing protocol (PIM or DVMRP) turns active, and be disabled if no any multicast routing protocol is active on the interface.
Current IGMP router version is 2	The IGMP running version on the interface, as specified with the **ip igmp version** command.
IGMP query interval is 125 seconds	Interval of the IGMP query message, as specified with the **ip igmp query-interval** command.
IGMP querier timeout is 0 seconds	The querier role expiring time. If this timer is running, there's other IGMP querier on this LAN.

IGMP max query response time is 10 seconds	Indicates the maximum allowed time before the host sending a responding report, as specified with the **ip igmp query-max-response-time** command.
Robustness variable is 2	Indicates the robustness value, as specified with the **ip igmp robustness-variable** command.
Last member query interval is 1 second	Indicates the interval of the switch sending last member query, as specified with the **ip igmp last-member-query-interval** command.
IGMP check subscriber source network state is enabled	Indicates IGMP will check whether the source IP of the received report/leave is in the same subnet with the receiving interface, as specified with the **ip igmp check-subscriber-source-network** command.
IGMP snooping is globally enabled	Indicates the IGMP snooping global state, as specified with the **enable ip igmp_snooping** command.
IGMP snooping is enabled on this interface	Indicates the IGMP snooping interface state, as specified with the **config ip igmp_snooping** command.
IGMP snooping fast-leave is disabled on this interface	Indicates the IGMP snooping fast-leave state, as specified with the **config ip igmp_snooping** command.
IGMP snooping querier is disabled on this interface	Indicates the IGMP snooping querier state is disabled, as specified with the **config ip igmp_snooping** command.

4-10 show ip igmp groups

Use this command to show the groups directly connected to the device and the group information learnt from IGMP.

show ip igmp groups [group *GROUP-ADDRESS* **| interface** *IFNAME***] [{detail | static}]**

Syntax Description	
N/A	Show the information about all the dynamic groups.
GROUP-ADDRESS	Address of the multicast group. This is a multicast IP address in four-part dotted-decimal notation.
IFNAME	Interface name.
static	Show the static group information, as specified with the **ip igmp static-group** command.
detail	Show detailed information.

Default None.

Command Mode User mode or Privileged mode.

Usage Guideline Use this command without any parameters to show group address, interface type, and information about all the multicast groups directly connected to the interface. Information about a specific group is displayed if key word **detail** is added to the command.

Example The following example shows information about all the groups:

```
Switch# show ip igmp groups
Interface     Multicast Group  Uptime      Group timer  Last Reporter
------------  ---------------  ----------  -----------  --------------
System        228.0.0.1        00:00:17    00:04:18     10.1.4.25
System        228.0.0.2        00:00:16    00:04:19     10.1.4.25
System        228.0.0.3        00:00:16    00:04:19     10.1.4.25
System        228.0.0.4        00:00:15    00:04:15     10.1.4.25
System        228.0.0.5        00:00:15    00:04:15     10.1.4.25
System        228.0.0.6        00:00:14    00:04:16     10.1.4.25
System        228.0.0.7        00:00:14    00:04:16     10.1.4.25
System        228.0.0.8        00:00:13    00:04:17     10.1.4.25
System        228.0.0.9        00:00:13    00:04:17     10.1.4.25
System        228.0.0.10       00:00:12    00:04:18     10.1.4.25
System        239.255.255.250  00:00:05    00:04:15     10.0.0.24

 Total Entries: 11
```

The following example shows detailed group information on a specific interface:

```
Switch# show ip igmp groups interface System detail
IGMP Group Detail Information

 Interface         : System
 Multicast Group   : 224.1.1.1
 Last Reporter : 10.0.31.1
 IP Querier    : SELF
 Up Time       : 00:00:19
 Group Timer   : 00:00:00
 Group Mode    : Include
 V1 Host Timer : 0
 V2 Host Timer : 0

 Source List Table:

    Source list        Timer(sec)
    ------------------ -----
    162.1.18.1         260
    162.1.18.2         260
    162.1.18.3         260
    162.1.18.4         260

    Total Source Entries: 4

Interface         : System
 Multicast Group   : 228.0.0.2
 Last Reporter : 10.1.4.25
 IP Querier    : SELF
 Up Time       : 00:02:46
 Group Timer   : 00:03:34
 Group Mode    : Exclude
 V1 Host Timer : 0
 V2 Host Timer : 214 seconds

 Source List Table:
     NULL

 Total Entries: 2
```

The following example shows detailed information of a specific group:

```
Switch# show ip igmp groups group 224.1.1.1 detail
IGMP Group Detail Information

 Interface         : System
 Multicast Group   : 224.1.1.1
 Last Reporter : 10.0.31.1
 IP Querier    : SELF
 Up Time       : 00:00:19
 Group Timer   : 00:00:00
 Group Mode    : Include
 V1 Host Timer : 0
 V2 Host Timer : 0

 Source List Table:

    Source list        Timer(sec)
    ------------------ -----
    162.1.18.1         260
    162.1.18.2         260
    162.1.18.3         260
    162.1.18.4         260

    Total Source Entries: 4

 Total Entries: 1
```

The following example shows the static group information:

```
Switch# show ip igmp groups static
Interface        Multicast Group
------------    ---------------
System           225.1.1.1
System           235.0.0.0

Total Entries: 2
```

Field	Description
Last Reporter	Specify the IP address of the host who sent the last IGMP report to this group.
IP Querier	Specify the querier's IP address on this LAN. SELF indicates this switch itself is the querier.
Up time	Time of the multicast group being learned.
Group timer	Time of the multicast group will be expired if no any more refresh.

V1 Host Timer	In seconds. The non-zero V1 Host Timer means the switch is running in Group Compatibility mode of IGMPv1 for the group. The IGMPv1 Host Present timer is set to Older Version Host Present Timeout seconds whenever an IGMPv1 Membership Report is received.
V2 Host Timer	In seconds. The non-zero V2 Host Timer means the switch is running in Group Compatibility mode of IGMPv2 for the group. The IGMPv2 Host Present timer is set to Older Version Host Present Timeout seconds whenever an IGMPv2 Membership Report is received.
Source List Table	Specify the source addresses' info of the multicast group in IGMPV3 reports.

Interface Commands

5-1 interface loopback

Use this command to create a loopback interface and enter the interface configuration mode. Use the no form of this command to delete a loopback interface

interface loopback <int>

no interface loopback <int>

Syntax Description	
int	The loopback interface number.

Default None.

Command Mode Global configuration mode

Usage Guideline Users can verify the settings by entering the show interface loopback command.

Example Create a loopback interface 2 and configure IP 10.1.1.1/8 to it.

```
Switch(config)# interface loopback 2
Switch(config-if)# ip address 10.1.1.1 255.0.0.0
```

5-2 shutdown

Use the command to disable an interface. Use the **no** command to enable an interface.

shutdown

no shutdown

Syntax Description None.

Default Default the interface is enabled.

Command Mode Interface configuration mode.

Usage Guideline This command is used to disable or enable an interface. You can verify the settings by entering the show interface loopback command.

Example To shutdown the loopback interface 1.

```
Switch(config)# interface loopback 1
Switch(config-if)# shutdown
```

5-3 show interface loopback

Use this command to display all the IP interfaces.

show interface loopback <int>

Syntax Description	
int	The loopback interface number.

Default None

Command Mode User mode or Privileged mode.

Usage Guideline Use this command to display the loopback interface.

Example To show interface loopback 2.

```
Switch# show interface loopback 2
Interface                    : loopback2
Interface Admin State        : Enabled
IPv4 Address                 : 10.1.1.1/8 (MANUAL)
```

IP Access List Commands

6-1 ip standard access-list

Use this command to enter the access list configuration mode and define a standard IP access list. Use the **no** form of this command to remove a standard IP access list.

ip standard access-list *ACCESS-LIST-NAME*

no ip standard access-list *ACCESS-LIST-NAME*

Syntax Description	
ACCESS-LIST-NAME	The name of the ip access-list to be configured. It can accept up to 16 characters. The syntax is general string that does not allow space.

Default None

Command Mode Global configuration mode.

Usage Guideline Standard IP access list is used by routing protocol.
Both the maximum number of standard IP access lists are 256 and the maximum number of rules in one standard IP access list are 16.

Users can verify the settings by entering the **show ip standard access-list** command.

Example To create an standard IP access list and enter the standard IP access list configuration mode:

```
Switch# configure terminal
Switch(config)# ip standard access-list Summer-Movie
Switch(config-ip-acl)#
```

6-2 deny

Use this command to set the deny rules of standard IP access list. Use the **no** form of this command to remove the deny rules.

deny *NETWORK-ADDRESS*

no deny *NETWORK-ADDRESS*

Syntax Description	
NETWORK-ADDRESS	Specifies a specific network address.

Default None.

Command Mode Access list configuration mode.

Usage Guideline One or multiple deny rules can be added to the list.
The maximum number of rules in one standard IP access list is 16.
There is an implicit deny at the end of the statement, if you only want to deny some specified route, please add another statement which is permit 0.0.0.0/0 at the end of the ip access list, in that way there will be no negative effects on the function of access list.

Users can verify the settings by entering the **show ip standard access-list** command.

Example To configure deny rules for a standard IP access list:

```
Switch# configure terminal
Switch(config)# ip standard access-list Summer-Movie
Switch(config-ip-acl)# deny 121.2.0.0/16
Switch(config-ip-acl)# deny 126.1.2.2/20
Switch(config-ip-acl)# exit
Switch(config)#
```

6-3 permit

Use this command to set the permit rules of standard IP access list. Use the **no** form of this command to remove the permit rules.

permit *NETWORK-ADDRESS*

no permit *NETWORK-ADDRESS*

Syntax Description	
NETWORK-ADDRESS	Specifies a specific network address.

Default None.

Command Mode Access list configuration mode.

Usage Guideline One or multiple permit rules can be added to the list.
The maximum number of rules in one standard IP access list is 16.

Users can verify the settings by entering the **show ip standard access-list** command.

Example To configure permit rules for a standard IP access list:

```
Switch# configure terminal
Switch(config)# ip standard access-list Summer-Movie
Switch(config-ip-acl)# permit 120.2.0.0/16
Switch(config-ip-acl)# permit 125.1.2.2/20
Switch(config-ip-acl)# exit
Switch(config)#
```

6-4 show ip standard access-list

Use this command to display the access-list configuration.

show ip standard access-list [*ACCESS-LIST-NAME***]**

Syntax Description	
ACCESS-LIST-NAME	(Optional) Specifies the name of a standard IP access list.

Default None.

Command Mode Privileged mode.

Usage Guideline Use this command to display the access-list configuration.

Example To show the content of standard IP access list “Summer-Movie”:

```
Switch# show ip standard access-list Summer-Movie

IP Standard Access-list:  Summer-Movie
Total Entries Number    :  2
      Permit 120.2.0.0/16
      Deny 125.1.2.2/20

Switch#
```

Field	Description
IP Standard Access-list	The name of standard IP access list. It is specified with the command **ip standard access-list**.
Total Entries Number	The total number of rules in this standard IP access list.
Permit/deny *NETWORK-ADDRESS*	Rules of the standard IP access list. They are specified with the command **permit** and **deny**.

IP Multicast (IPMC) Commands

7-1 ip mroute

Use this command to create static routes for multicast. Use the no form of this command to delete the static routes.

ip mroute *SOURCE-ADDRESS MASK* **{***RPF-ADDRESS* **| null}**

no ip mroute {*SOURCE-ADDRESS MASK* **| all }**

Syntax Description	
SOURCE-ADDRESS	Source IP address of the static route.
MASK	The network mask of the static route.
RPF-ADDRESS	Specify the RPF neighbor address. The interface where the RPF neighbor IP address is located is the RPF interface
null	If null is defined for the source network, RPF check will always fail for multicast traffic sent from this source network.
all	Specify that all the IP multicast static routes will be deleted

Default No IP multicast static route exists.

Command Mode Global configuration mode.

Usage Guideline This command is used to create an IP multicast static route entry used by PIM to do RPF check. When an IP multicast packet is received, the source IP address of the packet will be used to do the RPF check. If the source IP address of the received IP multicast packet matches the source network in a multicast static route, then it will be allowed only when it comes from the RPF interface, and it will be RPF check failed if it comes from other interfaces. If the source IP address of the received IP multicast packet does not match any multicast static route source network, dynamic unicast route will be used by PIM for RPF check.

To verify you configuration, use command **show ip mroute static**.

Example The following example creates a static route for network 139.1.1.1 255.255.0.0 for which the RPF interface neighbor address is 192.168.1.1.

```
Switch# configure terminal
Switch(config)# ip mroute 139.1.1.1 255.255.0.0 192.168.1.1
Switch(config)# end
```

The following example configures the RPF checking for source network 10.1.1.1/16 always fails.

```
Switch# configure terminal
Switch(config)# ip mroute 10.1.1.1 255.255.0.0 null
Switch(config)#end
```

Delete a multicast static route for source network 10.1.1.1 255.255.0.0.

```
Switch# configure terminal
Switch(config)# no ip mroute 10.1.1.1 255.255.0.0
Switch(config)#end
```

Delete all multicast static routes.

```
Switch# configure terminal
Switch(config)# no ip mroute all
Switch(config)# end
```

7-2 ip multicast-routing

This command enables global IP multicast routing. The **no** form of the command disables global IP multicast routing.

ip multicast-routing

no ip multicast-routing

Syntax Description None.

Default Disabled.

Command Mode Global configuration mode.

Usage Guideline When IP multicast routing is disabled, the system will stop routing of multicast packets even though the multicast routing protocol is enabled. If you want to use IP multicast routing for forwarding, you need use the **ip multicast-routing** command to enable global IP multicast routing state. When this command and any multicast routing protocol are both enabled, IGMP will automatically be enabled on the interface, and then the multicast routing forwarding can take effect.

To verify you configuration, use the command **show ip multicast-routing**.

Example Enable global IP multicast routing.

```
Switch# configure terminal
Switch(config)# ip multicast-routing
Switch(config)# end
```

Disable global IP multicast routing.

```
Switch# configure terminal
Switch(config)# no ip multicast-routing
Switch(config)# end
```

7-3 show ip mroute

Use this command to display IP multicast routing information.

show ip mroute [{[*GROUP-ADDRESS* **[***SOURCE-ADDRESS***] | dense | sparse | dvmrp | summary] | static }]**

Syntax Description	
GROUP-ADDRESS	Multicast group IP address.
SOURCE-ADDRESS	Multicast source IP address.
dense	Display PIM-DM multicast routing table.
sparse	Display PIM-SM multicast routing table.
dvmrp	Display DVMRP multicast routing table.
summary	Display a one-line, abbreviated summary of each entry in the IP multicast routing table.
static	Display the multicast static routes

Default None.

Command Mode User mode or Privileged mode

Usage Guideline This command is used to display the multicast routing entries learned on the switch or the multicast static routes created on the switch. You can specify the parameter to display the information that you concerning. If no parameter is specified, all IP multicast routing entries learned on the switch will be displayed.

Example The following example displays multicast route brief information.

```
Switch# show ip mroute summary

IP Multicast Routing Table: 2 entries
Flags: D – Dense, S – Sparse, V – DVMRP
Timers: Uptime/Expires

(10.10.1.52, 224.0.1.3), vlan1, 00:01:32/00:03:20, Flags: D
(20.1.1.1, 228.10.2.1), vlan10, 00:05:10/00:03:11, Flags: S
```

The following example displays all IP multicast routing information on the system.

```
Switch# show ip mroute

IP Multicast Routing Table
Flags: D - Dense, S - Sparse, V - DVMRP, s - SSM Group, F - Register flag
       P - Pruned, R - (S, G) RPT-bit set, T - SPT-bit set
Outgoing interface flags: W - Assert winner
Timers: Uptime/Expires

 (10.71.57.210, 235.0.0.4), 00:02:53/00:00:37, Flags: ST
  Incoming interface: System, RPF neighbor: 1.2.0.1
  Outgoing interface List:
VLAN3, Forwarding 00:00:04/00:04:20

 (20.2.2.10, 239.0.0.5), 00:02:53/00:00:37, Flags: VP
  Incoming interface: VLAN20, RPF neighbor: 2.3.0.1
  Outgoing interface List: NULL

 (30.9.7.4, 237.0.0.6), 00:02:53/00:00:37, Flags: D
  Incoming interface: VLAN30, RPF neighbor: 6.2.3.2
  Outgoing interface List:
 VLAN5, Forwarding

Total Entries: 3
```

The following example displays IP multicast routing information learned by PIM sparse mode.

```
Switch# show ip mroute sparse

(10.1.57.1, 235.0.0.0), 00:00:04/00:03:26, Flags: ST
  Incoming interface: System, RPF neighbor: NULL
  Outgoing interface list:
   ip4, Forwarding 00:00:04/00

Total Entries: 1
```

The following example displays IP multicast routing information for group source part (239.0.0.5, 20.2.2.10).

```
Switch#show ip mroute 239.0.0.5 20.2.2.10

(20.2.2.10, 239.0.0.5), 00:02:53/00:00:37, Flags: VP
  Incoming interface: VLAN20, RPF neighbor: 2.3.0.1
Outgoing interface List: NULL

Total Entries: 1
```

The following example displays the multicast static routes created on the system.

```
Switch#show ip mroute static

Mroute: 10.0.0.0/8, RPF neighbor: 11.1.1.1
Mroute: 11.0.0.0/8, RPF neighbor: NULL

 Total Entries   : 2
```

Field	Description
D - Dense	The entry is operating in PIM-DM mode.
S - Sparse	The entry is operating in PIM-SM mode.
s - SSM Group	The entry is a member of an SSM group.
V - DVMRP	The entry is operating in DVMRP mode.
F - Register Flag	Status of whether the software is registering for a multicast source.
P - Pruned	Route has been pruned. This information indicates that this switch has no outgoing for this group.
R (S, G) RPT-bit set	Specify this switch is the RPT upstream for this group, and this group is forwarding in SPT. The downstream switch has sent (S, G) prune message to this switch.
T – SPT-bit set	Status of whether the packets have been received on the shortest-path tree.
W - Assert winner	Assert winnerSpecify this outgoing is in assert state, and it is a assert winner.
(172.18.16.1, 235.0.0.0)	The source address and group address for this entry.
Uptime/Expire	The uptime and expire time for this entry.
RPF neighbor	The RPF neighbor address for the specified network address, as specified by command “**ip mroute**”.

7-4 show ip rpf

Use this command to show the RPF information for the specified source address.

show ip rpf *SOURCE-ADDRESS*

Syntax Description	
SOURCE-ADDRESS	Specify the source IP address.

Default None.

Command Mode User mode or Privileged mode

Usage Guideline This command is used to display the RPF information of the specified source address. The static multicast routing information, which created by command ip mroute, prefer than RPF information learnt by unicast routing protocol.

Example Display RPF information of 10.0.0.1

```
Switch# show ip rpf 10.0.0.1

Source IP:10.0.0.1
RPF interface: System
Type: unicast
Metric: 1
```

Display RPF information of 20.0.0.1

```
Switch# show ip rpf 20.0.0.1

Source IP:20.0.0.1
RPF interface: VLAN3
Type: unicast
Metric: 4
```

Display RPF information for 30.0.0.1

```
Switch# show ip rpf 30.0.0.1

Source IP:30.0.0.1
RPF interface: VLAN2
Type: unicast
Metric: 2
```

Display RPF information of 172.18.61.8

```
Switch# show ip rpf 172.18.61.8

Source IP:172.18.61.8
RPF address: 192.18.16.1
Type: Static
```

Field	Description
Source IP	Indicate the source IP address.
RPF interface	Indicate the RPF interface name for the specified source address.
Type	Specify the way the switch gets the RPF information. It can be Local, any unicast routing protocol or static configured.
Metric	The metric to achieve to the source network from the local switch.
RPF address	Specify RPF neighbor address, created by command “**ip mroute**”.

7-5 show ip multicast interface

Use to display the basic multicast information of an interface.

show ip multicast interface [*IFNAME* **]**

Syntax Description	
IFNAME	Specify the interface name.

Default None.

Command Mode User mode or Privileged mode.

Usage Guideline This command is used to display the basic multicast interface information, if no parameter specified, this command will display information for all interfaces.

Example Display all multicast interface info on the whole system.

```
Switch# show ip multicast interface

Interface Name  IP Address         Multicast Routing
--------------- ---------------    ------------------
System          10.90.90.90/8      PIM-SM
VLAN1           1.0.90.3/8         DVMRP
VLAN2           2.4.2.2/8          PIM-DM
VLAN3           3.4.4.3/8          N/A

Total Entries: 4
```

Display multicast interface info on interface VLAN1:

```
Switch# show ip multicast interface VLAN1

Interface Name  IP Address         Multicast Routing
--------------- ---------------    ------------------
VLAN1           1.0.90.3/8         DVMRP

Total Entries: 1
```

Field	Description
Interface Name	Name of the interface.
IP Address	IP address of the interface.
Multicast Routing	The multicast routing protocol running on the interface. N/A means no any multicast routing protocol is active on the interface.

7-6 show ip multicast-routing

Use this command to display IP multicast routing global state.

show ip multicast-routing

Syntax Description None.

Default None.

Command Mode User mode or Privileged mode.

Usage Guideline This command is used to display the IP multicast routing global state.

Example Display IP multicast routing informaiton.

```
Switch# show ip multicast-routing
IP multicast routing state: Enabled
```

Field	Description
IP multicast routing state	This state can be modified by command "**ip multicast-routing**".

IP Prefix List Commands

8-1 ip prefix-list

Use this command to create an IP prefix list or add a rule for an IP prefix list. Use the **no** form of this command to remove an IP prefix list or remove a rule for an IP prefix list.

ip prefix-list *PREFIX-LIST-NAME* **[[seq** *SEQ-NUMBER***] {deny | permit}** *NETWORK-ADDRESS* **[ge** *MINIMUM-PREFIX-LENGTH***] [le** *MAXIMUM-PREFIX- LENGTH***]]**

no ip prefix-list *PREFIX-LIST-NAME* **[[seq** *SEQ-NUMBER***] {deny | permit}** *NETWORK-ADDRESS* **[ge** *MINIMUM-PREFIX-LENGTH***] [le** *MAXIMUM-PREFIX- LENGTH***]]**

Syntax Description

PREFIX-LIST-NAME	The name of the IP prefix list. It can accept up to 16 characters. The syntax is general string that does not allow space.
seq *SEQ-NUMBER*	(Optional) Specifies the sequence number of the rule entry. The range is 1 to 65535.
deny	(Optional) Specifies the rule to deny the access when matched.
permit	(Optional) Specifies the rule to permit the access when matched.
NETWORK-ADDRESS	(Optional) Specifies the network address to match.
ge *MINIMUM-PREFIX-LENGTH*	(Optional) Specifies the minimum prefix length used to match the network address. The range is 1 to 32.
le *MAXIMUM-PREFIX-LENGTH*	(Optional) Specifies the maximum prefix length used to match the network address. The range is 1 to 32.

Default None.

Command Mode Global configuration mode

Usage Guideline The **ip prefix-list** command is used to create or configure an IP prefix list.

An IP prefix list can have multiple rule entries; each is represented by a sequence number. The rule with the lower sequence number will be evaluated first. If the sequence number is not specified for the defined rule entry, the sequence number will be automatically given. The automatically given sequence number will be a multiple of 5. Therefore, if the defined rule is the first rule in the prefix list, the automatically given sequence number will be 5. If the defined rule is not the first rule in the prefix list, the sequence number will be the number that is a multiple of 5 and larger than the largest sequence number of an existing rule in the prefix list.

A prefix list consists of an IP address and a bit mask. The bit mask is entered as a number from 1 to 32. An implicit denial is applied to traffic that does not match any prefix list entry. The IP route prefix list rule entry is defined to either permit or deny specific routes. Prefix lists are configured to match an exact prefix length or a prefix range.

The prefix list is processed using an exact match when neither the **ge** nor **le** is specified. If only the **ge** is specified, the range of the mask length used to match the network address is from the minimum prefix length to a full 32-bit length. If only the **le** is specified, the range of the mask length is from prefix length of network to the maximum prefix length. If both the **ge** and **le** is specified, the range of the mask length falls between the minimum prefix length and the maximum prefix length.
There is a restriction about the minimum prefix length and the maximum prefix length:
prefix length of network < the minimum prefix length < the maximum prefix length <= 32
For example:
If the specified network address is 10.1.2.3/16 and none of **ge** and **le** is specified, only the route 10.1.0.0/16 will match the rule. The route 10.1.2.0/24 will not.
If the network address is 10.1.0.0/16 and **ge** 24 is specified, the route 10.1.0.0/16 will not match the rule. The route 10.1.2.0/24 and the route 10.1.2.3/32 will match the rule.

There is a limitation about maximum number of IP prefix list and it is 256.

You can verify your settings by entering the **show ip prefix-list** command.

Example

To create and configure the IP prefix-list named “my_pref” to permit routes from the 10.0.0.0/8 network while set the maximum prefix length to 24:

```
Switch# configure terminal
Switch(config)# ip prefix-list my_pref permit 10.0.0.0/8 le 24
Switch(config)#
```

To create and configure the IP prefix-list named “ my_pref” to deny routes from the 12.0.0.0/12 network while set minimum prefix length to 20 and maximum prefix length to 24:

```
Switch# configure terminal
Switch(config)# ip prefix-list my_pref deny 12.0.0.0/12 ge 20 le 24
Switch(config)#
```

8-2 ip prefix-list description

Use this command to add the text description to a prefix list. Use the **no** form of this command to delete the description.

ip prefix-list *PREFIX-LIST-NAME* **description** *DESC*

no ip prefix-list *PREFIX-LIST-NAME* **description**

Syntax Description	
PREFIX-LIST-NAME	Specifies the name of the IP prefix list. It can accept up to 16 characters. The syntax is general string that does not allow space.
DESC	Specifies the text description. It supports maximum 80 characters.

Default None.

Command Mode Global configuration mode

Usage Guideline Use the **ip prefix-list description** command to add or delete the text description of an IP prefix list.

You can verify your settings by entering the **show ip prefix-list** command.

Example To set the description of one IP prefix list:

```
Switch# configure terminal
Switch(config)# ip prefix-list my_pref description allow routes from peer A
Switch(config)#
```

8-3 clear ip prefix-list counter

Use this command to reset hit counte of IP prefix list.

clear ip prefix-list counter {*PREFIX-LIST-NAME* [*NETWORK-ADDRESS*] |**all**}

Syntax Description	
PREFIX-LIST-NAME	Specifies the name of the IP prefix list. It can accept up to 16 characters. The syntax is general string that does not allow space.
NETWORK-ADDRESS	(Optional) Specifies the network entry of IP prefix list.
all	Clear the hit count of all IP prefix lists

Default None

Command Mode Privileged mode

Usage Guideline The hit count is the value that indicates the times of an prefix list entry is matched.

Example To clear the counter of all ip prefix-list:

```
Switch# clear ip prefix-list counter all
```

8-4 show ip prefix-list

Use this command to show the information about IP prefix list.

show ip prefix-list [*PREFIX-LIST-NAME*]

Syntax Description	
PREFIX-LIST-NAME	(Optional) Show information of specified IP prefix list.

Default None.

Command Mode Privileged mode.

Usage Guideline Use this command to show the information about IP prefix list.

Example To show the information of IP prefix list “my_pref”:

```
Switch# show ip prefix-list my_pref

IP Prefix List:  my_pref
Description: allow routes from peer A
Total Rule Number: 1
     Sequence 5 Permit 10.0.0.0/8 le 24

Switch#
```

show ip prefix-list Field Description:

Field	Description
IP Prefix List	The name of IP prefix list. It is specified with the command **ip prefix-list**.
Total Rule number	Rules number of the IP prefix list.

IP Route Commands

9-1 clear ip route

Use this command to remove all or specified static routes from the IP routing table.

clear ip route [vrf *VRF-NAME***] {* | *NETWORK* [***NET-MASK***]}**

Syntax Description	
vrf *VRF-NAME*	(Optional) Specifies to remove all routes of one VRF.
*	Specifies to remove all static routes.
NETWORK	IP address and network address are both accepted. If *NET-MASK* is not specified, the longest prefix matched route will be removed.
NET-MASK	(Optional) Specifies the network mask of the destination network.

Default None

Command Mode Privileged mode

Usage Guideline Use this command to remove all the static routes or the specified static routes from the IP routing table. If there are multi-paths to one destination, all these static routes will be removed.

Users can verify the settings by entering the **show ip route static** command.

Example Remove the static route 33.3.3.0/24:

```
Switch# clear ip route 33.3.3.0 255.255.255.0
```

Remove all static routes:

```
Switch# clear ip route *
```

Remove the static route 33.3.3.0/24 in VRF VPN-A:

```
Switch# clear ip route vrf VPN-A 33.3.3.0 255.255.255.0
```

9-2 route-preference default

Use this command to set the preference of static default route. Use **no** form of this command to restore it to the default setting.

route-preference [vrf *VRF-NAME***] default** *VALUE*

no route-preference [vrf *VRF-NAME***] default**

Syntax Description	
vrf *VRF-NAME*	(Optional) Specifies to set the route preference of VRF routing table.
VALUE	Preference of static default route. The value range is 1-999.

Default The default value of the static default route's preference is 1.

Command Mode Global configuration mode

Usage Guideline This command sets the preference of static default routes.
Among the different type default routes, the one with the lowest preference will be established as the active route. If that route has been found failed, then this route will be automatically deactivated and the route with the next lower preference will be the active route.

Users can verify the settings by entering the **show ip route-preference** command.

Example Set the preference of static default route to 50:

```
Switch# configure terminal
Switch(config)# route-preference default 50
```

Set the preference of static default route to 90 in VRF VPN-A:

```
Switch# configure terminal
Switch(config)# route-preference vrf VPN-A default 90
```

9-3 route-preference static

Use this command to set the preference of static route. Use **no** form of this command to restore to the default setting.

route-preference [vrf *VRF-NAME***] static** *VALUE*

no route-preference [vrf *VRF-NAME***] static**

Syntax Description	
vrf *VRF-NAME*	(Optional) Specifies to set the route preference of VRF routing table.
VALUE	Preference of static route. The value range is 1-999.

Default The default value of static route's preference is 60.

Command Mode Global configuration mode.

Usage Guideline Among the different type routes with same destination network address, the one with the lowest preference will be established as the active route. If that route has been found failed, then this route will be automatically deactivated and the route with the next lower preference will be the active route.

Users can verify the settings by entering the **show ip route-preference** command.

Example Set the preference of static route to 100:

```
Switch# configure terminal
Switch(config)# route-preference static 100
```

Set the preference of static route to 60 in VRF VPN-A:

```
Switch# configure terminal
Switch(config)# route-preference vrf VPN-A static 60
```

9-4 ip mtu

Use this command to set the Maximum Transmission Unit (MTU) size of IP packets sent on an interface. Use the **no** form of this command to restore to the default setting.

ip mtu *BYTES*

no ip mtu

Syntax Description	
BYTES	Maximum Transmission Unit of IP packet. The value range is 512-16383.

Default The default value of IP MTU is 1500

Command Mode Interface configuration mode

Usage Guideline If an outgoing IP packet from CPU interface exceeds the MTU set for the interface, software will fragment it before sending out.
Note: Changing the MTU value (with the jumbo frame command) won't affect the IP MTU value, vice verse is same. Therefore you should care both MTU and IP MTU sizes to make the system working correctly. For example, if IP MTU is larger than MTU at the egress port, the packet larger than MTU but less than IP MTU may be dropped by the egress port.

Use **show ipif** to see the current setting of IP MTU

Example Set the IP MTU of System (vlan 1) interface to 800 bytes:

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ip mtu 800
```

9-5 ip ecmp load-balance

Use this command to set the load-balancing algorithm for ECMP/WCMP route. Use **no** form of this command to remove the configuration set before.

ip ecmp load-balance [{sip | crc32_lower | crc32_upper} | dip | port](1)

no ip ecmp load-balance [{sip | crc32_lower | crc32_upper} | dip | port]

Syntax Description	
sip	(Optional) Specifies that the load-balancing algorithm will include the lower 5 bits of the source IP address. This attribution is mutually exclusive with crc32_lower and crc32_upper. If it is set, crc32_lower and crc32_upper will be excluded.
crc32_lower	(Optional) Specifies that the load-balancing algorithm will include the lower 5 bits of the CRC32 hash. This attribution is mutually exclusive with crc32_upper and sip. If it is set, crc32_upper and sip will be excluded.
crc32_upper	(Optional) Specifies that the load-balancing algorithm will include the upper 5 bits of the CRC32 hash. This attribution is mutually exclusive with crc32_lower and sip. If it is set, crc32_lower and sip will be excluded.
dip	(Optional) Specifies that the load-balancing algorithm will include the destination IP address.
port	(Optional) Specifies that the load-balancing algorithm will include the TCP or UDP port.

Default

By default, **dip** and **crc32_lower** is set.

Command Mode

Global configuration mode.

Usage Guideline

User can use any combination of **dip**, **port**, **sip**, **crc32_lower** or **crc32_upper** to build the Hash algorithm. **sip**, **crc32_lower** or **crc32_upper** are mutually exclusive with each other. User is required to select one and only one of them.

The **no** form of this command will remove the keywords it carries with as the components of a key from the saved setting. For example, if the system saves the setting of **sip**, **dip** and **port**. After the **no ip ecmp load-balance dip port** is executed, only **sip** is available for the key. If the **no** form of this command has the keywords not in the saved settings, the command runs properly. If using the **no** form of this command without any keywords, the configuration will go back to the default settings.

Use **show ip ecmp load-balance** to check the current setting of load-balancing algorithm.

Example

Set the load-balancing algorithm to use sip and TCP or UDP port:

```
Switch# configure terminal
Switch(config)# ip ecmp load-balance sip port
```

9-6 ip route

Use this command to add a static route entry. Use **no** form of this command to remove a static route entry. Primary and backup are mutually exclusive. Users can select only one when creating a new route. If user sets neither of these, the system will try to set the new route first by primary and second by backup and not set this route to be a multipath route. The weight is used to configure the weighted multiple paths (WCMP) function.

ip route [vrf *VRF-NAME***]** *NETWORK NET-MASK* **{***IP-ADDRESS* **[{primary | backup | weight** *NUMBER***}] | null0 | ip_tunnel** *TUNNEL-NAME***}**

no ip route [vrf *VRF-NAME***]** *NETWORK NET-MASK* **{***IP-ADDRESS* **| null0 | ip_tunnel** *TUNNEL-NAME***}**

Syntax Description	
vrf *VRF-NAME*	(Optional) Specifies to add this static route to the VRF routing table.
NETWORK	Specifies the network address of the destination. The destination of the route is determined by network and net-mask.
NET-MASK	Specifies the network mask of the destination.
IP-ADDRESS	Specifies the IP address of the next-hop router.
primary	(Optional) Specifies the route as the primary route to the destination.
backup	(Optional) Specifies the route as the backup route to the destination.
weight *NUMBER*	(Optional) Specifies the weight number greater than zero, but not greater than the maximum paths number for the WCMP. This number is used to replicate identical route path (multiple copies) in routing table, so the path get more chance to be hit for traffic routing.
null0	Specifies a black hole route.
ip_tunnel *TUNNEL-NAME*	Specifies to use an IP tunnel as the next-hop.

Default By default no static route is configured.

Command Mode Global configuration mode

Usage Guideline When the value of *NETWORK* and *NET-MASK* are both 0.0.0.0, it means to create a static default route.
Use the command with keyword **primary** or **backup** means the newly created route is a floating static route. The keyword **weight** means the newly created route is a static multipath route. The floating static route and the static multipath route are mutually exclusive. If none of the following parameters, "**primary**", "**backup**" or "**weight**," are selected (and **ip_tunnel** is not used), the static route will be
1. primary if there is no primary route to the same destination.
2. backup if there has been a primary route to the same destination.
3. fail to create if there have been a primary route and a backup route to the same destination.

4. fail to create if there has been one static multipath route to the same destination.

If **null0** is specified for one route, the traffic that matched its destination will be dropped.

Users can verify the settings by entering the **show ip route static** command.

Example

Add a static route entry with destination 20.0.0.0/8 and nexthop 10.1.1.254:

```
Switch# configure terminal
Switch(config)# ip route 20.0.0.0 255.0.0.0 10.1.1.254
```

Add a static weighted multipath route entry with destination 30.0.0.0/8 and two nexthops: 10.1.1.253, 10.1.1.254:

```
Switch# configure terminal
Switch(config)# ip route 30.0.0.0 255.0.0.0 10.1.1.253 weight 1
Switch(config)# ip route 30.0.0.0 255.0.0.0 10.1.1.254 weight 1
```

Add a static route entry with destination 40.0.0.0/8 and nexthop 10.1.1.254 and specify this route to be a backup static route.

```
Switch# configure terminal
Switch(config)# ip route 40.0.0.0 255.0.0.0 10.1.1.254 backup
```

Remove the static route with destination 20.0.0.0/8 and nexthop 10.1.1.254:

```
Switch# configure terminal
Switch(config)# no ip route 20.0.0.0 255.0.0.0 10.1.1.254
```

Add a static route using IP tunnel:

```
Switch# configure terminal
Switch(config)# ip route 100.1.1.0 255.255.255.0 ip_tunnel tunnel_1
```

To add a static route to VRF VPN-A:

```
Switch# configure terminal
Switch(config)# ip vrf VPN-A
Switch(config-vrf)# exit
Switch(config)# ip route vrf VPN-A 100.1.1.0 255.255.255.0 10.1.1.253
Switch(config)#
```

9-7 show ip route-preference

Use this command to display the preference of different route types.

show ip route-preference [vrf *VRF-NAME*] **[{connected | static | default | rip | ospf | ospfIntra | ospfInter | ospfExt1 | ospfExt2 | ebgp | ibgp}]**

Syntax Description	
vrf *VRF-NAME*	(Optional) Specifies to show the route preference of different route types of the VRF routing table.
connected	(Optional) Specifies to show the route preference of connected route.
static	(Optional) Specifies to show the route preference of static route.
default	(Optional) Specifies to show the route preference of static default route.
rip	(Optional) Specifies to show the route preference of RIP route.
ospf	(Optional) Specifies to show the route preference of all types of OSPF route.
ospfintra	(Optional) Specifies to show the route preference of OSPF intra-area route.
ospfInter	(Optional) Specifies to show the route preference of OSPF inter-area route.
ospfExt1	(Optional) Specifies to show the route preference of OSPF external type-1 route.
ospfExt2	(Optional) Specifies to show the route preference of OSPF external type-2 route.
ebgp	(Optional) Specifies to show the route preference of BGP AS-external route.
ibgp	(Optional) Specifies to show the route preference of BGP AS-internal route.

Default None

Command Mode Privileged mode

Usage Guideline In general, the higher the preference is, the lower the trust rating is. So, if there are two routes to a same destination, the source with lower preference will be selected to forward.
The preference for connected routes is fixed to 0. This means the connected route always has the highest priority.

Example To check the route preference of all route types:

```
Switch# show ip route-preference

Route Preference Settings

Protocol     Preference
----------   ----------
RIP          100
Static       60
Default      1
Connected    0
OSPF Intra   80
OSPF Inter   90
OSPF ExtT1   110
OSPF ExtT2   115
EBGP         70
IBGP         130
```

To check the route preference of OSPF route:

```
Switch# show ip route-preference ospf

Route Preference Settings

Protocol    Preference
----------  ----------
OSPF Intra  80
OSPF Inter  90
OSPF ExtT1  110
OSPF ExtT2  115
```

To check the route preference of RIP route:

```
Switch# show ip route-preference rip

Route Preference Settings

Protocol    Preference
----------  ----------
RIP         100
```

Field	Description
Protocol	The route type.
Preference	Route Preference.
OSPF Intra	OSPF intra-area route type.
OSPF Inter	OSPF inter-area route type.
OSPF ExtT1	OSPF AS external type-1 route.
OSPF ExtT2	OSPF AS external type-2 route.
Static	Static route.
Default	Static default route.
RIP	RIP route.
Connected	Connected route.
EBGP	BGP AS-external route.
IBGP	BGP AS-internal route.

To check the route preference of all route types of VRF VPN-A:

```
Switch# show ip route-preference vrf VPN-A

Route Preference Settings of VRF: VPN-A

Protocol    Preference
----------  ----------
RIP         100
Static      60
Default     1
Connected   0
OSPF Intra  80
OSPF Inter  90
OSPF ExtT1  110
OSPF ExtT2  115
EBGP        70
IBGP        130
```

9-8 show ip ecmp load-balance

Use this command to show the load-balancing algorithm settings.

show ip ecmp load-balance

Syntax Description None.

Default None.

Command Mode Privileged mode.

Usage Guideline Use this command to check the load-balancing algorithm settings.

Example Check the load-balancing algorithm settings:

```
Switch# show ip ecmp load-balance

ECMP Load Balance Algorithm :
  Destination IP : used.
  Source IP : not used.
  CRC_Low  : used.
  CRC_High : not used.
  TCP_UDP_Port : not used.
```

9-9 show ip route

Use the command to display the current state of the IP routing table.

show ip route [vrf *VRF-NAME***] [***NETWORK* **[***NET-MASK***]] [{count | connected | static | rip | ospf | bgp | weight}]**

Syntax Description	
vrf *VRF-NAME*	(Optional) Specifies to show routes of one VRF.
NETWORK	(Optional) Specifies the destination IP address of the route want to be displayed. If *NET-MASK* is not specified, the longest prefix matched route will be displayed.
NET-MASK	(Optional) Specifies the destination netmask of the route want to be displayed.
count	(Optional) Specifies to show the number of active route.
connected	(Optional) Specifies to show only connected routes.
static	(Optional) Specifies to show only static routes. One static route may be active or inactive.
rip	(Optional) Specifies to show only RIP routes.
ospf	(Optional) Specifies to show only OSPF routes.
bgp	(Optional) Specifies to show only BGP routes.
weight	(Optional) Specifies to show only multipath static routes.

Default None

Command Mode Privileged mode

Usage Guideline Use the command with keyword **count** means to show the number of active routes, active route is the route which had been written into chip and can forward traffic. User can specify the network as an IP address or a network address. They both are the same in this implementation. If *NET-MASK* is not specified, the longest prefix matched route will be displayed. If *NET-MASK* is specified, only the destination routes matched the specified network will be displayed

Example Check the IP routing table:

```
Switch# show ip route

Routing Table

IP Address/Netmask  Gateway          Interface     Cost      Protocol
------------------  ---------------  ------------  --------  --------
20.1.1.0/24         10.1.1.9         System        1         Static
30.1.1.0/24         10.1.1.9         System        1         Static
101.1.1.0/24        Null0            Null0         -         -
10.0.0.0/8          0.0.0.0          System        1         Connected

Total Entries : 4
```

Check all static routes:

```
Switch# show ip route static

Routing Table

IP Address/Netmask  Gateway    Cost   Protocol  Backup    Weight  Status
------------------  -------    ----   --------  ------    ------  ------
20.1.1.0/24         10.1.1.9   1      Static    Primary   None    Active
30.1.1.0/24         10.1.1.9   1      Static    None      2       Active
30.1.1.0/24         10.1.1.89  1      Static    None      2       Inactive
101.1.1.0/24        Null0      -      -         -         -       -
102.1.0.0/16        tunnel_1   1      Static    None      None    Inactive

Total Entries: 5
```

Check all static weighted multipath routes:

```
Switch# show ip route weight

Routing Table

IP Address/Netmask  Gateway          Cost   Protocol  Weight  Status
------------------  ---------------  -----  --------  ------  --------
30.1.1.0/24         10.1.1.9         1      Static    2       Active
30.1.1.0/24         10.1.1.89        1      Static    2       Inactive

Total Entries: 2
```

Check the VRF VPN-A's IP routing table:

```
Switch# show ip route vrf VPN-A

Routing Table  ( VRF: VPN-A )

IP Address/Netmask  Gateway          Interface     Cost      Protocol
------------------  ---------------  ------------  --------  --------
100.1.1.0/24        10.1.1.253       ip10          1         Static
10.0.0.0/8          0.0.0.0          ip10          1         Connected

Total Entries : 2

Switch#
```

Check the number of active routes:

```
Switch# show ip route count

--------- route info ----------
The num of active route: 3

Switch#
```

Field	Description
IP Address/Netmask	The network address of destination.
Gateway	The IP address of next router.
Interface	The name of the outgoing interface.
Cost	The metric of route.
Protocol	The route type.
Weight	The weight of static weighted multipath route.
Status	The status of static route. If be active, the static route is able to used to forward packet.

Multiprotocol Label Switching (MPLS) Commands

10-1 mpls ip (global configuration)

Use **mpls ip** command in global configuration mode to enable the MPLS forward globally. Use **no mpls ip** command in global configuration mode to disable MPLS forward globally.

mpls ip

no mpls ip

Syntax Description None.

Default Disabled.

Command Mode Global configuration mode.

Usage Guideline This command enables the MPLS function at the global level.

Example This example shows how to enable MPLS globally:

```
Switch(config)# mpls ip
```

10-2 snmp-server enable traps mpls

Use **snmp-server enable traps mpls** command to enable MPLS trap state. Use the **no** form of this command to disable MPLS trap state.

snmp-server enable traps mpls

no snmp-server enable traps mpls

Syntax Description None

Default Disabled

Command Mode Global configuration mode

Usage Guideline This command used to configure the MPLS LSP trap state. If the state is enabled, a trap is sent out when an LSP's operation status changes to up or down.

The user can verify their settings by entering the **show mpls** command.

Example This example shows how to enable MPLS trap state:

```
Switch(config)# snmp-server enable traps mpls
```

10-3 mpls ip (interface configuration)

Use **mpls ip** command in interface configuration mode to enable the MPLS forward on this interface. Use the **no mpls ip** command in interface configuration mode to disable the MPLS forward on this interface.

mpls ip

no mpls ip

Syntax Description None.

Default Disabled.

Command Mode Interface configuration mode.

Usage Guideline This command only can be applied on Layer 3 VLAN interface

Use the **mpls ip** command in the interface configuration mode to enable the MPLS forward on this interface.

For forwarding MPLS labeled packets through an interface, MPLS should be enabled globally and enabled on the interface.

Example This example shows how to enable MPLS on interface VLAN 100:

```
Switch(config)#interface vlan 100
Switch(config-if)#mpls ip
```

10-4 mpls static ftn

Use this command to add a static FTN entry. Use the **no mpls static ftn** command to remove the previous configured static FTN.

mpls static ftn NETWORK-PREFIX/PREFIX-LENGTH **out-label** *LABEL-VALUE* **nexthop** *IP-ADDRESS*

no mpls static ftn {*NETWORK-PREFIX/PREFIX-LENGTH* **| all }**

Syntax Description	
NETWORK-PREFIX/ PREFIX-LENGTH	Specifies the FEC of the static FTN
out-label *LABEL-VALUE*	Specifies the out-label of this FEC
nexthop *IP-ADDRESSS*	Specifies the next-hop IP address of this FEC

Default No static FTN.

Command Mode Global configuration mode.

Usage Guideline Use this command to add a static FTN entry.

At ingress LER (Label Edge Router), the incoming IP packets that are classified to the FEC (Forwarding Equivalence Class) will be pushed the MPLS label and forwarded to next hop according the FTN (FEC-to-NHLFE).

The follows figure shows the structure of a FTN that push label 100 for prefix FEC 172.18.10.0/24.

FEC		Next Hop Label Forwarding Entry (NHLFE)		
Type	Value	Next Hop	Label Operation	Out-label
IP prefix	172.18.10.0/24	110.1.1.2	push	100

The user can verify their settings by entering the **show mpls forwarding-table** command.

Example The follows example shows how to configure a static FTN that push label 100 for prefix FEC 172.18.10.0/24:

```
Switch(config)#mpls static ftn 172.18.10.0/24 out-label 100 nexthop
110.1.1.2
```

10-5 mpls static l2vc-ftn

Use the **mpls static l2vc-ftn** command to configure one static VC FTN item. Use the **no** form of this command to delete the configured FTN item.

mpls static l2vc-ftn *VC-ID IP-ADDRESS* **out-label** *LABEL-VALUE*

no mpls static l2vc-ftn *VC-ID IP-ADDRESS*

Syntax Description	
VC-ID	Specifies the PW (pseudo-wire) service instance ID. The range is 1-4294967295.
IP-ADDRESS	Specifies the peer LSR ID.
out-label *LABEL-VALUE*	Specifies the outgoing VC label.

Default No static VC FTN

Command Mode Global configuration mode

Usage Guideline This command is used to create one FTN for the VC instance.

Once the packets are received from the associated AC, the VC label will be pushed according the configured value. The tunnel label will be picked from the LSP that reaches the peer PE.

The user can verify their settings by entering the **show mpls forwarding-table** command.

Example To create one FTN for the VC instance:

```
Switch(config)# mpls static l2vc-ftn 2 10.1.1.1 out-label 100
```

10-6 mpls static ilm

Use this command to add a static ILM entry. Use **no mpls static ilm** command to remove the previous configured ILM.

For IP prefix FEC

mpls static ilm in-label *LABEL-VALUE* **forward-action { swap-label** *LABEL-VALUE* **| pop } nexthop** *IP-ADDRESS* **fec** *NETWORK-PREFIX/PREFIX-LENGTH*

For VC FEC

mpls static ilm in-label *LABEL-VALUE* **forward-action pop-l2vc-destport** *INTERFACE-ID* **fec** *VC-ID IP-ADDRESS*

no mpls static ilm { in-label *LABEL-VALUE* **| all }**

Syntax Description	
in-label *LABEL-VALUE*	Specifies the incoming label value of the ILM.
forward-action	Specify the forward behavior of this ILM entry. **swap-label:** swap the top label in the label stack and forward the MPLS packets to next-hop **pop:** pop the top label in the label stack and forward the MPLS packets to next-hop **pop-l2vc-destport:** pop all labels and forward the packets to outgoing interface
swap-label *LABEL-VALUE*	For the swap-label forward behavior, it specifies the swapped outgoing label value.
nexthop *IP-ADDRESS*	Specifies the next-hop IP address of this FEC.
fec *NETWORK-PREFIX/PREFIX-LENGTH*	Specifies the IP prefix FEC that is associated with the ILM.
pop-l2vc-destport *INTERFACE-ID*	Pop all labels and forward the packets to the specified outgoing interface. The interface can be an Ethernet port or a VLAN interface.
fec *VC-ID IP-ADDRESS*	Specifies the VC ID, peer LSR ID and IP address used. The range of VC ID is 1-4294967295.

Default No static ILM.

Command Mode Global configuration mode.

Usage Guideline Use this command to add a static ILM entry.

At LSR (Label Switching Router), the incoming MPLS packets that are matched the incoming label will be processed according configured ILM action. The label operation is either swapping the incoming top label to configured outgoing label or popping the top label. And then forward the packets to next-hop.

The following figure shows the structure of an ILM that swaps label from 100 to 200 for prefix FEC 172.18.10.0/24.

FEC	In-Label	Next Hop Label Forwarding Entry (NHLFE)		
		Next Hop	Label Operation	Out-label
172.18.10.0/24	100	120.1.1.3	swap	200

The user can verify their settings by entering the **show mpls forwarding-table** command.

Example

The following example shows how to configure a static ILM that swaps label from 100 to 200 for prefix FEC 172.18.10.0/24 at transit LSR:

```
Switch(config)# mpls static ilm in-label 100 forward-action swap-label 200
nexthop 120.1.1.3 fec 172.18.10.0/24
```

The following example shows how to configure a static ILM that pop label from 100 for prefix FEC 172.18.10.0/24 at egress LER:

```
Switch(config)# mpls static ilm in-label 100 forward-action pop nexthop
120.1.1.3 fec 172.18.10.0/24
```

The follows example shows how to configure a static ILM for VC 11 peer 210.1.1.1. The terminated packets will be forwarded to port 5.

```
Switch(config)# mpls static ilm in-label 200 forward-action pop-l2vc-
destport 5 vc 11 210.1.1.1
```

10-7 mpls label protocol ldp (global configuration)

Use the **mpls label protocol ldp** command in global configuration mode to enable LDP globally. Use **no mpls label protocol** in global configuration mode to disable LDP globally.

mpls label protocol ldp

no mpls label protocol

Syntax Description None.

Default Disabled.

Command Mode Global configuration mode.

Usage Guideline This command used to enable the LDP function globally and enter LDP configuration mode. LDP is running when MPLS is globally enabled too.

The user can verify their settings by entering the **show mpls ldp parameter** command.

Example This example shows how to enable LDP globally:

```
Switch(config)# mpls label protocol ldp
Switch(config-mpls-router)#
```

10-8 snmp-server enable traps ldp

Use the **snmp-server enable traps ldp** command to enable LDP trap state. Use the **no** form of this command to disable LDP trap state.

snmp-server enable traps ldp

no snmp-server enable traps ldp

Syntax Description None.

Default Disabled.

Command Mode Global configuration mode.

Usage Guideline This command used to configure the LDP trap state.

Example This example shows how to enable LDP trap state:

```
Switch(config)# snmp-server enable traps ldp
```

10-9 mpls label protocol ldp (interface configuration)

Use the **mpls label protocol ldp** command in interface configuration mode to enable LDP on this interface. Use **no mpls label protocol** command in interface configuration mode to disable LDP on this interface.

mpls label protocol ldp

no mpls label protocol

Syntax Description None.

Default Disabled.

Command Mode Interface configuration mode.

Usage Guideline This command only can be applied on a Layer 3 VLAN interface

Use the **mpls label protocol ldp** command in the interface configuration mode to enable LDP on this interface.

LDP is running on an interface only when:

1. MPLS and LDP are globally enabled.

2. MPLS and LDP are enabled on this interface.

The user can verify their settings by entering the **show mpls ldp interface** command.

Example This example shows how to enable LDP on interface VLAN 10:

```
Switch(config)# interface vlan 10
Switch(config-if)# mpls label protocol ldp
```

10-10 mpls ldp hello-holdtime

Use **mpls ldp hello-hellotime** command to configure the LDP link hello hold-time for the interface. Use the **no** form of this command to restore the default value.

mpls ldp hello-hellotime *SECONDS*

no mpls ldp hello-hellotime

Syntax Description	
SECONDS	Specifies the link hello hold-time in seconds. The range is 5-65535 seconds

Default 15 seconds.

Command Mode Interface configuration mode

Usage Guideline This command only can be applied on a Layer 3 VLAN interface

LDP sends link hello message periodically to discovery its directly connected neighbors. LDP maintains a hold timer for each discovered neighbor. If the timer expires without receipt of hello from the neighbor, LDP concludes that the neighbor has failed.

The user can verify their settings by entering the **show mpls ldp interface** command.

Example This example shows how to configure the hello hold time of VLAN 10 interface to 30 seconds:

```
Switch(config)# interface vlan 10
Switch(config-if)# mpls ldp hello-holdtime 30
```

10-11 mpls ldp hello-interval

Use the **mpls ldp hello- interval** command to configure the LDP link hello interval time for the interface. Use the **no** form of this command to restore the default value.

mpls ldp hello- interval *SECONDS*

no mpls ldp hello- interval

Syntax Description	
SECONDS	Specifies the link hello interval time in seconds. The range is 1-65535 seconds

Default 5 seconds.

Command Mode Interface configuration.

Usage Guideline This command only can be applied on a Layer 3 VLAN interface.

Use the **mpls ldp hello- interval** command to configure the LDP link hello interval time for the interface. LDP sends link hello message according the hello interval period.

The hello interval time on the interface shall less than its hello hold-time. It's recommend to set the hello interval less than one third of the hello hold-time.

The user can verify their settings by entering the **show mpls ldp interface** command.

Example This example shows how to configure the hello interval time of VLAN 10 interface to 10 seconds:

```
Switch(config)# interface vlan 10
Switch(config-if)# mpls ldp hello-interval 10
```

10-12 mpls ldp targeted-hello-accept

Use the **targeted-hello-accept** command to set the targeted hello message acceptable on this interface. Use the **no** form of this command to deny the targeted hello message acceptable.

mpls ldp targeted-hello-accept

no mpls ldp targeted-hello-accept

Syntax Description None.

Default Acceptable.

Command Mode Interface configuration mode.

Usage Guideline This command only can be applied on a Layer 3 VLAN interface.

If the targeted hello message is acceptable, the interface will responds to received targeted hello messages. Otherwise, if the received targeted hello is not coming from the local configured targeted peer, the targeted hello message will be ignored.

The user can verify their settings by entering the **show mpls ldp interface** command.

Example This example shows how to configure the VLAN 10 interface to accept the targeted hello message:

```
Switch(config)# interface vlan 10
Switch(config-if)# mpls ldp targeted-hello-accept
```

10-13 mpls ldp remote-peer

Use the **mpls ldp remote-peer** command to create a LDP targeted peer. Use the **no** form of this command to remove the previous configured LDP targeted peer.

mpls ldp remote-peer *IP-ADDRESS*

no mpls ldp remote-peer *IP-ADDRESS*

Syntax Description	
IP-ADDRESS	Specifies the LSR ID of the targeted peer.

Default No remote peer.

Command Mode Global configuration mode.

Usage Guideline This command is used to create a targeted peer and enter MPLS remote peer configuration mode. Targeted peer specifies a potential indirectly connected neighbor. The extended discovery will be used to discover the targeted peer.

The user can verify their settings by entering the **show mpls ldp remote-peer** command.

Example This example shows how to create a targeted peer 110.10.10.1:

```
Switch(config)# mpls ldp remote-peer 110.10.10.1
Switch(config-mpls-remote-peer)#
```

10-14 targeted-hello

Use the **targeted-hello** command to set the hold-time or interval for the extended peer hello message. Use the **no** form of this command to restore the default value.

targeted-hello { holdtime <seconds 15-65535> **| interval** <seconds 5-65535>**}**

no targeted-hello {holdtime | interval}

Syntax Description	
holdtime	The hold-time of the hello message for the extended mechanism.
interval	The interval of the hello message for the extended mechanism.
seconds	Specifies the time value.

Default By default, the hold-time of the hello message for the extended mechanism is 45 seconds, and the interval of the hello message is 15 seconds, which is one third of the hold-time.

Command Mode MPLS targeted peer configuration mode.

Usage Guideline It is necessary to ensure the hold-time of the target hello is larger than the interval value. Otherwise, LDP cannot work normally according to the requirement.

The user can verify their settings by entering the **show mpls ldp remote-peer** command.

Example This example shows how to configure the LDP extended discovery hello hold time to 90 seconds for targeted peer 110.10.10.1:

```
Switch(config)# mpls ldp remote-peer 110.10.10.1
Switch(config-mpls-remote-peer)# target-hello holdtime 90
```

10-15 ldp router-id

Use the **ldp router-id** command to set the LSR ID of the LDP. Use the **no ldp router-id** command to restore the LSR ID to default value.

ldp router-id *IP-ADDRESS*

no ldp router-id

Syntax Description	
IP-ADDRESS	Specifies the IPv4 address that will be used as LSR ID. The IPv4 address must be an IP address of an existed interface

Default

The LSR ID will be selected according to the following rules:

(1) If a loopback interface is configured, the LSR ID is set to the IP address of the loopback interface. If multiple loopback interfaces are configured, the loopback with the highest IP address will be used.

(2) If no loopback interface is configured, the LSR ID is set to the highest IP address of the link-up interfaces.

(3) If no interface is link-up, the LSR ID is set to the highest IP address of the interfaces.

Note: If LDP is running, LSR ID will not be auto-changed.

Command Mode

MPLS router configuration mode

Usage Guideline

The LSR ID is used to identify the LSR in the MPLS network. Recommend set the LSR ID to the IP address of a loopback interface.

The value of LSR ID should be global unique. By default, the LSR ID is used as transport-address. It is necessary to ensure the LSR ID is route reachable for other LSRs.

Note: If LDP is running, configuring LSR ID will lead to LDP restart.

The user can verify their settings by entering the **show mpls ldp parameter** command.

Example

This example shows how to configure LDP LSR ID to 110.10.10.30:

```
Switch(config-mpls-router)# ldp router-id 110.10.10.30
```

10-16 transport-address

Use this command to set the global transport address. Use the **no** form of this command to restore the default value.

transport-address {interface | *IP-ADDRESS* **}**

no transport-address

Syntax Description	
interface	Use the IP address of the corresponding interface as the transmission address for the session on each interface.
IP-ADDRESS	All sessions use this specified IP address as the transmission address uniformly.

Default Use the LSR ID as the transport-address.

Command Mode MPLS router configuration mode.

Usage Guideline This command is used to configure the LDP transport address. The transport address is used to establish LDP TCP connection. By default, the LSR ID is used as the transport address by all interfaces.

If you configure the transport address to “interface”, the IP address of each interface is used as the transport address.

If you configure the transport address to a specified IP address, this address is used as transport address by all interfaces.

Note 1: If LDP is running, configuring transport address will lead to LDP sessions restart.

Note 2: If LDP is running, link-down or deleting the interface which IP address is used as transport address will lead to the LDP session down, so suggestion using loopback interface as transport address.

The user can verify their settings by entering the **show mpls ldp parameter** command.

Example This example shows how to configure the transport address to 192.168.0.1:

```
Switch(config-mpls-router)# transport-address 192.168.0.1
```

10-17 backoff maximum

Use the **backoff maximum** command to configure the maximum back-off delay time. Use **no** form of this command to restore the default value.

backoff maximum *SECONDS*

no backoff maximum

Syntax Description	
SECONDS	The maximum back-off delay time. The range is 120-65535 seconds

Default 600 seconds.

Command Mode MPLS router configuration mode.

Usage Guideline The LDP back-off mechanism prevents two incompatibly configured LSRs from engaging in an endless sequence of session setup failures. If a session setup attempt fails due to an incompatibility, the active LSR delays its next attempt (that is, backs off), and then retries the session establishment.

The delay begins at 15 seconds, and it is increased exponentially with each successive failure until the maximum back-off delay is reached. The maximum [back off] delay is configurable, with the minimum amount being 120 seconds. The default value is 600 seconds.

If a session cannot be established and the trap/log state is enabled, LDP will send a trap/log to SNMP server to notify the session establishment failure.

The user can verify their settings by entering the **show mpls ldp parameter** command.

Example This example shows how to configure the maximum back-off delay time to 1000 seconds:

```
Switch(config-mpls-router)# backoff maximum 1000
```

10-18 keepalive-holdtime

Use the **keepalive-holdtime** command to configure the keep-alive hold-time for LDP sessions. Use the **no** form of this command to restore the default value.

keepalive-holdtime *SECONDS*

no keepalive-holdtime

Syntax Description	
SECONDS	Specifies the keep-alive hold-time in seconds. The range is 15-65535 seconds.

Default 40 seconds.

Command Mode MPLS router configuration mode.

Usage Guideline This command is used to configure the LDP session keep-alive hold-time.

LDP maintains a keep-alive hold timer for each peer session. If the keep-alive hold timer expires without receipt of an LDP PDU from the peer, LDP concludes that the peer has failed and terminates the LDP session.

Each LSR sends keep-alive messages at regular intervals to its LDP peers to keep the sessions active. The keep-alive interval is one third of the keep-alive hold-time.

Note: If LDP is running, configuring keep-alive hold-time will lead to LDP sessions restart.

The user can verify their settings by entering the **show mpls ldp parameter** command.

Example This example shows how to configure the keep-alive hold-time to 60 seconds:

```
Switch(config-mpls-router)# keepalive-holdtime 60
```

10-19 label-retention-mode

Use this command to set the label retention mode. Use the **no** form of this command to restore the default value.

label-retention-mode {liberal | conservative}

no label-retention-mode

Syntax Description	
liberal	Use the liberal label retention mode.
conservative	Use the conservative label retention mode.

Default Liberal label retention mode.

Command Mode MPLS router configuration mode.

Usage Guideline This command is used configure LDP label retention mode.

If the label distribution method is Downstream-Unsolicited and the label retention mode is conservative, once the LSR received label bindings from LSRs which are not its next hop for that FEC, it discards such bindings.

If the label retention mode is liberal, it maintains such bindings. It helps to speed up the setup of LSP in case there is a change in the next hop.

Note: If LDP is running, configuring label retention mode will lead to LDP sessions restart.

The user can verify their settings by entering the **show mpls ldp parameter** command.

Example This example shows how to configure the label retention mode to conservative:

```
Switch(config-mpls-router)#label-retention-mode conservative
```

10-20 lsp-control-mode

Use this command to set the LDP control mode. Use the **no** form of this command to restore the default value.

mpls ldp lsp-control-mode {independent | ordered}

no mpls ldp lsp-control-mode

Syntax Description	
independent	Use the independent control mode
ordered	Use the ordered control mode

Default Independent control mode.

Command Mode MPLS router configuration mode.

Usage Guideline This command is used to configure the LSP control mode.

In Independent LSP Control, each LSR independently binds a label to a FEC and distributes the binding to its label distribution peers.

In Ordered LSP Control, an LSR only binds a label to a FEC if it is the egress LSR for that FEC, or if it has already received a label binding for that FEC from its next hop for that FEC.

Note: If LDP is running, configuring the control mode will lead to LDP sessions restart.

The user can verify their settings by entering the **show mpls ldp parameter** command.

Example This example shows how to configure the LSP control mode to ordered:

```
Switch(config-mpls-router)#mpls ldp lsp-control-mode ordered
```

10-21 mpls ldp distribution-mode

Use this command to set the label distribution mode for the interface. Use the **no** form of this command to restore the default value.

mpls ldp distribution-mode {dod | du}

no mpls ldp distribution-mode

Syntax Description	
dod	Use the downstream on-demand distribution mode
du	Use the downstream unsolicited mode

Default Downstream unsolicited distribution mode

Command Mode Interface configuration mode

Usage Guideline This command only can be applied on a Layer 3 VLAN interface

This command is used to configure the label distribution method. If the label distribution method is Downstream-on-Demand, the downstream LSR advertises a label mapping when an upstream connection makes an explicit request.

If the method is Downstream-Unsolicited, it allows a LSR distributes label bindings to LSRs that have not explicitly requested them.

Note: If LDP is running, configuring label distribution method will lead to LDP sessions restart.

The user can verify their settings by entering the **show mpls ldp interface** command.

Example This example shows how to configure the label distribution mode to Downstream Unsolicited for VLAN 10 interface:

```
Switch(config)#interface vlan 10
Switch(config-if)# mpls ldp distribution-mode du
```

10-22 loop-detection

Use this command to enable loop detection. Use the **no** form of this command to disable loop detection.

loop-detection

no loop-detection

Syntax Description None.

Default Disabled.

Command Mode MPLS router configuration mode.

Usage Guideline This command is used to configure LDP loop detection.

The LDP loop detection mechanism makes use of the Path Vector and Hop Count TLVs carried by the label request and label mapping messages to detect looping LSPs.

Note: If LDP is running, configuring loop detection will lead to LDP sessions restart.

The user can verify their settings by entering the **show mpls ldp parameter** command.

Example This example shows how to enable LDP loop detection:

```
Switch(config-mpls-router)#loop-detection
```

10-23 max-hop-count

Use this command to configure the maximum hop count allowed for loop detection. Use the **no** form of this command to restore the default value.

max-hop-count *VALUE*

no max-hop-count

Syntax Description	
VALUE	Maximum hop count allowed for loop detection. The range is 1-255.

Default The default value is 254.

Command Mode MPLS router configuration mode.

Usage Guideline The hop count value is valid with the loop detection configured. If the hop count value in the label mapping message or the label request message of LDP is greater than the configured value, it is deemed that a loop occurs.

The user can verify their settings by entering the **show mpls ldp parameter** command.

Example This example shows how to configure the maximum hop count to 30:

```
Switch(config-mpls-router)#max-hop-count 30
```

10-24 max-path-vector

Use this command to configure the maximum path vector value allowed for loop detection. Use the **no** form of this command to restore the default value.

mpls ldp max-path-vector *VALUE*

no mpls ldp max-path-vector

Syntax Description	
VALUE	Maximum path vector value. The range is 1-255.

Default The default value is 254.

Command Mode MPLS router configuration mode.

Usage Guideline The path vector value is valid with the loop detection of the LDP instance enabled. If the LDR ID number that is in the path vector list of the label mapping message or the label request message of LDP is greater than the configured value, it is deemed that a loop occurs.

The user can verify their settings by entering the **show mpls ldp parameter** command.

Example This example shows how to configure the maximum path vector to 30:

```
Switch(config-mpls-router)# max-path-vector 30
```

10-25 explicit-null

Use this command to advertise an Explicit Null label in situations where it would normally advertise an Implicit Null label. Use the **no** form of this command to restore the default value.

explicit-null

no explicit-null

Syntax Description None.

Default Egress LSR advertise Implicit NULL label.

Command Mode MPLS router configuration mode.

Usage Guideline This command is used to configure LDP Penultimate Hop Popping (PHP) behavior. If the LSR is egress and the advertise label is Implicit Null label, the upstream will do Penultimate Hop Popping.

If the label distributed to Penultimate Hop is Explicit NULL label, the Penultimate Hop will don't pop it.

The user can verify their settings by entering the **show mpls ldp parameter** command.

Example This example shows how to configure the egress LSR advertise Explicit NULL label:

```
Switch(config-mpls-router)#explicit-null
```

10-26 md5 authentication

Use this command to enable the LDP authentication. Use the **no** form of this command to restore the default value.

md5 authentication

no md5 authentication

Syntax Description None.

Default By default, a peer has no password.

Command Mode MPLS router configuration mode.

Usage Guideline Use **md5 authentication** to enable LDP authentication. If the LDP MD5 authentication is enabled, the LSR applies the MD5 algorithm to compute the MD5 digest for the TCP segment that will be sent to the peer. This computation makes use of the peer password as well as the TCP segment. When the LSR receives a TCP segment with an MD5 digest, it validates the segment by calculating the MD5 digest (using its own record of the password) and compares the computed digest with the received digest. If the comparison fails, the segment is dropped without any response to the sender. The LSR ignores LDP Hellos from any LSR for which a password has not been configured.

Note: configuring the md5 authentication will lead to LDP restart.

The user can verify their settings by entering the **show mpls ldp parameter** command.

Example This example shows how to enable LDP MD5 authentication:

```
Switch(config-mpls-router)#md5 authentication
```

10-27 neighbor password

Use this command to configure a LDP peer password. Use the **no** form of this command to restore the default value.

neighbor *IP-ADDRESS* **password** *PASSWORD*

no neighbor *IP-ADDRESS* **password**

Syntax Description	
IP-ADDRESS	Specifies the peer IP address. The IP address shall be the peer's LSR ID.
password *PASSWORD*	Specifies the password. The maximum length of the password is 32 characters.

Default By default, a peer has no password.

Command Mode MPLS router configuration mode.

Usage Guideline Use this command to configure a LDP peer password. If the LDP MD5 authentication is enabled, the switch only establish session with these peers whose password is configured at both local and remote. The password configured on local must be same as remote peer.

Note: If the session of the peer is established, configuring the peer password will lead to the session restart.

The user can verify their settings by entering the **show mpls ldp neighbor password** command.

Example This example shows how to enable MD5 authentication and configure the peer 10.90.90.12 password to "abcd":

```
Switch(config-mpls-router)#md5 authentication
Switch(config-mpls-router)#neighbor 10.90.90.12 password abcd
```

10-28 show mpls

Use this command to show MPLS global configuration.

show mpls

Syntax Description None.

Default N/A.

Command Mode EXEC mode.

Usage Guideline This command is used to show MPLS global configuration.

Example To show the MPLS global configuration:

```
Switch# show mpls
MPLS Status: Enabled
Trap Status: Disabled
```

10-29 show mpls interface

Use this command to show MPLS enabled interfaces.

show mpls interface [*INTERFACE-ID***]**

Syntax Description	
INTERFACE-ID	(Optional) Specifies the interface that will display. If nothing is specified the command will display information for all interfaces.

Default N/A.

Command Mode EXEC mode.

Usage Guideline This command is used to show MPLS enabled interfaces.

Example To show MPLS enabeld interfaces:

```
Switch# show mpls interface
Interface  IP Address      Status
---------  -------------   -------
VLAN 10    10.90.90.1/24   Up
VLAN 20    172.18.1.1/24   Down

Total Entries: 2
```

10-30 show mpls forwarding-table

Use this command to show the MPLS label forwarding path information.

show mpls forwarding-table [*NETWORK-PREFIX/PREFIX-LENGTH* **] [{ftn | ilm}] [detail]**

Syntax Description	
NETWORK-PREFIX/ PREFIX-LENGTH	(Optional) specifies FEC. If no specified, show all FECs.
ftn	Specifies to only show FTN entries.
ilm	Specifies to only show ILM entries.
detail	Show detailed information of the MPLS label forwarding path information.

Default N/A

Command Mode EXEC mode

Usage Guideline This command shows the MPLS forwarding path information, including the FTN and ILM entries.

Example This example shows all MPLS label forwarding path information:

```
Switch# show mpls forwarding-table
LSP   FEC             In Label  Out Label   Out Interface   Next Hop
----  --------------  --------  ---------   -------------   ---------------
1     201.1.1.0/24    20        30          VLAN 10         172.18.1.1
2     201.2.1.0/24    60        40          VLAN 20         192.1.1.2
3     172.1.1.1/32    50        -           VLAN 10         172.18.1.1
4     192.1.1.0/24    -         70          VLAN 10         172.18.1.1
5     VC11/192.1.1.1  -         100/70      VLAN 10         172.18.1.1
6     VC11/192.1.1.1  200       -           -               -

Total Entries: 6
```

In the above example, LSP 5 is the outbound LSP of the VC FEC whose VC ID is 11 and peer is 192.1.1.1.

It pushes VC label 70 and tunnel label 100. The inbound LSP of the VC FEC is LSP 6. It pops incoming VC label 200 and forwards the terminated packets to Ethernet port 5.

This example shows all detail MPLS label forwarding path information:

:

```
Switch# show mpls forwarding-table detail
LSP: 1
Type: Transit           Status: Up
FEC: 201.1.1.0/24       Owner: Static
In Label:20             Out Label: swap 30
Next Hop: 172.18.1.1    Out Interface: VLAN 10

LSP: 2
Type: Transit           Status: Up
FEC: 201.2.1.0/24       Owner: LDP
In Label: 60            Out Label: swap 40
Next Hop: 192.1.1.2     Out Interface: VLAN 20

LSP: 3
Type: Egress            Status: Up
FEC: 172.1.1.1/32       Owner: LDP
In Label: 50            Out Label: pop
Next Hop: 172.18.1.1    Out Interface: VLAN 10

LSP: 4
Type: Ingress           Status: Up
FEC: 192.1.1.0/24       Owner: LDP
In Label: -             Out Label: push 70
Next Hop: 172.18.1.1    Out Interface: VLAN 10

LSP: 5
Type: Ingress           Status: Up
FEC: VC11/192.1.1.1     Owner: LDP
In Label: -             Out Label: push 100/70
Next Hop: 172.18.1.1    Out Interface: VLAN 10

LSP: 6
Type: Egress            Status: Up
FEC: VC11/192.1.1.1     Owner: LDP
In Label: 200           Out Label: pop

Total Entries: 6
```

This example shows FTN information:

```
Switch#show mpls forwarding-table ftn

FEC              Out Label   Next Hop    Out Interface
---------------  ----------  ----------  -------------
201.10.10.0/24   500         172.10.1.1  VLAN 10
202.1.1.0/24     600         172.10.1.1  VLAN 10
VC11/192.1.1.1   100/70      172.18.1.1  VLAN 10

Total Entries: 3
```

This example shows ILM information:

```
Switch#show mpls forwarding-table ilm

FEC                 In Label    Out Label   Out Interface  Next Hop
------------------  ----------  ----------  -------------  -------------
201.1.1.0/24        20          30          VLAN 10        172.18.1.1
172.1.1.1/32        50          -           VLAN 10        172.18.1.1
VC11/192.1.1.1      200         -           -              -

Total Entries: 3
```

10-31 show mpls ldp parameter

Use this command to show the LDP global information.

show mpls ldp parameter

Syntax Description None.

Default N/A.

Command Mode EXEC mode.

Usage Guideline This command is used to show LDP global information. It includes:

LSR ID

LDP version: At present, it is always 1.0.

LDP State: The global LDP state.

TCP port: The TCP port is used to establish the LDP session. It is not configurable in this system and is always the well-known LDP TCP port 646.

UDP port: The UDP port is used to discover the LDP neighbor. It is not configurable in this system and is always the well-known LDP UDP port 646.

Max PDU length: The max PDU length in this system is always 1500 bytes.

Max Backoff: The maximum backoff time.

Transport Address: Transport address for establishing LDP session.

Keep Alive Time: The keep-alive time of LDP session.

LSP Control Mode: Independent or Ordered mode.

Lable Retention: Conservative or liberal label retention mode.

Loop Detection: loop detection is enabled or disabled.

Path Vector Limit: The maximum LSRs that are contained in the Path Vector TLV of LDP label request or label mapping message.

Hop Count Limit: The maximum hop count for propagating LDP label request or label mapping message.

Authentication: The MD5 authorization state.

PHP: Penultimate Hop Popping behavior.

Trap Status: Trap state.

Example To show LDP global information:

```
Switch# show mpls ldp parameter
LSR ID                  : 172.18.1.1:0
LDP Version             : 1.0
LDP State               : Enabled
TCP Port                : 646
UDP Port                : 646
Max PDU Length          : 1500
Max Backoff             : 600 Seconds
Transport Address       : 172.18.1.1
Keep Alive Time         : 40 Seconds
LSP Control Mode        : Independent
Label Retention         : Liberal
Loop Detection          : Enabled
Path Vector Limit       : 255
Hop Count Limit         : 255
Authentication          : Enabled
PHP                     : Implicit null
Trap Status             : Enabled
```

10-32 show mpls ldp interface

Use this command to show the LDP interface information.

show mpls ldp interface [*INTERFACE-ID* **]**

Syntax Description	
INTERFACE-ID	(Optional) Specifies interface that will display. If no interface ID is specified the command will display information for all interfaces.

Default N/A.

Command Mode EXEC mode.

Usage Guideline This command is used to show LDP information on the interface.

Interface: IP interface name.

Admin State: The current LDP configure state of the interface.

Oper State: The current operational state of the interface.

Targeted Hello Accept: targeted hello message is acceptable or no.

Hello Interval: link hello interval.

Hello Hold Time: link hello hold-time.

Distribution Method: Downstream-Unsolicited (DU) or Downstream-on-Demand (DoD).

Example Show LDP information for all interfaces:

```
Switch# show mpls ldp interface
Interface: if1
---------------------------------------
Admin State           : Enabled
Oper State            : Disabled
Targeted Hello Accept : Acceptable
Hello Interval        : 5(Sec)
Hello Hold Time       : 15(Sec)
Distribution Method   : DoD

Interface: if2
---------------------------------------
Admin State           : Enabled
Oper State            : Disabled
Targeted Hello Accept : Acceptable
Hello Interval        : 5(Sec)
Hello Hold Time       : 15(Sec)
Distribution Method   : DoD

Total Entries: 2
```

10-33 show mpls ldp remote-peer

Use this command to show previous configured remote peer information.

show mpls ldp remote-peer [*IP-ADDRESS* **]**

Syntax Description	
IP-ADDRESS	(Optional) Specifies the remote peer that will display. If no IP Address is specified, the command will show all remote peers.

Default N/A.

Command Mode EXEC mode.

Usage Guideline This command is used to show previous configured LDP remote peer information.

Targeted Peer: Targeted peer LDP LSR ID.

Hello Interval: targeted hello interval.

Hold Time: targeted hello hold-time.

Example To show all remote peers:

```
Switch# show mpls ldp remote-peer
Remote Peer    Hello Interval   Hold Time
-------------  --------------   -----------
192.10.1.1     15(Sec)          45(Sec)
192.10.1.2     15(Sec)          45(Sec)

Total Entries: 2
```

10-34 show mpls ldp discovery

Use this command to show the LDP peer information.

show mpls ldp discovery

Syntax Description	
IP-ADDRESS	IP address which used as peer LSR ID. If no IP Address is specified, the command will display all neighbors.

Default N/A.

Command Mode EXEC mode.

Usage Guideline This command allows you to show the interfaces on which the LDP neighbor has been discovered.

Local LDP Identifier: The LDP identifier for the local router.

Interfaces: The interface information lists discovered by the active LDP.

xmit: The Hello messages sent on the interface.

recv: The Hello messages received on the interface.

Targeted Hellos: The sending path lists for all targeted hello messages.

active: The local LSR sends targeted Hello messages actively.

passive: The neighbor LSR sends targeted Hello messages actively and the local LSR responses.

Example To show all LDP neighbors:

```
Switch# show mpls ldp discovery
 Local LDP Identifier: 10.1.1.1:0
 Discovery Sources:
   Interfaces:
     VLAN 10 (ldp): xmit/recv
        LDP Id: 172.23.0.77:0
     VLAN 20 (ldp): xmit/recv
        LDP Id: 192.18.0.15:0
   Targeted Hellos:
     10.1.1.1 -> 10.133.0.33 (ldp): active, xmit/recv
        LDP Id: 10.133.0.33:0
     10.1.1.1 -> 172.18.30.2 (ldp): passive, xmit/recv
        LDP Id: 172.18.30.2:0

Total entries: 4
```

10-35 show mpls ldp neighbor

Use this command to show the LDP peer information.

show mpls ldp neighbor [*IP-ADDRESS***]**

Syntax Description	
IP-ADDRESS	IP address which used as peer LSR ID. If no IP Address is specified, the command will display all neighbors.

Default N/A.

Command Mode EXEC mode.

Usage Guideline This command is used to show all adjacencies discovered by LDP, includes:

Peer: Peer LDP LSR ID.

Transport Address: Peer's transport address.

Distribution Method: Downstream-Unsolicited (DU) or Downstream-on-Demand (DoD).

Keep Alive Time: The keep-alive time of the peer.

Loop Detect: The loop detection state of the peer.

Path Vector Limit: The path vector limit of the peer.

Max PDU Length: The maximum PDU length of the peer.

Example To show all LDP neighbors:

```
Switch#show mpls ldp neighbor
Peer : 202.11.1.1:0
 ---------------------------------------
 Protocol Version  : 1.0
 Transport address : 202.11.1.1
 Keep Alive Time   : 40 (sec)
 Distribute Method : DU
 Loop Detect       : Disabled
 Path vector limit : 0
 Max PDU Length    : 1500

 Peer : 192.1.1.1:0
 ---------------------------------------
 Protocol Version  : 1.0
 Transport address : 192.1.1.1
 Keep Alive Time   : 40 (sec)
 Distribute Method : DU
 Loop Detect       : Disabled
 Path vector limit : 1500
 Max PDU Length    : 0

 Peer : 202.20.1.1:0
 ---------------------------------------
 Protocol Version  : 1.0
 Transport address : 202.20.1.1
 Keep Alive Time   : 40 (sec)
 Distribute Method : DU
 Loop Detect       : Disabled
 Path vector limit : 0
 Max PDU Length    : 1500

Total Entries : 3
```

10-36 show mpls ldp session

Use this command to show LDP session information.

show mpls ldp session [peer *IP-ADDRESS*] **[{detail | statistic}]**

Syntax Description	
peer *IP-ADDRESS*	IP address which used as the peer LSR ID. If no specified, display all sessions.
detail	If specified this parameter, display detail information.
statistic	If specified this parameter, display session statistic.

Default None.

Command Mode EXEC mode.

Usage Guideline This command is used to show all LDP sessions. The information includes:

Peer: The peer LDP identifier of the session.

Status: The current state of the session. The state may be:

NONEXISTENT: Discovered neighbor but has not established the TCP connection.

INITIALIZED: Established the TCP connection, but has not sent initialization message.

OPENREC: As the passive role, it has received acceptable initialization message, and transmit initialization message and KeepAlive message.

OPENSENT: As the active role, has sent initialization message, but has not received keep-alive message.

OPERATIONAL: Received keep-alive message, session is established.

Role: Indicates if the local LSR for this session is active or passive.

Keep Alive: The negotiated keep-alive time. It is the smallest of the session peers.

Label Distribution: negotiated Label Distribution Method. Downstream-Unsolicited (DU) or Downstream-on-Demand (DoD).

If show detail, the following information will be displayed:

Loop Detect: The negotiated loop detection state.

Path Vector Limit: The negotiated path vector limitation.

Remain Time: The keep alive hold time remaining for this session.

Max PDU Length: The negotiated maximum PDU length.

Address List: Received IP addresses of peer.

If show statistic, the statistic for transmitted and received LDP message will be displayed.

Example To show all LDP session information:

```
Switch# show mpls ldp session
Peer        Status        Role      Keep Alive  Distribution Mode
----------  ------------  --------  ----------- ------------------
10.1.1.2:0  OPERATIONAL   Active    40(Sec)      DU
20.1.1.2:0  OPERATIONAL   Passive   40(Sec)      DU

Total Entries : 2
```

To show LDP session detail information for peer 10.1.1.2:

```
Switch# show mpls ldp session peer 10.1.1.2 detail

Peer               : 10.1.1.2:0
Status             : OPERATIONAL
Role               : Active
Keep Alive(Sec)    : 40
Remain Time(Sec)   : 20
Create Time        : 2009-12-1 14:10:30
Label Distribution : DU
Loop Detection     : Enabled
Path Vector Limit  : 255
Max PDU Length     : 1500
Address List       : 10.1.1.2
                     172.18.1.1

Total Entries: 1
```

To show LDP session statistics for peer 10.1.1.2:

```
Switch# show mpls ldp session peer 10.1.1.2 statistic

Peer 10.1.1.2
-----------------------------------------
Notification Message     : TX 10/RX 2
Initialization Message   : TX 2/RX 2
Keep Alive Message       : TX 100/RX 100
Address Message          : TX 1/RX 1
Address Withdraw Message : TX 0/RX 0
Label Mapping Message    : TX 2/RX 1
Label Request Message    : TX 2/RX 1
Label Withdraw Message   : TX 0/RX 0
Label Release Message    : TX 0/RX 0
Label Abort Message      : TX 0/RX 0

Total Entries: 1
```

10-37 show mpls ldp bindings

Use this command to show all LDP label binding information

show mpls ldp bindings

Syntax Description None.

Default None.

Command Mode EXEC mode.

Usage Guideline This command is used to show all LDP label bindings information.

Example To display all the LDP label bindings information:

```
Switch# show mpls ldp bindings

FEC: 130.1.1.0/24          State     : Established
   In label  : 70          Upstream  : 30.1.1.3
   Out label : 80          Downstream: 120.1.1.1

FEC: 172.18.1.0/24          State     : Established
   In label  : 20           Upstream  : 10.1.1.2
   Out label : 30           Downstream: 192.1.1.1

FEC: 172.18.2.0/24          State     : Established
   In label  : 50           Upstream  : 20.1.1.3
   Out label : 60           Downstream: 120.1.1.1

Total Entries : 2
```

In above example, the incoming label of FEC 172.18.1.0/24 is preserved for upstream LDP session restarting, and the outgoing label of FEC 172.18.2.0/24 is preserved for downstream LDP session restarting.

10-38 show mpls ldp statistic

Use this command to show the LDP global information.

show mpls ldp statistic

Syntax Description None.

Default N/A.

Command Mode EXEC mode.

Usage Guideline This command is used to show LDP statistic information.

Example To show LDP statistic information:

```
Switch# show mpls ldp statistic

SessionAttempts              :  0
SessionRejectedNoHelloErrors :  0
SessionRejectedAdErrors      :  0
SessionRejectedMaxPduErrors  :  0
SessionRejectedLRErrors      :  0
BadLdpIdentifierErrors       :  0
BadPduLengthErrors           :  0
BadMessageLengthErrors       :  0
BadTlvLengthErrors           :  0
MalformedTlvValueErrors      :  0
KeepAliveTimerExpErrors      :  0
ShutdownReceivedNotifications:  0
ShutdownSentNotifications    :  0
```

10-39 show mpls ldp neighbor password

Use this command to show the LDP neighbor password.

show mpls ldp neighbor password

Syntax Description None.

Default N/A.

Command Mode EXEC mode.

Usage Guideline Use this command to show all LDP neighbor password configuration.

Example To show LDP neighbors password configuration:

```
Switch#show mpls ldp neighbor password
Neighbor      Password
-----------   ----------
202.11.1.1    123456
192.1.1.1     abcd

Total Entries : 2
```

10-40 ping lsp

Use this command to check the connectivity of the LSP for specified FEC.

ping lsp *NETWORK-PREFIX/PREFIX-LENGTH* **[times** *VALUE* **| timeout** *SECONDS***]**

Syntax Description	
NETWORK-PREFIX/ PREFIX-LENGTH	Specifies the IPv4 prefix FEC which LSP connectivity will be checked.
times *VALUE*	Specifies the number of times to resend the same packet. The value range is 1-255 and the default value of times is 4.
timeout *SECONDS*	Specifies the timeout interval in seconds for an MPLS request packet. The value range is 1-99 seconds and the default value is 2 seconds.

Default N/A.

Command Mode EXEC mode.

Usage Guideline The **ping lsp** command is used to check the connectivity of the LSP for specified FEC. The FEC can be an IP prefix or a L2VPN Pseudowire.

If there is no LSP for the specified FEC, the “Destination unreachable” message will be displayed.

Otherwise, MPLS echo request messages will be sent out to along the LSP of the specified FEC. If the egress LSR received the request message, it will reply the request message sender with MPLS echo reply message.

If the sender cannot receive reply before timeout, the “Request time out” message will be displayed.

Example To check the connectivity of the LSP for network 192.1.1.0/24:

```
Switch# ping lsp 192.1.1.0/24

Ping 192.1.1.0/24

Reply from 192.1.1.1, time<10ms
Reply from 192.1.1.1, time<10ms
Reply from 192.1.1.1, time<10ms
Reply from 192.1.1.1, time<10ms

Ping Statistics for 192.1.1.0/24
Packets: Sent =4, Received =4, Lost =0
```

To check the connectivity of the LSP for network 110.1.1.0/24:

```
Switch# ping lsp 110.1.1.0/24

ping 110.1.1.0/24

Request time out
Request time out
Request time out
Request time out

Ping Statistics for 110.1.1.0/24
Packets: Sent =4, Received =0, Lost =4
```

10-41 traceroute lsp

Use this command for hop-by-hop fault localization as well as path tracing LSP of specified FEC.

traceroute lsp *NETWORK-PREFIX/PREFIX-LENGTH* [**timeout** *SECONDS*]

Syntax Description	
NETWORK-PREFIX/ PREFIX-LENGTH	Specifies the IPv4 prefix FEC which LSP connectivity will be checked.
timeout *SECONDS*	Specifies the timeout interval in seconds for an MPLS request packet. The value range is 1-99 seconds and the default value is 2 seconds.

Default N/A.

Command Mode EXEC mode.

Usage Guideline The **traceroute lsp** command is used for hop-by-hop fault localization as well as path tracing LSP of specified FEC. The FEC can be an IP prefix or a L2VPN Pseudowire.

If there is no LSP for the specified FEC, the “Destination unreachable” message will be displayed.

Otherwise, MPLS echo request messages will be sent out to along the LSP of the specified FEC. The TTL in the outmost label of the MPLS echo requests is set successively to 1, 2, 3, and so on. It force the echo request expired at each successive LSR along the LSP. The LSR returns an MPLS echo reply.

If the sender cannot receive reply before timeout, the traceroute will stop.

Example To trace route the LSP for network 192.1.1.0/24:

```
Switch# traceroute lsp 192.1.1.0/24

Tracing route to 192.1.1.0/24

1 Reply from 170.1.1, time<10ms
2 Reply from 200.1.2.3, time=20ms
3 Reply from 210.1.1.4, time=30ms
4 Reply from 192.1.1.1, time=40ms

Trace complete.
```

To trace route the LSP for network 110.1.1.0/24:

```
Switch# traceroute lsp 110.1.1.0/24

Tracing route to 110.1.1.0/24

1 Reply from 170.1.1, time<10ms
2 Request time out

Trace complete.
```

10-42 lsp trigger

Use this command to configure an LSP trigger filter rule. Use **no** form of this command to remove the rule.

lsp trigger *[SN]* **{permit | deny} {ip** *NETWORK-PREFIX/PREFIX-LENGTH* **| any}**

no lsp trigger [*SN* [- | ,]]

Syntax Description	
SN	(Optional) Specifies the sequence number of the LSP trigger filter rule. For creating new rule, if not specified, the SN begins from 10 and the increment is 10. For removing rule, if not specified, remove all rules. The SN range is 1-10000.
permit	Specifies permit LDP establishing LSP for the follows IP prefix FEC.
deny	Specifies not to permit LDP establishing LSP for the follows IP prefix FEC.
ip *NETWORK-PREFIX/PREFIX-LENGTH*	Specifies the IP prefix FEC on which the rule will apply.
any	Specifies the rule will apply on any IP prefix FEC.

Default No LSP trigger filter rule.

Command Mode MPLS router configuration mode.

Usage Guideline This command is used to configure an LSP trigger filter rules. The LSP trigger filter rules are IP access list rules that it is used to control the IP routes that can be used to trigger the establishment of an LSP. For example, if there are two routes for 172.18.1.0/24 and 172.18.2.0/24. If the LSP trigger filter permits 172.18.1.0/24 and denies 172.18.2.0/24, then the switch can only establish an LSP for 172.18.1.0/24.

Example To create LSP trigger filter rules that permit establish LSP for 192.1.1.0/24 and no permit establish LSP for other routes:

```
Switch(config)# mpls label protocol ldp
Switch(config-mpls-router)#lsp trigger 10 permit ip 192.1.1.0/24
Switch(config-mpls-router)#lsp trigger 20 deny any
Switch(config-mpls-router)#end
Switch#
```

To clear all LSP trigger filter rules:

```
Switch(config)# mpls label protocol ldp
Switch(config-mpls-router)#no lsp trigger
Switch(config-mpls-router)#end
Switch#
```

10-43 show lsp trigger

Use this command to show LSP trigger filter rule(s).

show lsp trigger *[SN]*

Syntax Description	
SN	(Optional) Specifies the sequence number of the LSP trigger filter rule to be shown. If no specified, all rules will be shown.

Default N/A.

Command Mode EXEC mode.

Usage Guideline Use this command to show LSP trigger filter rule(s).

Example To show all LSP trigger filter rules:

```
Switch#show lsp trigger
SN      Prefix FEC        Action
 -----   --------------    --------
10      192.1.1.0/24       Permit
20      Any                Deny

Total Entries : 2
```

Open Shortest Path First (OSPF) Commands

11-1 area

Use this command to create an OSPF area. To remove an area, use the **no** form of this command.

area *AREA-ID*

no area *AREA-ID*

Syntax Description	
AREA-ID	Specifies the ID of the area. The ID should be specified as an IP address.

Default The backbone area (0.0.0.0) is created by default.

Command Mode Router configuration mode

Usage Guideline The area created by this command is a normal area. Users can not create an existed area.
Use the **no** form of this command to remove a specified OSPF area and its configuration, including the removal of the area-based configuration commands, such as **area default-cost**, **area nssa**. Users can not remove the backbone area. There is a limitation about number of OSPF areas and it depends on project.
Users can verify the settings by entering the **show ip ospf** or **show ip ospf area** command.

Example To create an OSPF area with area ID 0.0.0.1:

```
Switch# configure terminal
Switch(config)# router ospf
Switch(config-router)# area 0.0.0.1
```

To remove the area 0.0.0.1:

```
Switch# configure terminal
Switch(config)# router ospf
Switch(config-router)# no area 0.0.0.1
```

11-2 area default-cost

To specify the cost associated with the default summary route that will be automatically injected to the stub area and no-so-stubby area (NSSA). Use the **no** command to restore to the default setting.

area *AREA-ID* **default-cost** *COST*

no area *AREA-ID* **default-cost**

Syntax Description	
AREA-ID	Specifies the ID of the area. The ID should be specified as an IP address.
COST	Specifies the cost for the default summary route used for a stub or NSSA area. The range of value is 0~65535.

Default The default value is 1.

Command Mode Router configuration mode

Usage Guideline Use this command on the area border router (ABR) that is attached to stub area or NSSA area to specify the cost associated with the default summary route generated by the ABR into the area.
One area must be created before set its default cost.
This command can only take effect on the stub area or NSSA area.

Users can verify the settings by entering the **show ip ospf** or **show ip ospf area** command.

Example To assign a default cost of 20 to stub area 0.0.0.1:

```
Switch# configure terminal
Switch(config)# router ospf
Switch(config-router)# area 0.0.0.1 stub
Switch(config-router)# area 0.0.0.1 default-cost 20
```

11-3 area nssa

Use this command to assign an area as a NSSA area. Use the **no** command to remove the NSSA related settings associated with the area.

area *AREA-ID* **nssa [no-summary] [translate]**

no area *AREA-ID* **nssa [no-summary] [translate]**

Syntax Description	
AREA-ID	Specifies the ID for the NSSA area. The ID should be specified as an IP address.
no-summary	(Optional) Specifies to prohibit summary routes advertised into the NSSA area. This function only take effect when the router is an ABR.
translate	(Optional) Specifies if leak type 7 LSA into other areas.

Default

By default no NSSA area is defined.
By default **no-summary** is not specified.
By default **translate** is not specified.

Command Mode

Router configuration mode

Usage Guideline

The command **no area** *AREA-ID* **nssa** removes all NSSA related settings associated with the area and the area becomes a normal area. Otherwise, use **no** command with keyword **no-summary** or **translate**, the area remains as a NSSA area and the specified parameter is unset.
A NSSA allows external routes to be advertised to the area in type 7 LSA. These routes then could be leaked into other areas if translate option is used. Although, the external routes from other areas still do not enter the NSSA.
Use the **area nssa** command to simplify administration if you are connecting a central site using OSPF to a remote site that is using a different routing protocol. You can extend OSPF to cover the remote connection by defining the area between the central router and the remote router as a NSSA.
For ASBR NSSA re-distribute, external routes will only be redistributed to NSSA area when redistribution is configured for the associated OSPF process. The external routes from other area within the same AS will not be injected to the NSSA area.
If there are multiple default routes generated into the NSSA area, the following priority will be followed: intra-route > inter-route > external route.
Users can verify the settings by entering the **show ip ospf** or **show ip ospf area** command.

Example

To assign OSPF area 0.0.0.2 to be a NSSA area and leak type 7 LSA into other areas:

```
Switch# configure terminal
Switch(config)# router ospf
Switch(config-router)# area 0.0.0.2 nssa no-summary
Switch(config-router)# area 0.0.0.2 nssa translate
```

11-4 area range

Use this command to summarize OSPF routes at an area border router (ABR). Use the **no** command to remove the defined summarization of routes.

area *AREA-ID* **range** *IP-ADDRESS NET-MASK* **[{advertise | not-advertise}]**

no area *AREA-ID* **range** *IP-ADDRESS NET-MASK*

Syntax Description	
AREA-ID	Specifies the area from which the routes will be summarized. The ID should be specified as an IP address.
IP-ADDRESS	IP address. With *NET-MASK* to inform the network segment whose routes are to be aggregated.
NET-MASK	IP address mask.
advertise	(Optional) The area range will be advertised.
not-advertise	(Optional) The area range will not be advertised.

Default By default no area range is configured for one area.
By default **advertise** is specified.

Command Mode Router configuration mode.

Usage Guideline Users can use this command on the area border router to summarize the intra-area routes. This command can be used to specify the summarized route for area 0 or for non-zero area.
Multiple area range commands can be configured. Thus, OSPF can summarize addresses for multiple sets of address ranges.
Users can verify the settings by entering the **show ip ospf** command.

Example To set one area range 192.168.0.0/255.255.0.0 in area 0.0.0.1:

```
Switch# configure terminal
Switch(config)# router ospf
Switch(config-router)# area 0.0.0.1
Switch(config-router)# area 0.0.0.1 range 192.168.0.0 255.255.0.0
```

11-5 area stub

Use this command to assign an area as a stub area. Use the **no** command to remove the stub related settings associated with the area.

area *AREA-ID* **stub [no-summary]**

no area *AREA-ID* **stub [no-summary]**

Syntax Description	
AREA-ID	Specifies the ID for the stub area. The ID should be specified as an IP address.
no-summary	(Optional) Specifies to prohibit summary routes advertised into the stub area. This will make the stub area becomes a totally stub area.

Default

By default no stub area is configured.
By default **no-summary** is not specified.

Command Mode

Router configuration mode

Usage Guideline

The command **no area** *AREA-ID* **stub** removes all stub related settings associated with the area and the area becomes a normal area. Otherwise, use **no** command with keyword **no-summary**, the area remains as a stub area and the specified parameter is unset.
Use the **no-summary** keyword to specify the area as a totally stubby area when the routers in the area do not requires to know the inter-area routes except type 3 default route.

Users can verify the settings by entering the **show ip ospf** or **show ip ospf area** command.

Example

To assign OSPF area 0.0.0.2 to be a stub area and prohibit summary routes advertised into this area:

```
Switch# configure terminal
Switch(config)# router ospf
Switch(config-router)# area 0.0.0.2 stub
Switch(config-router)# area 0.0.0.2 stub no-summary
```

11-6 area virtual-link

Use this command to configure a link for a non-backbone area that is physically separated from the backbone area. Use the **no** command to remove a virtual link.

area *AREA-ID* **virtual-link** *ROUTER-ID* **[authentication [message-digest | null]] [dead-interval** *SECONDS*] **[hello-interval** *SECONDS*] **[[authentication-key** *PASSWORD*] **| [message-digest-key** *KEY-ID* **md5** *KEY*]]

no area *AREA-ID* **virtual-link** *ROUTER-ID*

Syntax Description	
AREA-ID	Specifies the identifier of the area to establish the virtual link.
ROUTER-ID	Specifies the Router ID of the virtual link neighbor.
authentication	(Optional) Specifies authentication type. If the authentication type is not specified for the virtual-link, the simple password authentication type for the area will be used.
message-digest	(Optional) Specifies that MD5 authentication is used for the virtual link.
null	(Optional) No authentication is used.
hello-interval *SECONDS*	(Optional) Specifies the interval in seconds that the router sends the hello packet on the virtual link. The valid setting is 1-65535.
dead-interval *SECONDS*	(Optional) Specifies the interval in seconds that a neighbor is regarded as off-line if no hello packets are received within that time. The valid setting is 1-65535.
authentication-key *PASSWORD*	(Optional) Specifies up to 8 characters long password used for simple password authentication.
message-digest-key *KEY-ID* **md5** *KEY*	(Optional) Specifies up to 16 characters long digest key for MD5 authentication. The range of *KEY-ID* is 1-255.

Default

By default no virtual-link is configured.
Default authentication type is null.
Default hello-interval is 10 seconds.
Default dead-interval is 60 seconds.

Command Mode

Router configuration mode

Usage Guideline

In the OSPF routing domain, all areas must be connected with the backbone area. If an area disconnects from the backbone area, it requires establish a virtual link to connect the backbone area. Otherwise, the network communication will become abnormal.
The virtual link requires a connection between two ABR. The area that belongs to both ABR is called the transition area. A stub Area or NSSA area cannot act as a transition area.
The virtual link is a point to point link. The router will send the OSPF message to the neighbor router via unicast IP packet.
The simple text authentication type and MD5 authentication type are mutually exclusive.

The Dead interval must be larger than and multiple as Hello interval.

Users can verify the settings by entering the **show ip ospf** or **show ip ospf virtual-link** command.

Example

To configure a virtual link with neighbor 3.3.3.3 and set the authentication type to simple password with password “yourpass”:

```
Switch# configure terminal
Switch(config)# router ospf
Switch(config-router)# area 0.0.0.1
Switch(config-router)# area 0.0.0.1 virtual-link 3.3.3.3 dead-interval 10
hello-interval 5
Switch(config-router)# area 0.0.0.1 virtual-link 3.3.3.3 authentication
authentication-key yourpass
```

To set this virtual link’s authentication type to MD5:

```
Switch(config-router)# area 0.0.0.1 virtual-link 3.3.3.3 authentication
message-digest message-digest-key 1 md5 1234567812345678
```

11-7 clear ip ospf process

Use this command to restart the OSPF process.

clear ip ospf process [vrf *VRF-NAME***]**

Syntax Description	
vrf *VRF-NAME*	(Optional) Specifies to restart OSPF VRF instance.

Default None

Command Mode Global configuration mode

Usage Guideline Use this command to restart the OSPF protocol. If the OSPF is disabled before this command executed, nothing will be done.

Example To restart OSPF:

```
Switch# configure terminal
Switch(config)# clear ip ospf process
```

11-8 default-information originate

Use this command to generate a default external route (AS external LSA) into the OSPF routing domain. Use **no** command to disable the generation of AS external LSA default route.

default-information originate [always] [metric *METRIC-VALUE***]**

no default-information originate [always] [metric *METRIC-VALUE***]**

Syntax Description	
always	(Optional) Always generate the default route regardless of existence of a local default route.
metric *METRIC-VALUE*	(Optional) Specifies the cost associated with the generated default route. The value range is 1 to 65535.

Default

By default, this function is disabled.

The default value of metric is 1.

Command Mode

Router configuration mode

Usage Guideline

When the **default-information originate** command is used to import an AS external default route (network 0.0.0.0/0) into an OSPF routing domain, the router will automatically becomes an ASBR.
If **always** is specified, the default route is generated all the time. If **always** is not specified, the default route will only be generated when the default route exists locally.

Users can verify the settings by entering the **show ip ospf** command.

Example

To enable the default-information originate function and set the metric to 10:

```
Switch# configure terminal
Switch(config)# router ospf
Switch(config-router)# default-information originate metric 10
Switch(config-router)# default-information originate always
```

11-9 default-metric

Use this command to set default metric value of OSPF redistributed routes. Use the **no** command to restore to the default value.

default-metric *METRIC*

no default-metric

Syntax Description	
METRIC	Default metric value of OSPF redistributed routes. The value range is 1 to 16777214.

Default The default metric value of OSPF redistributed routes is 20.

Command Mode Router configuration mode

Usage Guideline The **default-metric** command is used in conjunction with the **redistribute** command to cause the OSPF to use the default metric value for the redistributed routes that have no metric specified.
Precedence of setting to determine the metric are: set metric in route map > metric in redistributed command > default-metric setting.

Users can verify the settings by entering the **show ip ospf** command.

Example To set the default metric value of OSPF redistributed routes to 10:

```
Switch# configure terminal
Switch(config)# router ospf
Switch(config-router)# default-metric 10
```

11-10 route-preference ospf

Use this command to set the management route preference of different types of OSPF routes. Use the **no** command to restore to the default value.

route-preference ospf {intra-area *VALUE* **| inter-area** *VALUE* **| external-1** *VALUE* **| external-2** *VALUE* **}**

no route-preference ospf

Syntax Description	
intra-area *VALUE*	(Optional) Specifies the route preference for all routes within an area. The value range is 1 to 999.
inter-area *VALUE*	(Optional) Specifies the route preference for all routes from one area to another area. The value range is 1 to 999.
external -1 *VALUE*	(Optional) Specifies the route preference for type-1 routes from other routing domains. The value range is 1 to 999.
external -2 *VALUE*	(Optional) Specifies the route preference for type-2 routes from other routing domains. The value range is 1 to 999.

Default The default value:

intra-area: 80.

inter-area: 90

external-1: 110

external-2: 115

Command Mode Router configuration mode.

Usage Guideline Use this command to set the route preference of different types of OSPF routes. A route preference is a rating of the trustworthiness of a routing information source, such as an individual router or a group of routers. In general, the higher the value, the lower the trust rating is.
Please note that changing route preference of routes may cause routing loop.

Users can verify the settings by entering the **show ip route-preference** command.

Example To change route preference of OSPF routes:

```
Switch# configure terminal
Switch(config)# router ospf
Switch(config-router)# route-preference ospf intra-area 50
```

11-11 distribute-list in

Use this command to configure LSA filtering. Use the **no** command to restore to the default value.

distribute-list *LIST-NAME* **in [***IPIF_NAME***]**

no distribute-list *LIST-NAME* **in [***IPIF_NAME***]**

Syntax Description	
LIST-NAME	Specifies to use one access list.
IPIF_NAME	(Optional) Specifies the name of the interface. If not specified, the configuration will apply to all interfaces.

Default By default no distribute list in is configured.

Command Mode Router configuration mode

Usage Guideline This configuration filters the received LSAs, and only those matching the filtering conditions are involved in the SPF calculation to generate the corresponding routes. It does not affect the link status database or the routing table of the neighbors. It only affects the routing entries calculated by the local OSPF.

Users can verify the settings by entering the **show ip ospf interface** command.

Example To set distribute list in on System interface:

```
Switch# configure terminal
Switch(config)# router ospf
Switch(config-router)# distribute-list 3 in System
```

11-12 ip ospf authentication

Use this command to configure the authentication type for an OSPF interface.
Use the **no** command to restore to default value.

ip ospf authentication [{message-digest | null}]

no ip ospf authentication

Syntax Description	
message-digest	(Optional) Specifies to use the MD5 authentication.
null	(Optional) No authentication is used.

Default By default no authentication is configured.

Command Mode Interface configuration mode

Usage Guideline The authentication type can be simple password authentication or MD5 authentication.
Use **no ip ospf authentication** or **ip ospf authentication null** command to remove the authentication.

Users can verify the settings by entering the **show ip ospf interface** command.

Example To set the System interface (vlan 1) authentication type to simple password:

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ip ospf authentication
Switch(config-if)# ip ospf authentication-key yourpass
```

To set the System interface (vlan 1) authentication type to MD5:

```
Switch(config)# interface vlan 1
Switch(config-if)# ip ospf authentication message-digest
Switch(config-if)# ip ospf message-digest-key 10 md5 yourpass
```

To remove the authentication on System interface (vlan 1):

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ip ospf authentication null
```

or:

```
Switch(config-if)# no ip ospf authentication
```

11-13 ip ospf authentication-key

Use this command to configure the plain text authentication key for an OSPF interface. Use the **no** command to delete the plain text authentication key.

ip ospf authentication-key *PASSWORD*

no ip ospf authentication-key

Syntax Description	
PASSWORD	Specifies up to 8 characters long for the plain text authentication key. The syntax is general string that does not allow space.

Default By default no key is configured.

Command Mode Interface configuration mode

Usage Guideline This command creates a password (key) that is inserted into the OSPF header when the router originates routing protocol packets. Assign a separate password to each network for different interfaces. Routers on the same network must use the same password to be able to exchange OSPF routing data.
Use the **ip ospf authentication** command to enable authentication. Configure the routers in the same routing domain with the same password.

Users can verify the settings by entering the **show ip ospf interface** command.

Example To set the System interface (vlan 1) authentication type to simple password:

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ip ospf authentication
Switch(config-if)# ip ospf authentication-key yourpass
```

11-14 ip ospf cost

Use this command to configure the cost of sending a packet on an OSPF interface. Use the **no** command to restore to the default value.

ip ospf cost *COST*

no ip ospf cost

Syntax Description	
COST	OSPF interface cost. The value range is 1 to 65535.

Default The default value is 1

Command Mode Interface configuration mode

Usage Guideline The interface cost reflects the overhead for sending the packet across the interface. This cost is advertised as the link cost in the router link advertisement. The cost is inversely proportional to the speed of an interface. The cost can be either manually assigned or be automatically determined.

Users can verify the settings by entering the **show ip ospf interface** command.

Example To set System interface's OSPF interface cost to 2:

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ip ospf cost 2
```

11-15 ip ospf dead-interval

Use this command to configure the interval during which at least one hello packet form a neighbor must be received before it is declared dead. Use the **no** command to restore it to the default value.

ip ospf dead-interval *SECONDS*

no ip ospf dead-interval

Syntax Description	
SECONDS	Specifies the interval in seconds. The value range is 1 to 65535.

Default The default interval is 40 seconds

Command Mode Interface configuration mode

Usage Guideline The dead-interval is the amount of time that the router waits to receive an OSPF hello packet from the neighbor before declaring the neighbor down.
This value is advertised in the router's hello packets. It must be the same for all routers on a specific network.
Please note that the dead-interval can not be less than the hello-interval and must be multiple times as hello-interval.

Users can verify the settings by entering the **show ip ospf interface** command.

Example To set the dead-interval of System interface (vlan 1) to 60 seconds:

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ip ospf dead-interval 60
```

11-16 ip ospf hello-interval

Use this command to configure the interval between hello packets. Use the **no** command to restore it to the default value.

ip ospf hello-interval *SECONDS*

no ip ospf hello-interval

Syntax Description	
SECONDS	Specifies the interval in seconds. The value range is 1 to 65535.

Default The default interval is 10 seconds

Command Mode Interface configuration mode

Usage Guideline The hello-interval is advertised in the hello packets.
Configure the same hello-interval for all routers on a specific network. A shorter hello interval ensures faster detection of topological changes but generates more routing traffic and might cause routing instability.
Please note that the dead-interval can not be less than the hello-interval and must be multiple times as hello-interval.

Users can verify the settings by entering the **show ip ospf interface** command.

Example To set the hello-interval of System interface (vlan 1) to 60 seconds:

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ip ospf hello-interval 60
```

11-17 ip ospf message-digest-key

Use this command to configure the MD5 digest key for OSPF interface. Use the **no** command to delete the MD5 key.

ip ospf message-digest-key *KEY-ID* **md5** *KEY*

no ip ospf message-digest-key

Syntax Description	
KEY-ID	Specifies a value for MD5 key identifier. The value range is 1 to 255.
KEY	Specifies up to 16 characters long for the OSPF MD5 message digest key. The syntax is general string that does not allow space.

Default By default no MD5 key is configured.

Command Mode Interface configuration mode

Usage Guideline The authentication for OSPF messages can be either operated in password mode or MD5 digest mode. This command defines the message digest key used by the MD5 digest mode.
In MD5 digest mode, the OSPF message sender will compute a message digest based on the message digest key for the TX message. The message digest and the key ID will be encoded in the packet. The receiver of the packet will verify the digest in the message against the digest computed based on the locally defined message digest key corresponding to the same key ID.
The same key ID on the neighboring router should be defined with the same key string.
All the neighboring routers on the same interface must use the same key to exchange the OSPF packet with each other. Normally, all neighboring routers on the interface use the same key

Users can verify the settings by entering the **show ip ospf interface** command.

Example To set the System interface (vlan 1) authentication type to MD5:

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ip ospf authentication message-digest
Switch(config-if)# ip ospf message-digest-key 10 md5 yourpass
```

11-18 ip ospf priority

Use this command to configure the router priority that is used to determine the designated router for the network. Use the **no** command to restore it to the default value.

ip ospf priority *PRIORITY*

no ip ospf priority

Syntax Description	
PRIORITY	Specifies the priority of the router on the interface. The value range is 0 to 255.

Default The default priority is 1.

Command Mode Interface configuration mode

Usage Guideline The OSPF router will determine a designated router for the multi-access network.This command sets the priority used to determine the OSPF Designated Router (DR) for a network. If two routers attempt to become the DR, the router with the higher router priority will be elected to the DR. If the routers have the same priority, the router with the higher router ID takes precedence.
Only routers with nonzero router priority values are eligible to become the designated or backup designated router.

Users can verify the settings by entering the **show ip ospf interface** command.

Example To set the priority of the System interface (vlan 1) to 50.

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ip ospf priority 50
```

11-19 network area

Use this command to enable OSPF routing with a specified Area ID on interfaces with IP addresses that match or belong to the specified network address. Use the **no** command to remove the configuration.

network *IPADDR NETMASK* **area** *AREA-ID*

no network *IPADDR NETMASK* **area** *AREA-ID*

Syntax Description	
IPADDR	Specifies IP address of the interface.
NETMASK	Specifies IP netmask of the interface.
AREA-ID	Specifies the identifier of the area to be associated with the OSPF address range.

Default

All interfaces belong to backbone area.
The OSPF is disabled on each interface.

Command Mode

Router configuration mode

Usage Guideline

OSPF routing can be enabled per IPv4 subnet basis. Each subnet can belong to one particular OSPF area.
Use **no** form of this command to remove the subnet from one particular OSPF area to backbone area and the administrative state of the interface becomes disabled.

Users can verify the settings by entering the **show ip ospf** or **show ip ospf interface** command.

Example

To enable OSPF interface (10.1.1.1/8) and set it to area 0.0.0.1:

```
Switch# configure terminal
Switch(config)# router ospf
Switch(config-router)# network 10.1.1.1 255.0.0.0 area 0.0.0.1
```

11-20 passive-interface

Use the command to configure the specified OSPF interface as passive interface. Use the **no** command to restore to the default value.

passive-interface {default | interface *IPIF_NAME***}**

no passive-interface {default | interface *IPIF_NAME***}**

Syntax Description	
default	Specifies all the interfaces as passive interfaces.
interface *IPIF_NAME*	Specifies the interface with this name as passive interface.

Default By default no interface is configured as passive interface

Command Mode Router configuration mode

Usage Guideline If an interface is passive, the OSPF protocol packets are neither sent nor received through the specified interface.

Users can verify the settings by entering the **show ip ospf interface** command.

Example To set all the interfaces to be passive:

```
Switch# configure terminal
Switch(config)# router ospf
Switch(config-router)# passive-interface default
```

To set System interface to be passive:

```
Switch# configure terminal
Switch(config)# router ospf
Switch(config-router)# passive-interface interface System
```

11-21 redistribute

Use to redistribute external routing information into the OSPF routing domain. Use the **no** command to disable redistribution.

redistribute {connected | static | rip | bgp} [metric *METRIC* **| metric-type {1 | 2} | route-map** *MAP-NAME***]**

no redistribute {connected | static | rip | bgp} [metric *METRIC* **| metric-type {1 | 2} | route-map** *MAP-NAME***]**

Syntax Description	
connected	Specifies to redistribute connected routes to OSPF
static	Specifies to redistribute static routes to OSPF
rip	Specifies to redistribute rip routes to OSPF
bgp	Specifies to redistribute bgp routes to OSPF
metric *METRIC*	(Optional) Specifies the metric for the redistributed routes. The value range is 0-16777214. If it is not specified or specified as 0, the redistributed routes will be associated with the metric as specified with the command **default-metric**.
metric-type {1 | 2}	(Optional) Allows the selection of one of two methods for calculating the metric value. 1 calculates the metric (for other routing protocols to OSPF) by adding the destination's interface cost to the metric entered in the Metric field. 2 uses the metric entered in the Metric field without change. If the metric type is not specified, it will be type 2.
route-map *MAP-NAME*	(Optional) Specifies a route map which will be used as the criteria to determine whether to redistribute specific routes. This *MAP-NAME* can be up to 16 characters long.

Default

By default route redistribution is disabled.
By default metric-type is 2
By default no route map is used.

Command Mode

Router configuration mode

Usage Guideline

External Routes can be redistributed to normal area as type 5 external routes, and redistributed to NSSA stub area as type 7 external routes by ASBR.
The external route type can be type 1 or type 2. If the redistributed external route is of type 1, the metric represents the internal metric. If the redistributed external route is of type 2, the metric represents the external metric. An internal metric will consider the cost of the route from itself to the redistributing router plus the advertised cost to reach the destination. An external metric only considers the advertised metric to reach the destination.
By default, connected and static route will not be re-distributed either.
Use the **redistribute** or the **default-information** router configuration commands make the router becomes an ASBR.

If a metric is not specified, metric will be the value set by the **default metric** command. If no value specified by **default-metric**, routes redistributed from other protocols will get 20 as the metric value with the following exception.

Note that if the redistricted route is a default route, then the metric is determined by the **default-information originate** command.

Users can verify the settings by entering the **show ip ospf** command.

Example

To enable redistribution of rip routes into the OSPF routing domain and set the metric to 5:

```
Switch# configure terminal
Switch(config)# router ospf
Switch(config-router)# redistribute rip metric 5 metric-type 1
```

11-22 router ospf

Use this command to enable OSPF and enter the router configuration mode. Use the **no** form of this command to disable OSPF.

router ospf [vrf *VRF-NAME***]**

no router ospf [vrf *VRF-NAME***]**

Syntax Description	
vrf *VRF-NAME*	(Optional) Specifies to create or delete the OSPF VRF instance.

Default By default OSPF is disabled.

Command Mode Global configuration mode.

Usage Guideline Use this command to enter router configuration mode to configure parameters needed by OSPF.

Users can verify the settings by entering the **show ip ospf** command.

Example To enter the router configuration mode and enable OSPF:

```
Switch# configure terminal
Switch(config)# router ospf
```

To disable OSPF:

```
Switch# configure terminal
Switch(config)# no router ospf
```

To create a new OSPF instance in VRF VPN-A and enter router configuration mode:

```
Switch# configure terminal
Switch(config)# router ospf vrf VPN-A
Switch(config-router)#
```

11-23 router-id

Use this command to configure the router ID. Use the **no** command to restore to the default value.

router-id *ROUTER-ID*

no router-id

Syntax Description	
ROUTER-ID	Specifies the router ID in IPv4 address format.

Default The router-id is automatically chosen based on the highest IP address present on the router. If a loopback interface is present, the loopback IP address will be used. If more than one loopback interface is present, the highest loopback IP will be used.

Command Mode Router configuration mode.

Usage Guideline Router ID is a 32-bit number assigned to each router running the OSPF protocol. This number uniquely identifies the router within an Autonomous System. You must configure each router with a unique router-id.

Users can verify the settings by entering the **show ip ospf** command.

Example To set the router-id to 1.1.1.1:

```
Switch# configure terminal
Switch(config)# router ospf
Switch(config-router)# router-id 1.1.1.1
```

To restore the router-id to auto select:

```
Switch# configure terminal
Switch(config)# router ospf
Switch(config-router)# no router-id
```

11-24 show ip ospf

Use this command to show general information about OSPF.

show ip ospf [vrf *VRF-NAME*]

Syntax Description	
vrf *VRF-NAME*	(Optional) Specifies to show brief information about the OSPF VRF instance.

Default None.

Command Mode Privileged mode

Usage Guideline Display general OSPF protocol information. It provides system-wise statistics and per area statistics for OSPF.

Example To check OSPF settings:

```
Switch# show ip ospf

OSPF Router ID : 1.1.1.1
State          : Enabled

Default Information Originate:
State  : Disabled
Always : On
Metric : 1

OSPF Interface Settings

Interface    IP Address         Area ID         State    Link      Metric
                                                         Status
------------ ------------------ --------------- -------- --------- --------
System       10.1.1.1/24        0.0.0.0         Enabled  Link Up   1
```

Field	Description
Interface	Name of the interface.
IP Address	IP address of the source IP address used to send out OSPF packet to neighbor.
Area ID	The area this interface belongs to. It is specified with the command **network area**.

Link Status	The lower layer link status of the interface.
Metric	OSPF interface cost. It is specified with the command **ip ospf cost**.

```
OSPF Area Settings

Area ID         Type   Stub Import Summary LSA Stub Default Cost Translate
--------------- ------ ----------------------- ---------------- ---------
0.0.0.0         Normal None                    None             None
0.0.0.1         Stub   Enabled                 1                None
```

Field	Description
Area ID	Identifier of area. ID 0.0.0.0 is backbone area.
Type	Type of area. It could be normal, stub or NSSA.
Stub Import Summary LSA	Whether to prohibit summary routes advertised into the area. It is only for stub or NSSA area. It is specified with the command **area stub** or **area nssa.**
Stub Default Cost	The cost for the default summary route used for a stub or NSSA area. It is specified with the command **area default-cost**.
Translate	Whether on NSSA area leak the type-7 LSA outside to other areas. It is only for NSSA area and specified with the command **area nssa**.

```
Virtual Interface Configuration

Transit         Virtual         Hello    Dead     Authentication Link
Area ID         Neighbor Router Interval Interval                Status
--------------- --------------- -------- -------- -------------- ------
4.4.4.4         1.1.1.1         10       60       MD5            Up
```

Field	Description
Transit Area ID	The non-backbone area the two endpoints of virtual link have in common.
Virtual Neighbor Router	Router ID of the other endpoint of the virtual link.
Hello Interval	The interval between hello packets. It is specified with the command **area virtual-link**.
Dead Interval	The interval during which at least one hello packet form a virtual neighbor must be received before it is declared dead. It is specified with the command **area virtual-link**.
Authentication	The authentication type used by the virtual link. It is specified with the command **area virtual-link**.

Link Status	When the other endpoint is reachable according to routing table, the virtual link is link up. Or it is link down.

```
OSPF Area Aggregation Settings

Area ID         Aggregated          LSDB     Advertise
                Network Address     Type
--------------- ------------------- -------- ---------
0.0.0.1         100.1.1.0/24        Summary  Enabled
```

Field	Description
Area ID	The area from which the routes will be summarized. It is specified with the command **area range**.
Aggregated Network Address	The network segment whose routes are to be aggregated. It is specified with the command **area range**.
LSDB Type	If the area is normal, it is used for summary LSA. If the area is NSSA, it is used for type-7 LSA.
Advertise	If the area range will be advertised. It is specified with the command **area range**.

```
OSPF Redistribution Settings

Source    Destination   Type      Metric       RouteMapName
Protocol  Protocol
--------  ------------  --------  ------------ ------------
STATIC    OSPF          ALL       10

Switch#
```

Field	Description
Source Protocol	The source route domain of redistribution. It is specified with the **redistribute** command.
Destination Protocols	The destination route domain of redistribution.
Type	The route type of source route domain of redistribution.
Metric	Metric of routes redistributed into RIP domain. It is specified with the **redistribute** command.
RouteMapName	Route map name used to filter routes redistributed into RIP domain. It is specified with the **redistribute** command.

To check OSPF settings in VRF VPN-A:

```
Switch# show ip ospf vrf VPN-A

OSPF On VRF : VPN-A
Router ID : 100.1.1.1 (Auto selected)
State     : Enabled

Default Information Originate:
State  : Disabled
Always : Off
Metric : 1

OSPF Interface Settings
Interface    IP Address         Area ID         State    Link      Metric
                                                         Status
------------ ------------------ --------------- -------- --------- -------
ip100        100.1.1.1/24       0.0.0.0         Disabled Link Up   1

OSPF Area Settings
Area ID         Type   Stub Import Summary LSA Stub Default Cost Translate
--------------- ------ ---------------------- ----------------- ---------
0.0.0.0        Normal None                    None              None


Virtual Interface Configuration
Transit         Virtual         Hello    Dead     Authentication Link
Area ID         Neighbor Router Interval Interval                Status
--------------- --------------- -------- -------- -------------- ------

OSPF Area Aggregation Settings
Area ID         Aggregated         LSDB     Advertise
                Network Address    Type
--------------- ------------------ -------- ---------

OSPF Redistribution Settings
Source    Destination   Type      Metric       RouteMapName
Protocol  Protocol
--------  ------------  --------  ------------ ------------
Switch#
```

11-25 show ip ospf area

Use this command to show general information about OSPF areas.

show ip ospf area [*AREA-ID***] [vrf** *VRF-NAME***]**

Syntax Description	
AREA-ID	(Optional) Show detail information about the specified area.
vrf *VRF-NAME*	(Optional) Specifies to show area information about the OSPF VRF instance.

Default None.

Command Mode Privileged mode

Usage Guideline This command is used to show OSPF areas information. When the area ID is specified, the detail information about this area will be displayed.

Example To check OSPF areas settings:

```
Switch# show ip ospf area

OSPF Area Settings

Area ID   Type   Stub Import Summary LSA Stub Default Cost Translate
--------- ------ ----------------------- ----------------- ---------
0.0.0.0   Normal None                    None              None
0.0.0.1   Stub   Enabled                 1                 None
0.0.0.2   NSSA   Enabled                 0                 Disabled

Switch#
```

Field	Description
Area ID	Identifier of area. ID 0.0.0.0 is backbone area.
Type	Type of area. It could be normal, stub or NSSA.
Stub Import Summary LSA	Whether to prohibit summary routes advertised into the area. It is only for stub or NSSA area. It is specified with the command **area stub** or **area nssa.**
Stub Default Cost	The cost for the default summary route used for a stub or NSSA area. It is specified with the command **area default-cost**.
Translate	Whether on NSSA area leak the type-7 LSA outside to other areas. It is only for NSSA area and specified with the command **area nssa**.

To check OSPF areas 0.0.0.0 detail information:

```
Switch# show ip ospf area 0.0.0.0

Area ID: 0.0.0.0                        Area Type: Normal

SPF algorithm runs for area 0.0.0.0: 0 time
Number of LSA in this area: 0           Checksum Sum: 0x0
Number of ABR in this area: 0           Number of ASBR in this area: 0

Switch#
```

Field	Description
Area ID	Identifier of area. ID 0.0.0.0 is backbone area.
Area Type	Type of area. It could be normal, stub or NSSA. It is specified with the command **area**, **area stub** and **area nssa**.
SPF algorithm runs for area	The times of SPF calculation in this area.
Number of LSA in this area	The count of LSAs in this area.
Checksum Sum	The value of checksum for all LSAs in this area.
Number of ABR in this area	The count of area border router in this area.
Number of ASBR in this area	The count of AS boundary router in this area.

To check OSPF areas settings in VRF VPN-A:

```
Switch#sh ip ospf area vrf VPN-A

OSPF Area Settings (VRF : VPN-A)

Area ID         Type   Stub Import Summary LSA Stub Default Cost Translate
--------------- ------ ---------------------- ----------------- ---------
0.0.0.0         Normal None                   None              None

Switch#
```

11-26 show ip ospf database

Use this command to display a database summary for OSPF information.

show ip ospf [vrf *VRF-NAME*] [*AREA-ID*] **database [{asbr-summary | external | network | router | summary | nssa-external | stub}] [{adv-device** *ROUTER-ID* **| self-originate}]**

Syntax Description	
vrf *VRF-NAME*	(Optional) Specifies to show LSA information about OSPF VRF instance.
AREA-ID	(Optional) Specifies the area ID.
asbr-summary	(Optional) Specifies to only show ASBR summary LSA information.
external	(Optional) Specifies to only show AS external LSA information.
network	(Optional) Specifies to only show Network LSA information.
router	(Optional) Specifies to only show Router LSA information.
summary	(Optional) Specifies to only show Summary LSA information.
nssa-external	(Optional) Specifies to only show NSSA type-7 LSA information.
stub	(Optional) Specifies to only show all LSA information in stub and NSSA area.
adv-device *ROUTER-ID*	(Optional) Specifies to display the LSA information generated by the specified advertising device.
self-originate	(Optional) Specifies to display the LSA information generated by the device itself.
N/A	Show brief information about all LSA information.

Default None

Command Mode Privileged mode

Usage Guideline In following cases, the detail information of LSAs will be displayed:
(1) LSA type is specified as **asbr-summary**, **external**, **network**, **router**, **summary**, **nssa-external** or **stub**;
(2) Area ID is specified;
(3) **self-originate** is specified;
(4) **adv-device** is specified**.**

Example To show brief information about all LSAs:

```
Switch# show ip ospf database

Area            LSDB      Advertising     Link State        Cost     Sequence
ID              Type      Router ID       ID                         Number
--------------- --------- --------------- ----------------- -------- ----------
0.0.0.0         RTRLink   1.1.1.1         1.1.1.1/0         *        0x8000000E
0.0.0.0         RTRLink   2.2.2.2         2.2.2.2/0         *        0x80000013
0.0.0.0         NETLink   2.2.2.2         10.1.1.2/24       *        0x8000000C
0.0.0.2         RTRLink   1.1.1.1         1.1.1.1/0         *        0x80000002
0.0.0.2         Summary   1.1.1.1         0.0.0.0/0         1        0x80000002
0.0.0.2         Summary   1.1.1.1         10.1.1.0/24       1        0x80000002
0.0.0.2         Summary   1.1.1.1         30.1.1.0/24       2        0x80000001
```

Field	Description
Area ID	The area this LSA belongs to.
LSDB Type	The LSA type.
Advertising Router ID	The ID of the router originates this LSA.
Link State ID	The link state ID of this LSA.
Cost	The cost used by route calculating.
Sequence Number	The sequence number of the LSA.

To show detail information of LSAs in area 0.0.0.0:

```
Switch# show ip ospf 0.0.0.0 database

Area ID: 0.0.0.0                    LS Type: Router Link
Link State ID: 1.1.1.1/0            Advertising Router: 1.1.1.1
Link State Age: 1462
Checksum: 0x68BA                    LS Sequence Number: 0x8000000E

Area ID: 0.0.0.0                    LS Type: Router Link
Link State ID: 2.2.2.2/0            Advertising Router: 2.2.2.2
Link State Age: 1468
Checksum: 0x531                     LS Sequence Number: 0x80000013

Area ID: 0.0.0.0                    LS Type: Network Link
Link State ID: 10.1.1.2/24          Advertising Router: 2.2.2.2
Link State Age: 1468
Checksum: 0xF735                    LS Sequence Number: 0x8000000C
```

Field	Description
Area ID	The area this LSA belongs to.
LS Type	The LSA type.
Link State ID	The link state ID of this LSA.
Advertising Router	The ID of the router originates this LSA.
Link State Age	The age of the LSA.
Checksum	The checksum of the LSA.
LS Sequence Number	The sequence number of the LSA.

To show detail information of all Router LSAs in area 0.0.0.0:

```
Switch# show ip ospf 0.0.0.0 database router

Area ID: 0.0.0.0                    LS Type: Router Link
Link State ID: 1.1.1.1/0            Advertising Router: 1.1.1.1
Link State Age: 120
Checksum: 0x66BB                    LS Sequence Number: 0x8000000F

Area ID: 0.0.0.0                    LS Type: Router Link
Link State ID: 2.2.2.2/0            Advertising Router: 2.2.2.2
Link State Age: 126
Checksum: 0x332                     LS Sequence Number: 0x80000014
```

To show detail information of all LSAs originated by self:

```
Switch# show ip ospf database self-originate

Area ID: 0.0.0.0                    LS Type: Router Link
Link State ID: 1.1.1.1/0            Advertising Router: 1.1.1.1
Link State Age: 175
Checksum: 0x66BB                    LS Sequence Number: 0x8000000F
```

11-27 show ip ospf interface

Use this command to display interface information for OSPF.

show ip ospf interface [*IPIF_NAME***] [vrf** *VRF-NAME***]**

Syntax Description	
IPIF_NAME	(Optional) Specifies the interface name to display the OSPF information.
vrf *VRF-NAME*	(Optional) Specifies to show interface information about OSPF VRF instance.

Default None.

Command Mode Privileged mode.

Usage Guideline Use this command to check OSPF interface settings.

Example To show information of all OSPF interfaces:

```
Switch# show ip ospf interface

Interface Name: System                IP Address: 10.1.1.1/24 (Link Up)
Network Medium Type: BROADCAST        Metric: 1
Area ID: 0.0.0.0                      Administrative State: Enabled
Priority: 1                           DR State: BDR
DR Address: 10.1.1.2                  Backup DR Address: 10.1.1.1
Hello Interval: 10                    Dead Interval: 40
Transmit Delay: 1                     Retransmit Time: 5
Authentication: None
Passive Mode: Disabled

Interface Name: ip100                IP Address: 192.168.100.1/24 (Link Down)
Network Medium Type: BROADCAST        Metric: 1
Area ID: 0.0.0.0                      Administrative State: Disabled
Priority: 1                           DR State: DOWN
DR Address: None                      Backup DR Address: None
Hello Interval: 10                    Dead Interval: 40
Transmit Delay: 1                     Retransmit Time: 5
Authentication: None
Passive Mode: Disabled
```

To show information of System interfaces:

```
Switch# show ip ospf interface System

Interface Name: System                      IP Address: 10.1.1.1/24 (Link Up)
Network Medium Type: BROADCAST              Metric: 1
Area ID: 0.0.0.0                            Administrative State: Enabled
Priority: 1                                 DR State: BDR
DR Address: 10.1.1.2                        Backup DR Address: 10.1.1.1
Hello Interval: 10                          Dead Interval: 40
Transmit Delay: 1                           Retransmit Time: 5
Authentication: None
Passive Mode: Disabled
```

Field	Description
Interface Name	Name of the interface.
IP Address	IP address of the source IP address used to send out OSPF packet to neighbor.
Network Medium Type	The type of OSPF network.
Metric	OSPF interface cost. It is specified with the command **ip ospf cost**.
Area ID	The area this interface belongs to. It is specified with the command **network area**.
Administrative State	The administrative state of this interface. It is specified with the command **network area**.
DR State	Interface state machine. It may be DR, BDR, OTHER, WAIT or DOWN.
DR Address	The IP address of the Designated Router.
Backup DR Address	The IP address of the Backup Designated Router.
Hello Interval	The interval between hello packets. It is specified with the command **ip ospf hello-interval**.
Dead Interval	The interval during which at least one hello packet form a neighbor must be received before it is declared dead. It is specified with the command **ip ospf dead-interval**.
Transmit Delay	The estimated number of seconds it takes to transmit a Link State Update Packet over this interface. It is not configurable and always is 1.
Retransmit Time	The number of seconds between LSA retransmissions, for adjacencies belonging to this interface. It is not configurable and always is 5.
Authentication	The authentication type used on this interface. It is specified with the command **ip ospf authentication**.

Passive Mode	The status of passive. It is specified with the command **passive-interface**.
Distribute List In	The inbound filter used on this interface. It is specified with the command **distribute-list in**.

11-28 show ip ospf neighbor

Use this command to display information on OSPF neighbors.

show ip ospf neighbor [{detail | *IPADDR*}] [vrf *VRF-NAME*]

Syntax Description	
detail	(Optional) Specifies to display detailed information of neighbors.
IPADDR	(Optional) Specifies the neighbor's IP address to display the OSPF information.
vrf *VRF-NAME*	(Optional) Specifies to show neighbor information about OSPF VRF instance.
N/A	Display brief information about all OSPF neighbors.

Default None.

Command Mode Privileged mode.

Usage Guideline Use this command to display information on OSPF neighbors.

Example To show brief information about all OSPF neighbors:

```
Switch# show ip ospf neighbor

IP Address of    Router ID of    Neighbor     Neighbor
Neighbor         Neighbor        Priority     State
-------------- --------------  --------     ----------
10.1.1.2         2.2.2.2         1            Full
```

Field	Description
IP Address of Neighbor	Interface address of the neighbor router.
Router ID of Neighbor	Router ID of the neighbor router.
Neighbor Priority	Priority of the neighbor router.
Neighbor State	State machine of adjacency.

To show detail information about neighbor with IP 10.1.1.2:

```
Switch# show ip ospf neighbor 10.1.1.2

Neighbor ID: 2.2.2.2                    IP Address: 10.1.1.2
Neighbor Options: 2                     Neighbor Priority: 1
Neighbor State: Full                    State Changes: 6 times
```

Field	Description
Neighbor ID	Router ID of the neighbor router.
IP Address	Interface address of the neighbor router.
Neighbor Options	Option in the Hello packet sent by neighbor router.
Neighbor Priority	Priority of the neighbor router.
Neighbor State	State machine of adjacency.
State Changes	The times that neighbor state has changed.

11-29 show ip ospf virtual-link

Use this command to show information about OSPF virtual link.

show ip ospf virtual-link [*AREA-ID NEIGHBOR-ID***] [vrf** *VRF-NAME***]**

Syntax Description	
AREA-ID	(Optional) Specifies the area ID which the virtual link belongs to.
NEIGHBOR-ID	(Optional) Specifies the router ID of peer of virtual link.
vrf *VRF-NAME*	(Optional) Specifies to show virtual link information about OSPF VRF instance.
N/A	Display brief information about all OSPF virtual links.

Default None

Command Mode Privileged mode

Usage Guideline Use this command to show virtual link information. If *AREA-ID* and *NEIGHBOR-ID* is specified, only the virtual link with the same area ID and neighbor ID will be displayed.

Example To show information about virtual link:

```
Switch# show ip ospf virtual-link

Virtual Interface Configuration

Transit       Virtual      Hello      Dead       Authentication     Link
Area ID       Neighbor     Interval   Interval                      Status
-------       --------     --------   --------   ----------------   ------
4.4.4.4       1.1.1.1      10         60         MD5                Up
4.4.4.4       6.6.6.6      10         250        Simple             Down

Total Entries: 2
```

Field	Description
Transit Area ID	The non-backbone area the two endpoints of virtual link have in common.
Virtual Neighbor Router	Router ID of the other endpoint of the virtual link.
Hello Interval	The interval between hello packets. It is specified with the command **area virtual-link**.
Dead Interval	The interval during which at least one hello packet form a virtual neighbor must be received before it is declared dead. It is specified with the command **area virtual-link**.

Authentication	The authentication type used by the virtual link. It is specified with the command **area virtual-link**.
Link Status	When the other endpoint is reachable according to routing table, the virtual link is link up. Or it is link down.

11-30 show ip ospf virtual-neighbor

Use this command to show information on OSPF neighbors built on virtual link.

show ip ospf virtual-neighbor [*AREA-ID NEIGHBOR-ID***] [vrf** *VRF-NAME***]**

Syntax Description	
AREA-ID	(Optional) Specifies the area ID which the virtual neighbor belongs to.
NEIGHBOR-ID	(Optional) Specifies the router ID of virtual neighbor.
vrf *VRF-NAME*	(Optional) Specifies to show virtual neighbor information about OSPF VRF instance.
N/A	Display brief information about all OSPF virtual neighbors.

Default None.

Command Mode Privileged Mode.

Usage Guideline Use this command to show information of the OSPF neighbor on virtual link. If the *AREA-ID* and *NEIGHBOR-ID* is specified, only the virtual neighbor with the same area ID and neighbor ID will be displayed.

Example To show information about virtual neighbor:

```
Switch# show ip ospf virtual-neighbor

Virtual Interface Configuration

Transit         Router ID of     IP Address of    Virtual Neighbor
Area ID         Virtual Neighbor Virtual Neighbor State
--------------- ---------------- ---------------- ---------------
1.1.1.1         2.2.2.2          100.1.1.1        Full

Total Entries : 1

Switch#
```

Field	Description
Transit Area ID	The non-backbone area the two endpoints of virtual neighbor have in common.
Router ID of Virtual Neighbor Router	Router ID of the other endpoint of the virtual neighbor.
IP Address of Virtual Neighbor	IP address of the other endpoint of the virtual neighbor.
Virtual Neighbor State	State machine of adjacency.

11-31 debug ip ospf

Use this command to turn on the OSPF debug function. Use the **no** form of this command to turn off the OSPF debug function.

debug ip ospf

no debug ip ospf

Syntax Description None

Default By default the OSPF debug function is turned off.

Command Mode Privileged mode.

Usage Guideline Use this command to turn on or turn off the OSPF debug function while the global debug function has been turned on before.

Example The following example turns on the OSPF debug function:

```
Switch# debug ip ospf
Switch#
```

11-32 debug ip ospf neighbor

Use this command to turn on the OSPF neighbor state debug switch. Use the **no** form of the command to turn off the OSPF neighbor state debug switch.

debug ip ospf neighbor

no debug ip ospf neighbor

Syntax Description None.

Default By default the OSPF neighbor state debug switch is turned off.

Command Mode Privileged mode.

Usage Guideline Use this command to turn on or turn off the OSPF neighbor state debug switch. When the neighbor state changes or some events happen to change the neighbor state, debug information will print if the OSPF debug function is turned on.

Use the command **debug ip ospf** to turn off the OSPF debug function.

Example The following example turns on OSPF neighbor state debug switch:

```
Switch# debug ip ospf neighbor
Switch#
NBR 2.2.2.2 state change from LOADING to FULL tic 100
NBR 3.3.3.3 state change from FULL to DOWN tic 100
```

11-33 debug ip ospf interface

Use this command to turn on the OSPF interface state debug switch. Use the **no** form of the command to turn off the OSPF interface state debug switch.

debug ip ospf interface

no debug ip ospf interface

Syntax Description None.

Default By default the OSPF interface state debug switch is turned off.

Command Mode Privileged mode.

Usage Guideline Use this command to turn on or turn off the OSPF interface state debug switch. When the OSPF interface state changes or some events happen to change the interface state, debug information will print. When DR selection happens, debug information will also print if the OSPF debug function is turned on.

Use the command **debug ip ospf** to turn off the OSPF debug function.

Example The following example turns on the OSPF interface state debug switch:

```
Switch# debug ip ospf interface
Switch#
intf 10.1.1.1 up tic 10
intf 100.1.1.1 down tic 20
OSPF: Select DR: 2.2.2.2
OSPF: Select BDR: 1.1.1.1
```

11-34 debug ip ospf lsa-originating

Use this command to turn on the OSPF LSA originating debug switch. Use the **no** form of the command to turn off the OSPF LSA originating debug switch.

debug ip ospf lsa-originating

no debug ip ospf lsa-originating

Syntax Description None.

Default By default the OSPF LSA originating debug switch is turned off.

Command Mode Privileged mode.

Usage Guideline Use this command to turn on or turn off the OSPF LSA originating debug switch. When the LSA originated, debug information will be printed if the OSPF debug function is turned on.

Use the command **debug ip ospf** to turn off the OSPF debug function.

Example The following example turns on the OSPF LSA originating debug switch:

```
Switch# debug ip ospf lsa-originating
Switch#
Build Router LSA id 100.1.1.2 for area 0.0.0.0 seq 80000001 tic 10
```

11-35 debug ip ospf lsa-flooding

Use this command to turn on the OSPF LSA flooding debug switch. Use the **no** form of the command to turn off the OSPF LSA flooding debug switch.

debug ip ospf lsa-flooding

no debug ip ospf lsa-flooding

Syntax Description None.

Default By default the OSPF LSA flooding debug switch is turned off.

Command Mode Privileged mode.

Usage Guideline Use this command to turn on or turn off the OSPF LSA flooding debug switch. When the LSA is received, it will be added into the local database or flooded to the neighboring router. The debug information will be print if the OSPF debug function is turned on.

Use the command **debug ip ospf** to turn off the OSPF debug function.

Example The following example turns on the OSPF LSA flooding debug switch:

```
Switch# debug ip ospf lsa-flooding
Switch#
Received LSA type 1 id 2.2.2.2 from nbr 2.2.2.2 in area 0.0.0.0 seq 80000001
csum fe3a tic 15
Flood LSAs in area 0.0.0.0 tic 15
```

11-36 debug ip ospf packet-receiving

Use this command to turn on the OSPF packet receiving debug switch. Use the **no** form of the command to turn off the OSPF packet receiving debug switch.

debug ip ospf packet-receiving

no debug ip ospf packet-receiving

Syntax Description None.

Default By default the OSPF packet receiving debug switch is turned off.

Command Mode Privileged mode.

Usage Guideline Use this command to turn on or turn off the OSPF packet receiving debug switch. When one OSPF protocol packet is received, the debug information will be print if the OSPF debug function is turned on.

Use the command **debug ip ospf** to turn off the OSPF debug function.

Example The following example turns on the OSPF packet receiving debug switch:

```
Switch# debug ip ospf packet-receiving
Switch#
Received a Hello packet from addr 10.1.1.2 at interface System tic 100
Received a Hello packet from addr 100.1.1.2 at interface ip100 tic 102
```

11-37 debug ip ospf packet-transmitting

Use this command to turn on the OSPF packet transmitting debug switch. Use the **no** form of the command to turn off the OSPF packet receiving debug switch.

debug ip ospf packet-transmitting

no debug ip ospf packet-transmitting

Syntax Description None.

Default By default the OSPF packet transmitting debug switch is turned off.

Command Mode Privileged mode.

Usage Guideline Use this command to turn on or turn off the OSPF packet transmitting debug switch. When one OSPF protocol packet is sent out, the debug information will be printed if the OSPF debug function is turned on.

Use the command **debug ip ospf** to turn off the OSPF debug function.

Example The following example turns on the OSPF packet transmitting debug switch:

```
Switch# debug ip ospf packet-transmitting
Switch#
Send out a Hello on interface 10.1.1.1 dst 255.0.0.5 tic 200
Send out a Hello on interface 100.1.1.1 dst 255.0.0.5 tic 220
```

11-38 debug ip ospf spf

Use this command to turn on the OSPF SPF calculation debug switch. Use the **no** form of the command to turn off the OSPF SPF calculation debug switch.

debug ip ospf spf

no debug ip ospf spf

Syntax Description None.

Default By default the OSPF SPF calculation switch is turned off.

Command Mode Privileged mode.

Usage Guideline Use this command to turn on or turn off the OSPF SPF calculation debug switch. When one SFP calculation is processing, the debug information will be print if the OSPF debug function is turned on.

Use the command **debug ip ospf** to turn off the OSPF debug function.

Example The following example turns on the OSPF SPF calculation debug switch:

```
Switch# debug ip ospf spf
Switch#
Running SPF-intra for area 0.0.0.0 tic 300
SPF-intra calculation completed tic 310
```

11-39 debug ip ospf timer

Use this command to turn on the OSPF timer debug switch. Use the **no** form of the command to turn off the OSPF timer debug switch.

debug ip ospf timer

no debug ip ospf timer

Syntax Description None.

Default By default the OSPF timer switch is turned off.

Command Mode Privileged mode.

Usage Guideline Use this command to turn on or turn off the OSPF timer debug switch. When the event, related to OSPF timer happens, the debug information will be printed if the OSPF debug function is turned on.

Use the command **debug ip ospf** to turn off the OSPF debug function.

Example The following example turns on the OSPF timer debug switch:

```
Switch# debug ip ospf timer
Switch#
Start Hello timer at interface System tic 20
Wait timer expired at interface System tic 100
```

11-40 debug ip ospf virtual-link

Use this command to turn on the OSPF virtual link debug switch. Use the **no** form of the command to turn off the OSPF virtual link debug switch.

debug ip ospf virtual-link

no debug ip ospf virtual-link

Syntax Description None.

Default By default the OSPF virtual link switch is turned off if the OSPF debug function is turned on.

Command Mode Privileged mode.

Usage Guideline Use this command to turn on or turn off the OSPF virtual link debug switch. When the event, related to the OSPF virtual link happens, the debug information will be printed.

Use the command **debug ip ospf** to turn off the OSPF debug function.

Example The following example turns on the OSPF virtual link debug switch:

```
Switch# debug ip ospf virtual-link
Switch#
Virtual link up transit area 1.1.1.1 vnbr 3.3.3.3 tic 260
```

11-41 debug ip ospf route

Use this command to turn on the OSPF route debug switch. Use the **no** form of the command to turn off the OSPF route debug switch.

debug ip ospf route

no debug ip ospf route

Syntax Description None.

Default By default the OSPF route switch is turned off.

Command Mode Privileged mode.

Usage Guideline Use this command to turn on or turn off the OSPF route debug switch. When one OSPF route is added, updated or deleted, the debug information will be printed if the OSPF debug function is turned on.

Use the command **debug ip ospf** to turn off the OSPF debug function.

Example The following example turns on the OSPF route debug switch:

```
Switch# debug ip ospf route
Switch#
Add an OSPF route level 1 dst 172.18.1.1 mask 255.255.255.0  nh cnt 1 cost
10 cost2: 0 tic: 300
```

11-42 debug ip ospf redistribution

Use this command to turn on the OSPF redistribution debug switch. Use the **no** form of the command to turn off the OSPF redistribution debug switch.

debug ip ospf redistribution

no debug ip ospf redistribution

Syntax Description None.

Default By default the OSPF redistribution switch is turned off.

Command Mode Privileged mode.

Usage Guideline Use this command to turn on or turn off the OSPF redistribution debug switch. When one route of another protocol is redistributed into OSPF or not redistributed into OSPF any more, the debug information will be print if the OSPF debug function is turned on.

Use the command **debug ip ospf** to turn off the OSPF debug function.

Example The following example turns on the OSPF redistribution debug switch:

```
Switch# debug ip ospf redistribution
Switch#
Import AS external route from src 5 net 192.1.1.1  mask 255.255.255.0 type 2
cost 50 fwd 10.1.1.100 tic 500
```

11-43 debug ip ospf show counter

Use this command to display the OSPF statistic counter.

debug ip ospf show counter [packet | neighbor | spf]

Syntax Description	
packet	(Optional) Specifies to display the OSPF packet counter.
neighbor	(Optional) Specifies to display the OSPF neighbor counter.
spf	(Optional) Specifies to display the OSPF SPF event counter.
N/A	Display all OSPF counters.

Default None.

Command Mode Privileged mode.

Usage Guideline Use this command to check statistic information about the OSPF packet, neighbor and SPF calculation.

Example The following example displays all OSPF statistic counters:

```
Switch# debug ip ospf show counter

OSPF Debug Statistic Counters
Packet Receiving:
  Total  : 5
  Hello  : 5
  DD     : 0
  LSR    : 0
  LSU    : 0
  LSAck  : 0
  Drop   : 0
  Auth Fail : 0

Packet Sending:
  Total  : 5
  Hello  : 5
  DD     : 0
  LSR    : 0
  LSU    : 0
  LSAck  : 0

Neighbor State:
  Change : 3
  SeqMismatch : 0

SPF Calculation:
  Intra  : 1
  Inter  : 1
  Extern : 1
```

11-44 debug ip ospf clear counter

Use this command to reset the OSPF statistic counter.

debug ip ospf clear counter [packet | neighbor | spf]

Syntax Description	
packet	(Optional) Specifies to clear the OSPF packet counter.
neighbor	(Optional) Specifies to clear the OSPF neighbor counter.
spf	(Optional) Specifies to clear the OSPF SPF event counter.
N/A	Clear all OSPF counters.

Default None.

Command Mode Privileged mode.

Usage Guideline Use this command to reset the OSPF statistic counter. After the reset, the specified counter will change to 0.

Example The following example resets all OSPF statistic counters:

```
Switch# debug ip ospf clear counter
Switch#
```

11-45 debug ip ospf show database

Use this command to display detailed information about the OSPF LSDB.

debug ip ospf show database {rt-link | net-link | summary-link | external-link | type7-link}

Syntax Description	
rt-link	Specifies to display information about the **rt-link** parameter.
net-link	Specifies to display information about the **net-link** parameter.
summary-link	Specifies to display information about the **summary-link** parameter.
external-link	Specifies to display information about the **external-link** parameter.
type7-link	Specifies to display information about the **type7-link** parameter.

Default None.

Command Mode Privileged mode.

Usage Guideline Use this command to check detailed information about the OSPF LSDB.

Example The following example displays detailed information about the Router's LSA:

```
Switch# debug ip ospf show database rt-link

OSPF Phase2 RT Link:

===========
AREA 0.0.0.0:
 Router LSA:
 Link-State ID: 100.1.1.2
 Advertising Router: 100.1.1.2
 LS Age: 10 Seconds
 Options: 0x2
 .... ...0 = 0 Bit Isn't Set
 .... ..1. = E: ExternalRoutingCapability
 .... .0.. = MC: NOT Multicast Capable
 .... 0... = N/P: NSSA Bit
 ...0 .... = EA: Not Support Rcv And Fwd EA_LSA
 ..0. .... = DC: Not Support Handling Of Demand Circuits
 .0.. .... = O: O Bit Isn't Set
 0... .... = 7 Bit Isn't Set
 LS Sequence Number: 0x80000001
 Length: 36
 Flags: 0x0
 .... ...0 = B: NO Area Border Router
 .... ..0. = E: NO AS Boundary Router
 .... .0.. = V: NO Virtual Link Endpoint
 Number Of Links: 1
 Type: Stub      ID: 10.1.1.0        Data: 255.255.255.0    Metric: 1
 Internal Field:
 Del_flag: 0x0  I_ref_count: 0  Seq: 0x80000001  Csum: 0x4d28
 Rxtime: 0  Txtime: 0  Orgage: 0
 Current Time: 10
```

11-46 debug ip ospf show request-list

Use this command to display current LSA information of the internal OSPF's request list.

debug ip ospf show request-list

Syntax Description None.

Default None.

Command Mode Privileged mode.

Usage Guideline Use this command to check the information about the LSAs OSPF that is requesting to neighbors.

Example The following example displays the current requested LSA:

```
Switch# debug ip ospf show request-list

OSPF Request List:

*Area 0.0.0.0:
Circuit: 1.1.1.1
Neighbor: 90.2.0.1  IP: 1.1.1.2
 LSID: 192.194.134.0  RTID: 90.2.0.1
 LSID: 192.194.135.0  RTID: 90.2.0.1
 LSID: 192.194.136.0  RTID: 90.2.0.1
 LSID: 192.194.137.0  RTID: 90.2.0.1
 LSID: 192.194.138.0  RTID: 90.2.0.1
```

11-47 debug ip ospf show redistribution

Use this command to display the current internal OSPF redistribution list.

debug ip ospf show redistribution

Syntax Description None.

Default None.

Command Mode Privileged mode.

Usage Guideline Use this command to check the information about the external route imported into OSPF.

Example The following example displays the external routes imported into OSPF:

```
Switch# debug ip ospf show redistribution

OSPF Redistribution List:

IP                  Nexthop          State Type Tag
------------------  ---------------  ----- ---- ---------------
1.1.1.0/24          0.0.0.0          ON    2    0.0.0.0

OSPF ASE Table:

IP                  Nexthop          State Type Tag
------------------  ---------------  ----- ---- ---------------
1.1.1.0/24          0.0.0.0          ON    2    0.0.0.0
```

11-48 debug ip ospf show summary-list

Use this command to display the current internal OSPF summary list.

debug ip ospf show summary-list

Syntax Description None.

Default None.

Command Mode Privileged mode.

Usage Guideline Use this command to check the information about the route to be aggregated.

Example The following example displays route information to be aggregated:

```
Switch# debug ip ospf show summary-list

OSPF Summary List:

Area 0.0.0.0:
Circuit: 1.1.1.1
Neighbor: 90.2.0.1  IP: 1.1.1.2
LSID: 1.1.1.1 RTID: 1.1.1.1

Circuit: 2.2.2.1

Circuit: 10.1.1.6
```

11-49 debug ip ospf log

Use this command to turn on the OSPF debug log function. Use the **no** form of this command to turn off the OSPF debug log function.

debug ip ospf log

no debug ip ospf log

Syntax Description None.

Default None.

Command Mode Privileged mode.

Usage Guideline Use this command to turn on or turn off the OSPF debug log function. When some important OSPF events happen, some system log entries will be added.

Example The following example turns on the OSPF debug log function:

```
Switch# debug ip ospf log
Switch#
```

Protocol Independent Multicast (PIM) Commands

12-1 ip pim

To enable Protocol Independent Multicast (PIM) on an interface, use the **ip pim** command in interface configuration mode. To disable PIM on the interface, use the **no** form of this command.

ip pim {dense-mode | sparse-mode | sparse-dense-mode}

no ip pim

Syntax Description	
dense-mode	Enables dense mode of operation.
sparse-mode	Enables sparse mode of operation.
sparse-dense-mode	Enables sparse-dense-mode of operation.

Default PIM is disabled on all interfaces

Command Mode Interface configuration mode.

Usage Guideline This command enables PIM protocol on the specified interface. An interface can be configured to be in dense mode, sparse mode or sparse-dense mode.
If you want to use PIM to forward multicast packets, use **ip multicast-routing** command to enable multicast global state.

To verify your configuration, use **show ip pim sparse-mode interface** or **show ip pim dense-mode interface**.

Example This command configures interface VLAN 1 to enable PIM dense-mode.

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ip pim dense-mode
```

Disable pim on interface VLAN 1.

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# no ip pim
```

12-2 ip pim query-interval

To configure the frequency of Protocol Independent Multicast (PIM) router query messages, use the **ip pim query-interval** command in interface configuration mode. To return to the default interval, use the **no** form of this command.

ip pim query-interval *SECONDS*

no ip pim query-interval

Syntax Description	
SECONDS	Interval of sending the hello message, in the range of 1 to 65535 seconds.

Default 30 seconds

Command Mode Interface configuration mode.

Usage Guideline The change of hello interval would lead to the change of hello hold time. The principle of the updating hold time is configured hello interval * 3.5.

To verify your configuration, use **show ip pim dense-mode interface detail** or **show ip pim sparse-mode interface detail**.

Example Configure the PIM query interval of VLAN 1 to 60 seconds.

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ip pim query-interval 60
```

Configure the query interval of VLAN 2 back to default.

```
Switch# configure terminal
Switch(config)# interface vlan 2
Switch(config-if)# no ip pim query-interval
```

12-3 ip pim join-prune-interval

To configure the interval of Protocol Independent Multicast (PIM) router join/prune messages, use the **ip pim join-prune-interval** command in global configuration mode. To return default, use the **no** form of this command.

ip pim join-prune-interval *SECONDS*

no ip pim join-prune-interval

Syntax Description	
SECONDS	Interval of sending the join/prune message, in the range of 1 to 65535 seconds.

Default 60 seconds.

Command Mode Global configuration mode

Usage Guideline This command only takes effect when the interface is PIM SM enabled.

When configure the Join/Prune interval, the user needs to consider the factors, such as configured bandwidth and expected average number of multicast route entries for the attached network or link (e.g., the period would be longer for lower-speed links, or for routers in the center of the network that expect to have a larger number of entries).

For SM-mode, router will periodically send the join message based on this interval. The hold-time in a Join/Prune message is (3.5 * join-prune-interval). The receiving router will start a timer based on this hold-time, and prune the interface if hold-time timer expires.

You can verify your configuration through command **show ip pim sparse-mode interface detail.**

Example Configure the PIM join/prune interval to 1000 seconds.

```
Switch# configure terminal
Switch(config)# ip pim join-prune-interval 1000
```

Configure the PIM join/prune interval back to default.

```
Switch# configure terminal
Switch(config)#no ip pim join-prune-interval
```

12-4 ip pim dr-priority

To configure the priority for which a switch is elected as the designated router (DR), use the **ip pim dr-priority** command in interface configuration mode. To return default, use the **no** form of this command.

ip pim dr-priority *PRIORITY*

no ip pim dr-priority

Syntax Description	
PRIORITY	The larger the value, the higher the priority is. The range is 0 to 4294967294.

Default 1

Command Mode Interface configuration mode

Usage Guideline The switch with the biggest priority would be selected as DR on a LAN. If several switches have the same
DR priority, the one with the highest IP address would be selected. If the DR priority field is not set in PIM hello messages, the one with highest IP address is selected to be DR.

To verify your configuration, use **show ip pim sparse-mode interface detail**.

Example Configure the priority of VLAN 1 to be 100.

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ip pim dr-priority 100
```

Configure DR priority of VLAN 2 back to default.

```
Switch# configure terminal
Switch(config)# interface vlan 2
Switch(config-if)# no ip pim dr-priority
```

12-5 ip pim register-suppression

Use the **ip pim register-suppression** command to configure the register suppression time. To return to the default interval, use the **no** form of this command.

ip pim register-suppression *SECONDS*

no ip pim register-suppression

Syntax Description	
SECONDS	Specify the value of register suppression time. The range of this value is 11-255 seconds.

Default 60 seconds.

Command Mode Global configuration mode.

Usage Guideline When a DR receives the register-stop message, it will start the suppression timer. During suppression period, a DR stops sending the register message to the RP.

Use the command on the first hop router.

Please be noted, the parameter Register Probe Time in RFC 4601 is fixed to 5. Because the value of the Register Probe Time must be less than half the value of the Register Suppression Time to prevent a possible negative value in the setting of the Register-Stop Timer, the minimal value for Register Suppression Time is 11.

To verify your configuration, use command **show ip pim**.

Example Configure the PIM register suppression to be 100 seconds.

```
Switch# configure terminal
Switch(config)# ip pim  register-suppression 100
```

Restore the default value.

```
Switch# configure terminal
Switch(config)# no ip pim register-suppression
```

12-6 ip pim rp-address

Use the ip pim rp-address command to create a static RP in PIM-SM. To delete the static RP entry, use the **no** form of this command.

ip pim rp-address *RP-ADDRESS* ***[****ACCESS_LIST****]***

no ip pim rp-address *RP-ADDRESS*

Syntax Description	
RP-ADDRESS	Format X.X.X.X; specify the IP address of RP.
ACCESS_LIST	The name of the access list.

Default No static RP entry.

Command Mode Global configuration mode.

Usage Guideline This Command is used to configure static RP.

If no ACL is configured in this command, it means this static RP support all the multicast groups 224.0.0.0/4. To disable this configuration, use **no ip pim rp-address** *RP-ADDRESS.*

You can configure only one ACL list on one RP, and in each list, the same group range can exist. And for the same group range entry, only the first configured one can work. If the working group range is deleted, the switch will auto search if there is another entry existed with the same group range. If does, this new entry will be selected, this may change the static RP address.The number of ACL entry configured to static RP is limited, and the total number of group range configured to static RP is also limited. If any limitation exceeded, no more static RP can be created.

To verify your configuration, you can use **show ip pim**.

Example Configure static RP address 172.18.62.1 with group range 234.0.0.0/12.

```
Switch# configure terminal
Switch(config)# ip pim rp-address 172.18.62.1 statirp-acl
Switch(config)# ip standard access-list statirp-acl
Switch(config-standard-acl)#permit 234.0.0.0/12
Switch(config-standard-acl)#end
```

Configure static RP address 172.18.63.254 with group range 224.0.0.0/4.

```
Switch# configure terminal
Switch(config)# ip pim rp-address 172.18.63.254
```

Delete access list of static RP binding at 172.18.62.1.

```
Switch# configure terminal
Switch(config)# no ip pim rp-address 172.18.62.1
```

12-7 ip pim rp-candidate

To configure the router to advertise itself as a Protocol Independent Multicast (PIM) Version 2 candidate rendezvous point (RP) to the bootstrap router (BSR), use the **ip pim rp-candidate** command in global configuration mode. To return default, use the **no** form of this command. If no parameter is added in **no** command, the device will restore default value for interval of CRP-Adv and priority of CRP interface. If interface name added in **no** form of this command, the device will clean the ACL information binding on this interface.

ip pim rp-candidate *IFNAME* **[interval** *SECONDS***] [priority** *PRIORITY***] [group-list** *ACCESS_LIST***] [wildcard-prefix-cnt {0|1}]**

no ip pim rp-candidate [*IFNAME***]**

Syntax Description	
IFNAME	Interface name. The IP address associated with this interface is advertised as a candidate RP address.
ACCESS_LIST	The name of access list. If no **group-list** is specified, the switch is a candidate RP for all groups.
SECONDS	Specify interval of sending CRP-Adv message to BSR,. The range is 0 to 102.
PRIORITY	Specify the priority of this CRP interface, in the range 0 to 255.
0	Specify the Prefix Count value of the wildcard address (224.0.0.0/24) to be set to 0 in PIM C-RP-Adv message.
1	Specify that the wildcard prefix count value will be set to 1 in PIM C-RP-Adv message.

Default No candidate RP is configured. The default CRP-Adv interval is 60 seconds. The default priority value is 192. The default wildcard prefix count is 0.

Command Mode Global configuration mode

Usage Guideline This command is used to configure candidate RP information of PIM. The change of CRP-Adv interval would also change the hold time of the CRP at the RP. The hold time at RP is CRP-Adv interval multiplied by 2.5.

It is possible to have the cast, multiple CRP mapping to the same groups. At this situation, the method below is used.

1. Perform longest match on group-range to obtain a list of RPs.
2. From this list of matching RPs, find the one with highest priority. Eliminate any RPs from the list that have lower priorities.
3. If only one RP remains in the list, use that RP.
4. If multiple RPs are in the list, use the PIM hash function to choose one.

So, you can use this command to configure the priority of this CRP to specify the sequence to select the RP for the groups.

This command can cause the router to send a PIM Version 2 message advertising itself as a candidate RP to the BSR and set the parameter of this CRP. To specify an

interface as the candidate RP of a specific group, execute this command with ACL. One interface can only configure one ACL.The number of ACL entry configured to candidate RP is limited, and the total number of group range configured to candidate RP is also limited. If any limitation exceeded, no more candidate RP can be created.

To verify your configuration, use **show ip pim**.

Example

Configure candidate RP interface ipif1 with group range 234.0.0.0/12, and priority set to 100.

```
Switch# configure terminal
Switch(config)# ip pim rp-candidate ipif1 priority 100 group-list crp-acl
Switch(config)# ip standard access-list crp-acl
Switch(config-standard-acl)#permit 234.0.0.0/12
Switch(config-standard-acl)#end
```

Set CRP configuration back to default:

```
Switch# configure terminal
Switch(config)# no ip pim rp-candidate ipif1
```

The following example configures the PIM wildcard prefix count to be 1:

```
Switch# configure terminal
Switch(config)# ip pim rp-candidate ipif1 wildcard-prefix-cnt 1
```

Delete all CRP ACL list binding on the interface ipif1:

```
Switch# configure terminal
Switch(config)# no ip pim rp-candidate ipif1
```

12-8 ip pim spt-threshold

Use this command to configure the condition to switchover to the source tree. To restore the default setting, use **no** form of this command.

ip pim spt-threshold { 0 | infinity }

no ip pim spt-threshold

Syntax Description	
0	To establish the source tree right at the arrival of the first packet.
infinity	Always rely on the shared tree.

Default Infinity.

Command Mode Global configuration mode.

Usage Guideline Use this command on the last hop of the router.

In PIM-SM mode, initially the multicast traffic from the source will be flowing along the RPT share tree to the receiver. After the first packet arrives at the last hop router, for each group of traffic, it can operate in one of the following two modes. With mode “infinity”, the traffic keeps following the share tree. With mode “0”, the source tree will be established and the traffic switchover to the source tree.

To verify your configuration, use command **show ip pim**.

Example To configure PIM work in SPT mode at the arrival of the first packet.

```
Switch# configure terminal
Switch(config)# ip pim spt-threshold 0
```

To configure PIM work always in RPT mode.

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

12-9 ip pim rp-register-kat

Use this command to configure the keep alive time when RP receiving a register message. To restore default value, use **no** form of this command.

ip pim rp-register-kat *SECONDS*

no ip pim rp-register-kat

Syntax Description	
SECONDS	Keep alive time, in the range 1 to 65525 seconds.

Default 185 seconds.

Command Mode Global configuration mode.

Usage Guideline When the DR receives multicast stream, it will send register message to the RP of the group. And when the RP receives this message, it would set up a timer for this (S, G) entry. This command configures the value of this timer.

To verify your configuration, use command **show ip pim**.

Example To configure PIM register keep alive time to 500 seconds.

```
Switch# configure terminal
Switch(config)# ip pim rp-register-kat 500
```

To restore the default value:

```
Switch# configure terminal
Switch(config)# no ip pim rp-register-kat
```

12-10 ip pim bsr-candidate

This command is used to enable the candidate bootstrap function of the interface or set the hash mask length of calculating the property RP. To return default, use **no** form of this command.

ip pim bsr-candidate *IFNAME* **[hash-mask-length** *VALUE***] [priority** *PRIORITY***]**

no ip pim bsr-candidate *IFNAME*

Syntax Description	
IFNAME	Specify the interface whose IP address will be announced as the bootstrap router address.
VALUE	Enter a hash mask length, which will be used with the IP address of the candidate RP and the multicast group address, to calculate the hash algorithm used by the router to determine which CRP on the PIM-SM enabled network will be the RP. The range is 0 to 32.
PRIORITY	Configure priority for a BSR candidate. The candidate with the highest priority is preferred. If the priority values are the same, the router with the highest IP address is preferred. The range is 0 to 255. If not specified, the default priority is 64.

Default The hash mask length is 30, the priority is 64, and the BSR function is disabled.

Command Mode Global configuration mode

Usage Guideline This command only takes effect when the interface specified by the command has IP address configured and is PIM-SM enabled.

This command causes the router to send bootstrap messages to announce the IP address of the designated interface as the BSR candidate address.

The hash mask is used by all routers within a domain, to map a group to one of the RPs from the matching set of group-range-to-RP mappings (this set all have the same longest mask length and same highest priority). The algorithm takes as input the group address, and the addresses of the candidate RPs from the mappings, and gives as output one RP address to be used.

To verify your configuration, use command **show ip pim sparse-mode bsr-router.**

Example Configure the PIM candidate BSR priority to be 10 and hash mask length to be 32.

```
Switch# configure terminal
Switch(config)# ip pim bsr-candidate ipif1 hash-mask-length 32 priority 10
```

Disable the function of BSR in ipif1.

```
Switch# configure terminal
Switch(config)# no ip pim bsr-candidate ipif1
```

12-11 ip pim old-register-checksum

Use this command to specify for which RP, the switch should calculate checksum include the data portion or not when transmitting and receiving register messages. To restore the default setting, use **no** form of this command.

ip pim old-register-checksum rp-address *RP-ADDRESS*

no ip pim old-register-checksum rp-address *RP-ADDRESS*

Syntax Description	
RP-ADDRESS	Specifies that the RP will expect to receive a register packet in which the checksum will include the data portion or not.

Default The checksum in register message to any RP doesn't include data portion.

Command Mode Global configuration mode.

Usage Guideline This command is used to decide the checksum in register packet will include the data portion or not. As defined in RFC 4601, the checksum for Registers is done only on the first 8 bytes of the packet, including the PIM header and the next 4 bytes, excluding the data packet portion. Some earlier PIM-SM routers calculate checksum for register packet including data portion. This configuration makes our routers communicate with those earlier routers smoothly. The default setting is not including data portion.

To verify your configuration, use command **show ip pim.**

Example Configure checksum include data for RP 172.18.63.2

```
Switch# configure terminal
Switch(config)# ip pim old-register-checksum rp-address 172.18.63.2
```

Delete checksum include RP 172.18.63.2

```
Switch# configure terminal
Switch(config)#no ip pim old-register-checksum rp-address 172.18.63.2
```

12-12 ip pim ssm

Use this command to configure the SSM multicast group address range. Use the **no** form of the command to disable PIM SSM.

ip pim ssm {default | range *ACCESS-LIST***}**

no ip pim ssm

Syntax Description	
ACCESS-LIST	Specify a standard IP access list that defines the user-specified SSM group addresses.
default	Use the default SSM group addresses. The default SSM group address range is 232/8.

Default PIM SSM is disabled.

Command Mode Global configuration mode

Usage Guideline For an SSM group, the switch will use (S, G) in IGMPv3 report to join SPT. And if the group address of configured range is reported by IGMPv1/v2, it will be ignored by IGMP module. If the ACL entry configured for SSM group address range includes multiple networks, only the first group network will work.

To verify your configuration, use command **show ip pim .**

Example Configure the PIM SSM function enable, use default group address range.

```
Switch# configure terminal
Switch(config)#ip pim ssm default
```

Configure the PIM SSM function enable, and group address range is 239.0.0.0/11

```
Switch# configure terminal
Switch(config)# ip pim ssm range ssm-acl
Switch(config)# ip standard access-list ssm-acl
Switch(config-standard-acl)#permit 239.0.0.0/11
Switch(config-standard-acl)#end
```

The following example disables PIM SSM function.

```
Switch# configure terminal
Switch(config)#no ip pim ssm
```

12-13 show ip pim dense-mode interface

This command is used to display information about PIM-DM interface.

show ip pim dense-mode interface [*IFNAME* **[detail]]**

Syntax Description	
IFNAME	Specify the interface name to be displayed. If no interface name, display all PIM-DM interfaces.
detail	Show detailed information.

Default None.

Command Mode User mode or Privileged mode.

Usage Guideline This command displays PIM-DM configuration information.

Example Display the information of all PIM-DM interfaces.

```
Switch# show ip pim dense-mode interface

IP Address       Interface    Mode  state    Nbr count
---------------- ------------ ----- -------- ----------
10.90.90.90      System       DM    Enabled  1
172.18.1.11      ipif1        DM    Enabled  2

Total Entries: 2
```

Display the detail information of PIM-DM interface System.

```
Switch# show ip pim dense-mode interface System detail

Interface Name: System
Address 10.90.90.90, DR 10.90.90.90
Hello period 30 seconds, Next hello in 29 seconds
Neighbor:
 10.2.0.2
 10.2.0.5
```

Field	Description
IP Address	The IP Address of the interface displayed.
Interface	The name of the interface.
Mode	The mode of PIM of this interface, To change mode of PIM, use **ip pim** command.
state	The PIM-DM state of this interface.
Nbr count	The numbers of neighbors connected to this interface in the LAN.

Neighbor	The address of the neighbors.
DR	The DR address of this LAN

12-14 show ip pim neighbor

This command is used to display PIM neighbor information.

show ip pim neighbor *[IFNAME]*

Syntax Description	
IFNAME	Specify the interface to display the neighbor. If no *IFNAME* specified, all interface's neighbor would be displayed.

Default None.

Command Mode User mode or Privileged mode.

Usage Guideline Use this command to display the neighbor information of PIM. Both PIM-SM and PIM-DM neighbor would be displayed.

Example Display all the interface's neighbor information.

```
Switch# show ip pim neighbor

Neighbor Address  Interface     Uptime      Expires     mode
---------------  ------------  ----------  ----------  -----
10.2.0.2          System        00:00:32    00:01:26    SM

Total Entries: 1
```

Field	Description
Neighbor Address	Specify the neighbor's address.
Interface	Specify the name of interface binding by the neighbor.
Uptime	Length of time (in hours, minutes, and seconds) that the router has known about this neighbor.
Expires	Time (in hours, minutes, and seconds) this neighbor expires.
mode	The mode of this interface. To configure this value, use command **ip pim .**

12-15 show ip pim sparse-mode bsr-router

This command displays PIM-SM bootstrap router information.

show ip pim sparse-mode bsr-router

Syntax Description None.

Default None.

Command Mode User mode or Privileged mode.

Usage Guideline This command is used to show BSR information.

Example Display PIM BSR information.

```
Switch# show ip pim sparse-mode bsr-router
PIMv2 Bootstrap information

This System is the Bootstrap Router (BSR)
BSR Address: 10.90.90.90
BSR Priority: 100, Hash mask length: 30
Role: Candidate BSR  Priority: 100  Hash mask lenth: 30
Next bootstrap message in 00:00:17
state: Elected BSR
Candidate RP: 10.90.90.90(System)
  Group acl: crp-system
Candidate RP: 172.16.11.254(ipif1)
  Group acl: crp-acl
Candidate RP priority : 192
Holdtime 150 seconds
Advertisement interval 60 seconds
Next Cand_RP_advertisement in 00:00:15
```

Field	Description
BSR Address	IP address of the bootstrap router.
BSR Priority	Priority as configured in the **ip pim bsr-candidate** command.
Role	The role of our CBSR
Priority	Priority of our CBSR.
Hash mask length	Length of a mask (32 bits maximum) that is to be ANDed with the group address before the hash function is called. This value is configured in the **ip pim bsr-candidate** command.
state	State of this switch (elected or not)
Next Cand_RP_advertisement in	Time in hours, minutes, and seconds in which the next candidate rendezvous-point advertisement will be sent.

Next bootstrap message in	Time in hours, minutes, and seconds in which the next bootstrap message is due from this BSR.
Holdtime	The hold time of the candidate RP, this value is configured by **ip pim rp-candidate**
Candidate RP	Candidate RP information of this switch.

12-16 show ip pim sparse-mode interface

This command displays PIM-SM interface information.

show ip pim sparse-mode interface [*IFNAME* **[detail]]**

Syntax Description	
IFNAME	Specify the interface to display the neighbor. If no *IFNAME* specified, all interface's neighbor would be displayed.
detail	Display detailed information.

Default None.

Command Mode User mode or Privileged mode.

Usage Guideline Use to display PIM-SM interface information.

Example Show all PIM-SM interface information.

```
Switch# show ip pim sparse-mode interface

IP Address       Interface    Mode  state    Nbr count
---------------- ------------ ----- -------- ----------
10.90.90.90      System       SM    Enabled  1
172.18.63.1      ipif1        SM    Enabled  2

Total Entries: 2
```

Display the detail of PIM interface System.

```
Switch# show ip pim sparse-mode interface System detail

Interface Name: System
Address 10.90.90.90, DR 10.90.90.90
My DR priority is: 1
Hello period 30 seconds, Next hello in 7 seconds
Join/Prune interval 60 seconds
Neighbors:
 10.2.0.2
```

Field	Description
IP Address	The IP Address of the interface displayed.
Interface	The name of the interface.
Mode	The mode of PIM of this interface, To change mode of PIM, use **ip pim** command.
state	The PIM-DM state of this interface.
Nbr count	The number of neighbors connect to this interface

Neighbors	List address of the neighbors below.
Join/Prune interval	The period join message of PIM-SM if this switch has outgoing for a specified group. This value is configured by **ip pim join-prune-interval**.
DR	The DR address of this LAN. To change DR of a LAN, use command **ip pim dr-priority.**

12-17 show ip pim sparse-mode rp mapping

Use this command to display RP mapping information.

show ip pim sparse-mode rp mapping

Syntax Description None.

Default None.

Command Mode User mode or Privileged mode.

Usage Guideline This command is used to display PIM-SM RP mapping information.

Example Display PIM-SM RP mapping information.

```
Switch# show ip pim sparse-mode rp mapping

Group(s): 229.1.3.0/28
  RP: 10.2.0.2
  via bootstrap, priority 192, RP hold time: 150
  Uptime: 00:17:37, expires: 00:01:52
Group(s): 229.1.5.16/28
  RP: 10.90.90.90
  via bootstrap, priority 192, RP hold time: 150
  Uptime: 00:16:54, expires: 00:01:36
Group(s): 231.0.0.0/8
  RP: 10.90.90.90
  via bootstrap, priority 192, RP hold time: 150
  Uptime: 00:16:54, expires: 00:01:36
Group(s): 233.0.0.0/8
  RP: 10.90.90.90
  via bootstrap, priority 192, RP hold time: 150
  Uptime: 00:16:54, expires: 00:01:36
Group(s): 239.0.0.0/11, static
  RP: 172.18.254.1
```

Field	Description
Groups	Group range mapping to the RP below.
RP	Address of the rendezvous point for that group.
RP hold time	Hold time of the RP.
static	Group-to-mapping information from the static rendezvous-point configuration. Create by command **ip pim rp-address.**
expires	Time (in hours, minutes, and seconds) after which the information about candidate RP entry expires. If the router does not receive any refresh messages in this time, it discards information.

Uptime	Length of time (in hours, minutes, and seconds) that the router has known about this rendezvous point.

12-18 show ip pim sparse-mode rp-hash

To display which rendezvous point is being selected for a specified group, use the **show ip pim spars-mode rp-hash** command.

show ip pim sparse-mode rp-hash *GROUP-ADDRESS*

Syntax Description	
GROUP-ADDRESS	Rendezvous-point information for the specified group address.

Default None.

Command Mode User mode or Privileged mode.

Usage Guideline This command displays which rendezvous point was selected for the group specified. It also shows whether this rendezvous point was selected manually or by the PIM Version 2 bootstrap mechanism.

Example Show PIM-SM RP information for 229.1.3.1.

```
Switch#show ip pim sparse-mode rp-hash 229.1.3.1

RP: 10.2.0.2, via bootstrap
Uptime 00:36:46, expires in 00:01:44
```

Show PIM-SM RP information for 239.0.0.0.

```
Switch#show ip pim sparse-mode rp-hash 239.0.0.0
RP: 10.90.90.90, static
```

Field	Description
static	Group-to-mapping information from the static rendezvous-point configuration.
RP	Address of the rendezvous point for that group.

12-19 show ip pim

Use this command to display PIM global information.

show ip pim

Syntax Description None.

Default None.

Command Mode User mode or Privileged mode.

Usage Guideline Use this command to display global information of PIM.

Example The following example shows global information of PIM.

```
Switch#show ip pim

Register Suppression Time     : 100
Register Keepalive Time       : 185
C-RP Wildcard Prefix Count    : 1
SPT Threshold                    : 0

RP Address
  1.1.1.1, group-list: static-rp-acl

RP Candidate
  ip1, group-list: candidate-rp
  System, group-list: crp-system

SSM Group  : ssm-acl

Old Register Checksum to RP Address
----------------------------------
172.18.1.2
```

Field	Description
Register Keepalive Time	Value in seconds. To configure this value, use command **ip pim rp-register-kat**.
Register Suppression Time	Value in seconds. To configure this value, use command **ip pim register-suppression**.
SPT Threshold	Specify whether the switch forwarding in SPT, use command **ip pim spt-threshold** to change the value.
C-RP Wildcard Prefix Count	Specify the value to be set about Prefix Count value of the wildcard address (224.0.0.0/24) in PIM C-RP-Adv message. To modify the setting, use command **ip pim rp-candidate**

RP Address	Display the static RP information. To configure static RP, use command **ip pim rp-address**.
RP Candidate	Display the candidate RP information. To configure candidate RP, use command **ip pim rp-candidate**.
SSM Group	This field specifies the SSM ACL information. Use command **ip pim ssm** to configure this value.
Old Register Checksum	For the RP list, the register packets checksum will include data portion. To configure this value, use command **ip pim old-register-checksum**.

Routing Information Protocol (RIP) Commands

13-1 route-preference

Use this command to configure the route preference for the Routing Information Protocol (RIP) routes. Use the **no** form of this command to restore to the default value.

route-preference *VALUE*

no route-preference

Syntax Description	
VALUE	Route preference of RIP route.The value range is 1-999.

Default The default value of route preference of RIP route is 100.

Command Mode Router configuration mode and Router address family configuration mode.

Usage Guideline This command sets the route preference of the RIP routes. A route preference is a rating of the trustworthiness of a routing information source, such as an individual router or a group of routers. In general, the higher the value, the lower the trust rating is.

You can verify your settings by entering the **show ip route-preference** command.

Example To set the route preference of RIP routes to 120:

```
Switch# configure terminal
Switch(config)# router rip
Switch(config-router)# route-preference 120
```

To restore the route preference of RIP route to default value:

```
Switch# configure terminal
Switch(config)# router rip
Switch(config-router)# no route-preference
```

To set the route preference of RIP routes to 120 of RIP VRF VPN-A instance:

```
Switch# configure terminal
Switch(config)# router rip
Switch(config)# address-family ipv4 vrf VPN-A
Switch(config-router-af)# route-preference 120
```

13-2 distribute-list in (RIP)

Use this command to filter RIP routes inserted into the routing table. Use the **no** form of this command to remove the setting.

distribute-list *LIST_NAME* **in** *IPIF_NAME*

no distribute-list *LIST_NAME* **in** *IPIF_NAME*

Syntax Description	
LIST_NAME	The name of standard IP access list.
IPIF_NAME	Interface name on which the access list should be applied to incoming updates.

Default By default no distribute-list in is configured.

Command Mode Router configuration mode and Router address family configuration mode.

Usage Guideline This command must specify an access list name. According to access list rule, one route is determined to be or not to be inserted into routing table. It is independent to specify access list rule on each interface. The special access list will not effect the route to be inserted into routing table before it is created.

You can verify your settings by entering the **show ip rip interface** command.

Example To configure the System interface to use access list list1 to filter RIP route:

```
Switch# configure terminal
Switch(config)# ip standard access-list list1
Switch(config-ip-acl)# permit 172.18.0.0/16
Switch(config-ip-acl)# exit
Switch(config)# router rip
Switch(config-router)# distribute-list list1 in System
```

13-3 ip rip authentication mode

Use this command to configure the simple password authentication type used by RIP interface. Use the **no** form of this command to restore to the default value.

ip rip authentication mode text

no ip rip authentication mode

Syntax Description None.

Default By default no-authentication is used by RIP interface.

Command Mode Interface configuration mode.

Usage Guideline RIP Version 1 does not support authentication. To exchange RIP routing information directly, all devices must have the same IP authentication mode; otherwise, the RIP packets exchange will fail.

You can verify your settings by entering the **show ip rip** or **show ip rip interface** command.

Example Set System interface (vlan 1) to use simple password authentication:

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ip rip authentication mode text
```

13-4 ip rip authentication text-password

Use this command to configure the plaintext password for RIP simple password authentication. Use the **no** form of this command to remove the plaintext password.

ip rip authentication text-password *PASSWORD-STRING*

no ip rip authentication text-password

Syntax Description	
PASSWORD-STRING	The plaintext password that must be sent and received in the RIP packets on the RIP interface using simple password authentication. The string can contain from 1 to 16 uppercase and lowercase alphanumeric characters.

Default By default no plaintext password is configured.

Command Mode Interface configuration mode.

Usage Guideline The RIP Version 1 does not support RIP authentication.

To exchange RIP information directly, the password must be identify.

You can configure the plaintext password and text authentication mode individually. When enable the simple password authentication, the plaintext password should be used. If the plaintext password is not configured, the update packets should be sent and received without authentication.

You can verify your settings by entering the **show ip rip interface** command.

Example To configure System interface (vlan 1) to use simple password authentication and set the plaintext password to 1234:

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ip rip authentication mode text
Switch(config-if)# ip rip authentication text-password 1234
```

13-5 ip rip receive enable

Use this command to receive RIP packets on an RIP interface. Use the **no** form of this command to prohibit receiving RIP packets on the interface.

ip rip receive enable

no ip rip receive enable

Syntax Description None.

Default By default receiving RIP packets is enabled on each RIP interface.

Command Mode Interface configuration mode.

Usage Guideline Use the **no** form of this command to prevent from receiving RIP packets on the interface, the RIP protocol should not receive the packets coming from the interface.

On one interface whose sending packets is disabled or Version 1, disabling receiving packets will cause the configuration of authentication on this interface to be cleared and can't be restored when enable interface receiving packets again. The authentication needs to be reconfigured.

With the **no** form of this command, the configuration set by **ip rip receive version** command will be cleared. After enable interface receiving packets again, the receive version of the interface depends on global version setting with the **version** command.

You can verify your settings by entering the **show ip rip** or **show ip rip interface** command.

Example Configure the System interface (vlan 1) to not receive RIP packets:

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# no ip rip receive enable
```

13-6 ip rip receive version

Use this command to specify the version of RIP packet received on an RIP interface. Use the **no** form of this command to restore to the default value.

ip rip receive version [1 | 2](1)

no ip rip receive version

Syntax Description	
1	(Optional) Accepts RIP Version 1 packets on the interface.
2	(Optional) Accepts RIP Version 2 packets on the interface.

Default Depends on the configuration with the **version** command.

Command Mode Interface configuration mode.

Usage Guideline Use this command to override the default behavior of RIP as specified by the **version** command. If the interface receive version isn't specified, it should depend on the global version setting. This command applies only to the interface being configured. You can configure the interface to accept both RIP Version 1 and Version 2. When the send state is disabled or send version is Version 1, configure the receive version to Version 1 should cause the configuration of authentication cleared, because authentication only exists when the interface send or receive version is Version 2.

You can verify your settings by entering the **show ip rip** or **show ip rip interface** command.

Example Configure the System interface (vlan 1) to receive both RIP version 1 and version 2 packets:

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ip rip receive version 1 2
```

13-7 ip rip send enable

Use this command to send RIP packets on an RIP interface. Use the **no** form of this command to prohibit sending RIP packets on the interface.

ip rip send enable

no ip rip send enable

Syntax Description None.

Default By default send RIP packets is enabled on RIP interface.

Command Mode Interface configuration mode.

Usage Guideline Use the **no** form of this command to prevent from sending RIP packets on the interface, the RIP protocol should not send out RIP packets.

On one interface whose receiving packets is disabled or Version 1, disabling sending packets will cause the configuration of authentication on this interface to be cleared and can't be restored when enable interface sending packets again. The authentication needs to be reconfigured.

With the **no** form of this command, the configuration set by **ip rip send version** command will be cleared. After enable interface sending packets again, the send version of the interface depends on global version setting with the **version** command.

You can verify your settings by entering the **show ip rip** or **show ip rip interface** command.

Example Configure the System interface (vlan 1) to not send out RIP packets:

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# no ip rip send enable
```

13-8 ip rip send version

Use this command to specify the version of RIP packet sent on an RIP interface. Use the **no** form of this command to restore to the default value.

ip rip send version {1 | 2}

no ip rip send version

Syntax Description	
1	(Optional) Sends only RIP Version 1 packets out the interface.
2	(Optional) Sends only RIP Version 2 packets out the interface.

Default Depends on the configuration with the **version** command.

Command Mode Interface configuration mode.

Usage Guideline Use this command to override the default behavior of RIP as specified by the **version** command. If the interface send version isn't specified, it should depend on the global version setting. This command applies only to the interface being configured. When the receive state is disabled or receive version is Version 1, configure the send version to Version 1 should cause the configuration of authentication cleared, because authentication only exists when the interface send or receive version is Version 2.

You can verify your settings by entering the **show ip rip** or **show ip rip interface** command.

Example Configure the System interface (vlan 1) to only send RIP version 2 packets:

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ip rip send version 2
```

13-9 ip rip v2-broadcast

Use this command to send RIP version 2 update packets as broadcast instead of multicast. Use the **no** form of this command to restore to the default value.

ip rip v2-broadcast

no ip rip v2-broadcast

Syntax Description None.

Default By default this function is disabled.

Command Mode Interface configuration mode.

Usage Guideline Use this command to broadcast RIP version 2 updates to hosts that do not listen to multicast broadcast. Version 2 updates (requests and responses) will be sent to the IP broadcast address instead of the IP multicast address 224.0.0.9.

In order to reduce unnecessary load on those hosts that are not listening to RIP Version 2 broadcast, the system uses an IP multicast address for periodic broadcasts. The IP multicast address is 224.0.0.9.

When the interface send version is 2, use this command to enable v2-broadcast. If the send version is version 1, the command should not be effective. If restore the interface version to 2, the v2-broadcast setting should be cleared.

You can verify your settings by entering the **show ip rip interface** command.

Example To configure System (vlan 1) interface to send RIP version 2 packet with broadcast:

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ip rip send version 2
Switch(config-if)# ip rip v2-broadcast
```

13-10 network

Use this command to enable RIP on one interface. Use the **no** form of this command to restore to the default setting.

network *NETWORK-NUMBER*

no network *NETWORK-NUMBER*

Syntax Description	
NETWORK-NUMBER	IP address of the network of directly connected networks. The interface whose IP address belongs to the network can transmit and receive the RIP packets.

Default By default RIP is enabled on no interface.

Command Mode Router configuration mode and Router address family configuration mode.

Usage Guideline You can verify your settings by entering the **show ip rip** command.

Example To enable RIP on System interface (10.0.0.0/8):

```
Switch# configure terminal
Switch(config)# router rip
Switch(config-router)# network 10.0.0.0
```

To enable RIP on interface ip100 associated to VRF VPN-A(100.1.1.1/24):

```
Switch# configure terminal
Switch(config)# router rip
Switch(config)# address-faimly ipv4 vrf VPN-A
Switch(config-router-af)# network 100.1.1.0
```

13-11 redistribute (RIP)

Use this command to redistribute routes from one other routing domain into RIP domain. Use **no** form of the command to remove route redistribution settings to RIP.

redistribute {connected | static | bgp |ospf} [metric *VALUE*] **[route-map** *MAP_NAME*]

no redistribute {connected | static | bgp |ospf} [metric *VALUE*] **[route-map** *MAP_NAME*]

Syntax Description	
connected	(Optional) Specifies the connected routes are to be redistributed into RIP domain.
static	(Optional) Specifies the static routes are to be redistributed into RIP domain.
bgp	(Optional) Specifies the BGP routes are to be redistributed into RIP domain.
ospf	(Optional) Specifies the OSPF routes are to be redistributed into RIP domain.
metric *VALUE*	(Optional) Specifies the RIP route metric value for the redistributed routes. The value range is 0 to 16.
route-map *MAP_NAME*	(Optional) Route map that should be interrogated to filter the importation of routes from this source routing protocol to the RIP protocol. If not specified, all routes are redistributed.

Default

By default no route redistribution to RIP is configured.

The default value of metric is 0.

By default no route map is configured.

Command Mode

Router configuration mode

Usage Guideline

This command is used to add route redistribution from other routing protocols into RIP on the switch. Changing or disabling any keyword will not affect the state of other key-words. It is not necessary to convert the metric of one routing protocol into that of another routing protocol for route redistribution, since different routing protocols use different metric measurement methods. However, a symbolic metric suggest to be set for route redistribution.

You can filter the routes redistributed into RIP domain using the route map. If the specified route map is not defined, all routes should be redistributed. You can use the route-map math-clauses to filter the routes, and use the route-map set-clauses to set the metric of routes redistributed into RIP domain.

You can verify your settings by entering the **show ip rip** command.

Example

To configure the redistribution of static route to RIP:

```
Switch# configure terminal
Switch(config)# router rip
Switch(config-router)# redistribute static
```

To configure the redistribution of OSPF route to RIP and specify the metric to 2:

```
Switch# configure terminal
Switch(config)# router rip
Switch(config-router)# redistribute ospf metric 2
```

To configure the redistribution of OSPF route to RIP and use route map:

```
Switch# configure terminal
Switch(config)# route-map map1 permit 1
Switch(config-route-map)# match ip address list1
Switch(config-route-map)# set metric 4
Switch(config-route-map)# exit
Switch(config)# router rip
Switch(config-router)# redistribute ospf route-map map1
```

To configure the redistribution of static route to RIP VRF VPN-A instance:

```
Switch# configure terminal
Switch(config)# router rip
Switch(config)# address-family ipv4 vrf VPN-A
Switch(config-router-af)# redistribute static
```

13-12 router rip

Use this command to enable RIP and enter the RIP router configuration mode. Use the **no** form of this command to disable RIP.

router rip

no router rip

Syntax Description None.

Default By default RIP is disabled.

Command Mode Global configuration mode.

Usage Guideline This command is used to enable the RIP and enter the Router configuration mode of RIP protocol. The **no** form of this command will disable RIP function.

You can verify your settings by entering the **show ip rip** command.

Example To enable RIP and enter RIP router configuration mode:

```
Switch# configure terminal
Switch(config)# router rip
Switch(config-router)#
```

13-13 show ip rip

Use this command to show the RIP information.

show ip rip [vrf *VRF-NAME*]

Syntax Description	
vrf *VRF-NAME*	(Optional) Specifies to display information about the RIP VRF instance.

Default None.

Command Mode Privileged mode.

Usage Guideline This command is used to show the settings about RIP timers, status, redistribution, and interface RIP version, authentication, and status.

Example To check RIP information:

```
Switch#show ip rip

RIP Global State            : Enabled
Update Time                 : 30 seconds
Timeout Time                : 180 seconds
Garbage Collection Time     : 120 seconds

RIP Interface Settings

Interface     IP Address         TX Mode   RX Mode     Authen-    State
                                                       tication
------------ ------------       -------   --------    --------   -----
System        10.90.90.90/8      V1 Only   V1 or V2    Disabled   Disabled

Total Entries: 1

OSPF Redistribution Settings

Source    Destination   Type      Metric       RouteMapName
Protocol  Protocol
--------  ------------  ----      ------       ------------
STATIC     RIP          ALL       10

Total Entries: 1

Switch#
```

Field	Description
RIP Global state	The global status of RIP, the value is Disabled or Enabled.
Update Time	Rate (in seconds) at which update packets are set.
Timeout Time	Interval of time (in seconds) after which a route is declared invalid.
Garbage Collection Time	Amount of time (in seconds) that must pass before the route is removed from the garbage list.
Interface	The interface name.
IP Address	The interface ip address.
TX Mode	The version of sending RIP packets on the interface. The value is V1 Only, V2 Comp., V2 Only, or Disabled.
RX Mode	The version of receiving RIP packets on the interface. The value is V1 Only, V2 Only, V1 or V2, or Disabled.
Authentication	The authentication state. The value is Disabled or Enabled.
State	Status of RIP protocol on the interface. The value is Disabled or Enabled.
Source Protocol	The source route domain of redistribution.
Destination Protocols	The field always is RIP, namely the destination route domain of redistribution.
Type	The field always is ALL.
Metric	Metric of routes redistributed into RIP domain.
RouteMapName	Route map name used to filter routes redistributed into RIP domain

To check RIP information in VRF VPN-A:

```
Switch#show ip rip vrf VPN-A

VRF: VPN-A
RIP Global State            : Enabled
Update Time                 : 40 seconds
Timeout Time                : 120 seconds
Garbage Collection Time     : 120 seconds

RIP Interface Settings
Interface     IP Address      TX Mode    RX Mode       Authen-    State
                                                       tication
------------ --------------- ---------- ------------ ---------- -----
ip100         100.1.1.1/24    V1 Only    V1 or V2      Disabled   Disabled

Total Entries : 1

RIP Redistribution Settings
Source    Destination   Type      Metric       RouteMapName
Protocol  Protocol
--------  ------------  --------  ------------ ------------
OSPF      RIP           All       Transparency

Total Entries : 1

Switch#
```

13-14 show ip rip interface

This command is used to show information of all RIP interfaces.

show ip rip interface

Syntax Description None

Default None

Command Mode Privileged mode

Usage Guideline This command will display all interfaces specific information, such as: authentication, send version, receive version, and v2 broadcast mode, status.

Example To check settings of all RIP interfaces:

```
Switch#show ip rip interface

RIP Interface Settings

Interface Name: System                    IP Address: 80.1.1.5/16 (Link Up)
Interface Metric: 1                       Administrative State: Enabled
TX Mode: V2 Broadcast                     RX Mode: V1 or V2
Authentication: Disabled
Distribute List In: list1

Interface Name: n81                       IP Address: 81.1.1.5/16 (Link Down)
Interface Metric: 1                       Administrative State: Enabled
TX Mode: V1 Broadcast                     RX Mode: V1 or V2
Authentication: Enabled
Password for Authentication: 1234

Total Entries : 2

Switch#
```

Field	Description
Interface	The interface name.
IP Address	The interface ip address and the link state.
Interface Metric	The interface transmitted metric, the value always is 1.
Administrative State	Status of RIP protocol on the interface. The value is Disabled or Enabled.
TX Mode	The version of sending RIP packets on the interface. V1 Broadcast, V2 Multicast, V2 Broadcast or Disabled.

RX Mode	The version of receiving RIP packets on the interface. The value is V1 Only, V2 Only, V1 or V2, or Disabled.
Authentication	The authentication state. The value is Disabled or Enabled.
Password for Authentication	The value of password.
Distribute List In	Access list name used to distribute-list in.
Total Entries	The total value of interfaces.

To check settings of all RIP interfaces in VRF VPN-A:

```
Switch#show ip rip interface vrf VPN-A

RIP Interface Settings

Interface Name: ip100                    IP Address: 100.1.1.1/24 (Link Up)
Interface Metric: 1                      Administrative State: Disabled
TX Mode: V1 Broadcast                    RX Mode: V1 or V2
Authentication: Disabled

Total Entries : 1

Switch#
```

13-15 timers basic

To adjust Routing Information Protocol (RIP) network timers. To restore the default timers use the **no** form of this command.

timers basic *UPDATE TIMEOUT GARBAGE_COLLECTION*

no timers basic

Syntax Description	
UPDATE	Rate (in seconds) at which updates are sent. The default is 30 seconds. The value range is 5 to 65535.
TIMEOUT	Interval of time (in seconds) after which a route is declared invalid. A route becomes invalid when there is an absence of updates that refresh the route. The invalid route is put in the garbage list, marked as inaccessible, and advertised as unreachable. The default value is 180 seconds. The value range is 5 to 65535.
GARBAGE_COLLECTION	Amount of time (in seconds) that must pass before the route is removed from the garbage list. Before timeout, the entry is advertised as unreachable. The default is 120 seconds. The value range is 5 to 65535.

Default By default the update time is 30 seconds, the timeout time is 180 seconds and the garbage_collection time is120 seconds.

Command Mode Router configuration mode and Router address family configuration mode.

Usage Guideline The basic timers' parameters for RIP are adjustable. Although the RIP protocol don't require the router process RIP protocol with same basic timers, otherwise RIP is executing a distributed, asynchronous routing algorithm, these timers suggest to be the same for all routers and access servers in the network.

In the command, we don't check that if the update timer is bigger than timeout timer, the user should configure the update timer bigger than timeout timer to ensure RIP to work.

You can verify your settings by entering the **show ip rip** command.

Example To configure RIP update time to 20 seconds, timeout time to 180 seconds, and garbage_collection time to 100:

```
Switch#configure terminal
Switch(config)#router rip
Switch(config-router)#timers basic 20 180 100
```

To configure RIP update time to 40 seconds, timeout time to 120 seconds, and garbage collection time to 120 in VRF VPN-A:

```
Switch#configure terminal
Switch(config)#router rip
Switch(config)#address-family ipv4 vrf VPN-A
Switch(config-router-af)#timer basic 40 120 120
```

13-16 version

Use this command to specify Routing Information Protocol (RIP) version globally as the default version for all interfaces. Use the **no** form of this command to restore to the default value.

version {1 | 2}

no version

Syntax Description	
1	(Optional) Specifies RIP Version 1.
2	(Optional) Specifies RIP Version 2.

Default By default RIPv1 packets are sent out and both RIPv1 and RIPv2 packets are received.

Command Mode Router configuration mode and Router address family configuration mode.

Usage Guideline This command defines the default RIP version. This version will be override if version is explicitly specified for the interface (e.g. interface command **ip rip receive version**).

Please note when receiving and sending packets are all be disabled or both version is Version 1, the configuration of authentication will be cleared.

You can verify your settings by entering the **show ip rip** command.

Example To configure RIP global version to Version 2:

```
Switch#configure terminal
Switch(config)#router rip
Switch(config-router)#version 2
```

To configure RIP global version to Version 2 in VRF VPN-A:

```
Switch#configure terminal
Switch(config)#router rip
Switch(config)#address-family ipv4 vrf VPN-A
Switch(config-router-af)#version 2
```

13-17 address-family ipv4 vrf (RIP)

Use this command to create an RIP VRF instance and enter RIP VRF address family configuration mode. Use the no form of this command to destroy RIP VRF instance.

address-family ipv4 vrf *VRF-NAME*

no address-family ipv4 vrf *VRF-NAME*

Syntax Description	
vf *VRF-NAME*	Specifies the name of the VRF.

Default By default, no RIP VRF instance is created.

Command Mode Router configuration mode.

Usage Guideline This command is used to configure RIP routing instances that use IPv4 address prefixes. After executing this command, the address family configuration mode will be entered and a new RIP VRF routing instance will be created with this command. If the **no** form of this command is executed, the related configurations of the RIP VRF instance will be removed.

You can verify your settings by entering the **show ip rip vrf** command.

Example To create a new RIP instance in VRF VPN-A:

```
Switch# configure terminal
Switch(config)# router rip
Switch(config-router)# address-family ipv4 vrf VPN-A
Switch(config-router-af)#
```

13-18 exit address-family

Use this command to exit the address family configuration mode.

exit address-family

Syntax Description None

Default None

Command Mode Address family configuration mode.

Usage Guideline This command is used to exit address family configuration mode.

Example To exit address family configuration mode:

```
Switch# configure terminal
Switch(config)# router rip
Switch(config-router)# address-family ipv4 vrf VPN-A
Switch(config-router-af)#network 10.1.1.0
Switch(config-router-af)#exit address-family
Switch(config-router)#
```

Route Map Commands

14-1 route-map

Use this command to create or configure a route map or enter route map configuration mode. Use the **no** form of this command to delete a route map or remove a clause of route map.

route-map *MAP-NAME* **[permit | deny] [***SEQUENCE-NUM***]**

no route-map *MAP-NAME* **[permit | deny] [***SEQUENCE-NUM***]**

Syntax Description	
MAP-NAME	Specifies the name of route map. It can accept up to 16 characters. The syntax is general string that does not allow space.
permit	(Optional) Specifies a permit clause. If the match commands of one permit clause are met, the route will be redistributed while the set commands of this clause may modify the information of the route to be redistributed. If the match commands of one permit clause are not met, the next clause of this route map will be tested.
deny	(Optional) Specifies a deny clause. If the match commands of one deny clause are met, the route will not be redistributed.
SEQUENCE-NUM	(Optional) Specifies the sequence number of clause. Each clause has a sequence number, which indicates the position of the clause. The clause with lower sequence number is preferred. The range is 1 to 65535.

Default The permit keyword is the default.

The default value of the sequence number of the first clause is 10.

Command Mode Global configuration mode.

Usage Guideline The route map can be used in route redistribution and route filtering. A route map could be configured with multiple permit/deny clauses, which can have multiple match or set commands.

The clause with lower sequence number has higher priority. If the route map clause with low sequence number is not met, the next clause with higher sequence number will be tested. If all clauses are not met, the test result is to deny (This means the route map is ended with a implicit deny clause if this route map is not empty). If one clause is met, next clauses will be skipped.

When one clause is tested, the logical AND algorithm is applied for multiple match commands and the logical OR algorithm is applied for multiple objects within one match command.

There is a limitation about sequence number. If the route map has been configured with one clause, the sequence number must be specified when configure more clauses for this route map.

There is a maximum count about route map and it is project dependent.
The clauses of one route map also have a maximum count and it is also project dependent.

If no argument is specified when use **no route-map** command, the route map is deleted.

You can verify your settings by entering the **show route-map** command.

Examples To add one route map and enter the route map configuration mode:

```
Switch# configure terminal
Switch(config)# route-map rmap1 permit 10
Switch(config-route-map)#
```

14-2 match as-path

Use this command to add a match command to match a BGP autonomous system (AS) path access list. Use the **no** form of this command to delete the match command with BGP autonomous system path access list.

match as-path *ACCESS-LIST-NAME*

no match as-path

Syntax Description	
ACCESS-LIST-NAME	Specifies the name of the path access list. The length is up to 16 characters.

Default None

Command Mode Route map configuration mode.

Usage Guideline Only one path access list is supported. If this command is executed with a different path access list, the old one will be overwritten.

You can verify your settings by entering the **show route-map** command.

Examples To add a match clause to match AS path access list:

```
Switch# configure terminal
Switch(config)# route-map rmap1 permit 10
Switch(config-route-map)# match as-path PATH_AC
Switch(config-route-map)#
```

14-3 match community

Use this command to add a match command to match a Border Gateway Protocol (BGP) community list. Use the **no** form of this command to delete the match command with BGP community list.

match community *COMMUNITY-LIST-NAME* [**exact**]

no match community

Syntax Description	
COMMUNITY-LIST-NAME	Specifies the name of BGP community list. The length is up to 16 characters.
exact	(Optional) Specifies to match BGP community list exactly.

Default None.

Command Mode Route map configuration mode.

Usage Guideline The BGP community list is created with the command **ip community-list**.

If **exact** is specified, the communities in the community list must be exactly same as the communities of the route.

If **exact** is not specified, this command is matched as long as one community is matched.

Only one community list is supported. If this command is executed with a different community list, the old one will be overwritten.

You can verify your settings by entering the **show route-map** command.

Examples To add a match command to match a BGP community list:

```
Switch# configure terminal
Switch(config)# ip community-list standard DLINK-COMMUNITY permit 101:1
Switch(config)# route-map rmap1 permit 10
Switch(config-route-map)# match community DLINK-COMMUNITY exact
Switch(config-route-map)#
```

14-4 match extcommunity

Use this command to add a match command to match a Border Gateway Protocol (BGP) extended community (extcommunity) list. Use the **no** form of this command to delete the match command with BGP extended community list.

match extcommunity *EXTCOMMUNITY-LIST-NAME*

no match extcommunity

Syntax Description	
EXTCOMMUNITY-LIST-NAME	Specifies the name of the BGP extended community list. The length is up to 16 characters.

Default None.

Command Mode Route Map Configuration Mode.

Usage Guideline The BGP extended community list is created with the command **ip extcommunity-list**.

Only one community list is supported. If this command is executed with a different community list, the old one will be overwritten.

You can verify your settings by entering the **show route-map** command.

Examples To add a match command to match a BGP extended community list:

```
Switch# configure terminal
Switch(config)# ip extcommunity-list standard EXTCOM permit rt
192.168.1.1:100
Switch(config)# route-map rmap1 permit 10
Switch(config-route-map)# match extcommunity EXTCOM
Switch(config-route-map)#
```

14-5 match interface

Use this command to add a match command to match the outgoing interface of routes. Use the **no** form of this command to delete the match command with outgoing interface of routes.

match interface *IPIF_NAME*

no match interface

Syntax Description	
IPIF_NAME	Specifies the name of the outgoing interface of routes.

Default None.

Command Mode Route map configuration mode

Usage Guideline Only one interface is supported. If this command is executed with a different interface, the old one will be overwritten.

You can verify your settings by entering the **show route-map** command.

Examples To add a match command to match an outgoing interface of routes:

```
Switch# configure terminal
Switch(config)# route-map rmap1 permit 10
Switch(config-route-map)# match interface System
Switch(config-route-map)#
```

14-6 match ip address

Use this command to add a match command to match the destination network address of routes. Use the **no** form of this command to delete the match command with destination network address of routes.

match ip address {*ACCESS-LIST-NAME* **| prefix-list** *PREFIX-LIST-NAME*}

no match ip address {*ACCESS-LIST-NAME* **| prefix-list** *PREFIX-LIST-NAME*}

Syntax Description	
ACCESS-LIST-NAME	Specifies the name of a standard IP access list. The maximum length is 16 characters.
PREFIX-LIST-NAME	Specifies the name of an IP prefix list. The maximum length is 16 characters.

Default None

Command Mode Route map configuration mode

Usage Guideline The standard IP access list is created with the command **ip standard access-list**.

The prefix list is created with the command **ip prefix-list**.

Only one of them can be supported for matching destination network address at one time.

The destination network address is tested with the specified standard IP access list or prefix list.

You can verify your settings by entering the **show route-map** command.

Examples To add a match command to match destination network address of routes using standard IP access list:

```
Switch# configure terminal
Switch(config)# ip standard access-list Strict-Control
Switch(config-ip-acl)# permit 10.1.1.0/24
Switch(config-ip-acl)# exit
Switch(config)# route-map rmap1 permit 10
Switch(config-route-map)# match ip address Strict-Control
Switch(config-route-map)#
```

14-7 match ip next-hop

Use this command to add a match command to match the next hop of routes. Use the **no** form of this command to delete the match command with next hop of routes.

match ip next-hop {*ACCESS-LIST-NAME* **| prefix-list** *PREFIX-LIST-NAME*}

no match ip next-hop {*ACCESS-LIST-NAME* **| prefix-list** *PREFIX-LIST-NAME*}

Syntax Description	
ACCESS-LIST-NAME	Specify to match the next hop of the route according to the access list. The maximum length is 16 characters.
PREFIX-LIST-NAME	Specify to match the next hop of the route according to the prefix list. The maximum length is 16 characters.

Default None

Command Mode Route map configuration mode.

Usage Guideline The standard IP access list is created with the command **ip standard access-list**.

The prefix list is created with the command **ip prefix-list**.

Only one of them can be supported for matching the next hop of routes at one time.

The next hop of routes is tested with the specified standard IP access list or prefix list.

You can verify your settings by entering the **show route-map** command.

Examples To add a match command to match destination network address of routes using standard IP access list:

```
Switch# configure terminal
Switch(config)# ip standard access-list Strict-Control
Switch(config-ip-acl)# permit 10.1.1.0/24
Switch(config-ip-acl)# exit
Switch(config)# route-map rmap1 permit 10
Switch(config-route-map)# match ip next-hop Strict-Control
Switch(config-route-map)#
```

14-8 match ip route-source

Use this command to add a match command to match the source router IP address of the routes. Use the **no** form of this command to delete the match command with source router IP address.

match ip route-source *ACCESS-LIST-NAME*

no match ip route-source

Syntax Description	
ACCESS-LIST-NAME	Specifies the name of a standard IP access list. The maximum length is 16 characters.

Default None.

Command Mode Route map configuration mode.

Usage Guideline The standard IP access list is created with the command **ip standard access-list**.

Only one standard IP access list is supported. If this command is executed with a different standard IP access list, the old one will be overwritten.

You can verify your settings by entering the **show route-map** command.

Examples To add a match command to match source router IP address of routes using standard IP access list:

```
Switch# configure terminal
Switch(config)# ip standard access-list LocalServer
Switch(config-ip-acl)# permit 172.19.10.1/32
Switch(config-ip-acl)# exit
Switch(config)# route-map rmap1 permit 10
Switch(config-route-map)# match ip route-source LocalServer
Switch(config-route-map)#
```

14-9 match metric

Use this command to add a match command to match the metric of routes. Use the **no** form of this command to delete the match command with metric of routes.

match metric *NUMBER*

no match metric

Syntax Description	
NUMBER	Specifies the metric of routes.The range is 0 to 4294967294.

Default None.

Command Mode Route map configuration mode.

Usage Guideline You can verify your settings by entering the **show route-map** command.

Examples To add a match command to match the metric of routes:

```
Switch# configure terminal
Switch(config)# route-map rmap1 permit 10
Switch(config-route-map)# match metric 5
Switch(config-route-map)#
```

14-10 match route-type

Use this command to add a match command to match the type of routes. Use the **no** form of this command to delete the match command with type of routes.

match route-type {internal| external| type-1 | type-2}

no match route-type

Syntax Description	
internal	Intra-area and inter-area routes of Open Shortest Path First (OSPF).
external	Autonomous system external route of OSPF, including type-1 and type-2 external route.
type-1	Type-1 external route of OSPF.
type-2	Type-2 external route of OSPF.

Default None

Command Mode Route map configuration mode

Usage Guideline All types of routes, internal, external, type-1 and type-2, are only for OSPF.

You can verify your settings by entering the **show route-map** command.

Examples To add a match command to match the metric of routes:

```
Switch# configure terminal
Switch(config)# route-map rmap1 permit 10
Switch(config-route-map)# match route-type internal
Switch(config-route-map)#
```

14-11 set as-path prepend

Use this command to add a set command to modify an autonomous system path of BGP routes. Use the **no** form of this command to delete this set command.

set as-path prepend *ASPATH-LIST*

no set as-path prepend

Syntax Description	
ASPATH-LIST	Specifies the path list to be appended before the autonomous system path of the route. It could be an AS number or a list of AS numbers separated by comma.

Default None.

Command Mode Route map configuration mode.

Usage Guideline Use this command to change the length of the autonomous system path of BGP route. This can affect the best path selection.

You can verify your settings by entering the **show route-map** command.

Examples To add a set command to append an autonomous system path list to BGP routes:

```
Switch# configure terminal
Switch(config)# route-map mapaspath permit 10
Switch(config-route-map)# set as-path prepend 1,10,100,200
Switch(config-route-map)#
```

14-12 set community

Use this command to add a set command to modify the BGP communities attribute. Use the **no** form of this command to delete this set command.

set community [*COMMUNITY-SET* | **internet** | **local-as** | **no-advertise** | **no-export**](1) [**additive**]

no set community

Syntax Description	
COMMUNITY-SET	(Optional) A 32-bits integer number represented by AA:NN, where AA (AS number) is the upper part of the word and NN (community number, user-specified) is the lower part of the word
internet	(Optional) Specifies routes to be advertised to all peers (internal and external)
local-as	(Optional) Specifies routes not to be advertised to external BGP peers.
no-advertise	(Optional) Specifies routes not to be advertised to other BGP peers.
no-export	(Optional) Specifies routes not to be advertised outside of autonomous system boundary.
additive	(Optional) Specifies to add the community to the existed communities.

Default None

Command Mode Route map configuration mode.

Usage Guideline Use this command to modify the BGP community attribute.

If **additive** is not specified, the existing communities in the routes will be replaced.

You can verify your settings by entering the **show route-map** command.

Examples To add a set command to replace the BGP communities attribute:

```
Switch# configure terminal
Switch(config)# route-map mapdampending permit 10
Switch(config-route-map)# set community 2:1
Switch(config-route-map)#
```

14-13 set dampening

Use this command to add a set command specify the dampening parameters of routes. Use the **no** form of this command to delete this set command.

set dampening *HALF-LIFE REUSE SUPPRESS MAX-SUPPRESS-TIME UN-REACHABILITY-HALF-LIFE*

no set dampening

Syntax Description	
HALF-LIFE	Specifies the time (in minutes) after which the penalty of the reachable routes is decreased by half. The range is 1 to 45.
REUSE	If the penalty of a route is lower than this value, the route is unsuppressed.The range is 1 to 20000
SUPPRESS	If the penalty of a route is higher than this value, the route is suppressed.The range is 1 to 20000.
MAX-SUPPRESS-TIME	Specifies the maximum time (in minutes) a route can be suppressed. The range is 1 to 255.
UN-REACHABILITY-HALF-LIFE	Specifies the time (in minutes) after which the penalty of the unreachable routes is decreased by half. The range is 1 to 45.

Default

HALF-LIFE: 15 minutes.

REUSE: 750.

SUPPRESS: 2000.

MAX-SUPPRESS-TIME: 60 minutes

UN-REACHABILITY-HALF-LIFE: 15 minutes

Command Mode

Route map configuration mode

Usage Guideline

Use this command to modify the dampening parameters of routes when match conditions are met.

You can verify your settings by entering the **show route-map** command.

Examples To add a set command to modify the dampening parameters of route 120.1.1.0/24:

```
Switch# configure terminal
Switch(config)# ip standard access-list Strict-Control
Switch(config-ip-acl)# permit 120.1.1.0/24
Switch(config-ip-acl)# exit
Switch(config)# route-map rmap1 permit 10
Switch(config-route-map)# match ip address Strict-Control
Switch(config-route-map)# set dampening 14 500 900 60 15
Switch(config-route-map)#
```

14-14 set ip next-hop

Use this command to add a set command to modify the next hop of routes. Use the **no** form of this command to delete this set command.

set ip next-hop {*IP-ADDRESS* | **peer-address**}

no set ip next-hop

Syntax Description	
IP-ADDRESS	Specifies the IP address the next hop.
peer-address	This setting will take effect for both the ingress and egress directions. When set next hop to peer's address, for ingress direction, the next hop will be set to the neighbor peer address. For egress direction, the next hop associated with the route in the packet will be local router id.

Default None

Command Mode Route map configuration mode.

Usage Guideline Use this command to modify the next hop of route when match conditions are met.

You can verify your settings by entering the **show route-map** command.

Examples To add a set command to modify the next hop of route 10.1.1.0/24:

```
Switch# configure terminal
Switch(config)# ip standard access-list Strict-Control
Switch(config-ip-acl)# permit 10.1.1.0/24
Switch(config-ip-acl)# exit
Switch(config)# route-map mapnexthop permit 10
Switch(config-route-map)# match ip address Strict-Control
Switch(config-route-map)# set ip next-hop 120.1.2.2
Switch(config-route-map)#
```

14-15 set local-preference

Use this command to add a set command to modify the local preference attribute of routes. Use the **no** form of this command to delete this set command.

set local-preference *NUMBER*

no set local-preference

Syntax Description	
NUMBER	Specifies the value of local preference. The range is 0 to 4294967295.

Default The default value of local preference is 100.

Command Mode Route map configuration mode

Usage Guideline Use this command to modify the local preference attribute of route when match conditions are met.

By default, the BGP router will send the default local preference with the routes to IBGP neighbors and to EBGP neighbors which are in one confederation. It can be overwritten by the local preference set by the route map. For the received route, the local preference sent with the route will be used in the best path selection. This local preference will be overwritten if the local preference is ingress set by the route map.

For the connected routes, the default local preference will be used for them in the best path selection.

This will take effect for both ingress and egress directions.

You can verify your settings by entering the **show route-map** command.

Examples To add a set command to modify the local preference of route 120.1.1.0/24:

```
Switch# configure terminal
Switch(config)# ip standard access-list Strict-Control
Switch(config-ip-acl)# permit 120.1.1.0/24
Switch(config-ip-acl)# exit
Switch(config)# route-map mapprefer permit 10
Switch(config-route-map)# match ip address Strict-Control
Switch(config-route-map)# set local-preference 500
Switch(config-route-map)#
```

14-16 set metric

Use this command to add a set command to modify the metric of routes. Use the **no** form of this command to delete this command.

set metric *NUMBER*

no set metric

Syntax Description	
NUMBER	Specifies the metric of routes. The range is 0 to 4294967294.

Default None

Command Mode Route map configuration mode

Usage Guideline Use this command to modify the metric of routes to be redistributed.

You can verify your settings by entering the **show route-map** command.

Examples To add a set command to modify the metric of routes:

```
Switch# configure terminal
Switch(config)# route-map mapmetric permit 10
Switch(config-route-map)# set metric 100
Switch(config-route-map)#
```

14-17 set metric-type

Use this command to add a set command to modify the metric type of routes. Use the **no** form of this command to delete this set command.

set metric-type { **type-1** | **type-2**}

no set metric-type

Syntax Description	
type-1	OSPF external type 1 metric.
type-2	OSPF external type 2 metric.

Default None

Command Mode Route map configuration mode

Usage Guideline This command is only applied to the routes redistributed to OSPF.

You can verify your settings by entering the **show route-map** command.

Examples To add a set command to modify the metric type of routes:

```
Switch# configure terminal
Switch(config)# route-map mapmetrictype permit 10
Switch(config-route-map)# set metric-type type-1
Switch(config-route-map)#
```

14-18 set origin

Use this command to add a set command to modify the BGP origin code. Use the **no** form of this command to delete this set command.

set origin {**igp** | **egp** | **incomplete**}

no set origin

Syntax Description	
igp	Specifies that the origin code of the route will be set to IGP.
egp	Specifies that the origin code of the route will be set to EGP.
incomplete	Specifies that the origin code of the route will be set to INCOMPLETE.

Default None.

Command Mode Route map configuration mode

Usage Guideline Use this command to modify the BGP origin code route attribute.

The origin code (ORIGIN) is a well-known mandatory attribute that indicates the origin of the prefix or, rather, the way in which the prefix was injected into BGP.

There are three origin codes, listed in order of preference:

IGP, meaning the prefix was originated from information learned from an interior gateway protocol.

EGP, meaning the prefix originated from the EGP protocol, which BGP replaced.

INCOMPLETE, meaning the prefix originated from some unknown source, for example, redistribute.

You can verify your settings by entering the **show route-map** command.

Examples To add a set command to modify the origin code of routes:

```
Switch# configure terminal
Switch(config)# route-map maporigin permit 10
Switch(config-route-map)# match as-path PATH_ACL
Switch(config-route-map)# set origin egp
Switch(config-route-map)#
```

14-19 set weight

Use this command to add a set command to specify the weight of BGP routes Use the **no** form of this command to delete this set command.

set weight *NUMBER*

no set weight

Syntax Description	
NUMBER	Specifies the value of weight. The range is 0 to 65535.

Default None

Command Mode Route map configuration mode.

Usage Guideline Weights set by this command will override the weights specified by BGP neighbor commands. In other words, the weights specified with the command set weight in route map configuration mode override the weights specified with the command neighbor weight in BGP router mode.

You can verify your settings by entering the **show route-map** command.

Examples To add a set command to modify the weight of BGP routes:

```
Switch# configure terminal
Switch(config)# route-map mapweight permit 10
Switch(config-route-map)# match as-path PATH_ACL
Switch(config-route-map)# set weight 30
Switch(config-route-map)#
```

14-20 show route-map

Use this command to show route map settings.

show route-map [*MAP-NAME*]

Syntax Description	
MAP-NAME	(Optional) Specifies the name of a route map. The maximum length is 16 characters.

Default None

Command Mode Privileged mode

Usage Guideline Use this command to check the settings of route map, including permit or deny clauses and match or set commands.

Examples To show information of route map “maptest”:

```
Switch#show route-map maptest

   route-map :   maptest
--------------------------
      sequence : 10   (Permit)
            Match clauses:
                  route-source : acl1
                  ip next-hop : acl2
                  interface : System
                  metric : 30
                  route-type : external
            Set clauses:
                  dampening : 40 2000 2000 200 40
                  next-hop : 10.1.1.100
                  local-preference : 3000
                  metric-type : type-1
                  origin : igp
                  weight : 300
                  as-path : 20 30

Switch#
```

Virtual LAN (VLAN) Commands

15-1 vlan mapping profile

Use vlan mapping profile configuration command to enter VLAN mapping profile configuration mode. If the VLAN mapping profile doesn't exist, it will be created. Use no command to remove the VLAN mapping profile.

vlan mapping profile *ID* **[type [ethernet | ip | ipv6]]**

no vlan mapping profile *ID*

Syntax Description	
ID	Specify the ID of the VLAN mapping profile. Lower ID has higher priority. The ID range is 1-1000.
type	Specify the profile types. Different profile can match different fields. **ethernet**: the profile can match L2 fields **ip**: the profile can match L3 IP fields **ipv6**: the profile can match IPv6 destination or source address.

Default No VLAN mapping profile.

Command Mode Global configuration mode.

Usage Guideline A VLAN mapping profile can be used to provide flexible and powerful flow-based VLAN translation.

For creating a VLAN mapping profile, user must specify the type to decide which fields can be matched by the profile rules.

The follows table shows the type and the fields that can be matched.

Parameters	Fields
etnernet	Destination MAC address, source MAC address, 802.1p priority, inner VID, Ethernet type.
ip	IPv4 destination address, IPv4 source address, DSCP, TCP/UDP port number, IP protocol.
ethernet & ip	Destination MAC address, source MAC address, 802.1p priority, inner VID, Ethernet type, IPv4 destination address, IPv4 source address, DSCP, TCP/UDP port number, L3 protocol.
ipv6	IPv6 destination address or IPv6 source address.

Example This example shows how to create a VLAN mapping profile for matching Ethernet fields.

```
Switch(config)#vlan mapping profile 1 type ethernet
```

You can verify your settings by entering the **show vlan mapping profile** command.

15-2 vlan mapping rule

Use the rule command in VLAN mapping profile configuration mode to configure the VLAN mapping rules of the profile. Use the no rule command to remove the previous configured rules

rule {SN} match [src-mac *MAC-ADDRESS* **| dst-mac** *MAC-ADDRESS* **| priority** *COS-VALUE* **| inner-vid** *VLAN-ID* **| ether-type** *VALUE* **| src-ip** *NETWORK-PREFIX* **| dst-ip** *NETWORK-PREFIX* **| src-ipv6** *IPV6- NETWORK-PREFIX / PREFIX-LENGTH* **| dst-ipv6** *IPV6- NETWORK-PREFIX / PREFIX-LENGTH* **| dscp** *VALUE* **| src-port** *VALUE* **| dst-port** *VALUE* **| ip-protocol** *VALUE* **] { dot1q-tunnel | translate } outer-vid** *VLAN-ID* **[priority** *COS-VALUE* **] [inner-vid** *VLAN-ID***]**

no rule SN [ID]

Syntax Description	
SN	(Optional) Specifies the sequence number of the VFP rule. If no specified, the SN begins from 10 and the increment is 10. The SN range is 1-10000.
src-mac *MAC-ADDRESS*	Specifies the source MAC address.
dst-mac *MAC-ADDRESS*	Specifies the destination MAC address.
priority *COS-VALUE*	Specifies the 802.1p priority.
inner-vid *VLAN-ID*	Specifies the inner VLAN ID.
ether-type *VALUE*	Specifies the Ethernet type.
src-ip *NETWORK-PREFIX*	Specifies the source IPv4 address.
dst-ip *NETWORK-PREFIX*	Specifies the destination IPv4 address.
src-ipv6 *IPV6-NETWORK-PREFIX / PREFIX-LENGTH*	Specifies the source IPv6 address.
dst-ipv6 *IPV6-NETWORK-PREFIX / PREFIX-LENGTH*	Specifies the destination IPv6 address.
dscp *VALUE*	Specifies the DSCP value.
src-port *VALUE*	Specifies the source TCP/UDP port number.
dst-port *VALUE*	Specifies the destination TCP/UDP port number.
ip-protocol *VALUE*	Specifies the L3 protocol value.
action	Specifies the follows parameters are the action for matched packets.
dot1q-tunnel	Specifies the follows outer-vid will be added for matched packets.
translate	Specifies the follows outer-vid will replace the outer-vid of the matched packets.
outer-vid *VLAN-ID*	Specifies the new outer VLAN ID
priority *COS-VALUE*	(Optional) Specifies the 802.1p priority in the new outer TAG
inner-vid *VLAN-ID*	(Optional) Specifies the new inner VLAN ID

Default No VLAN mapping rule

Command Mode VLAN mapping profile configuration mode

Usage Guideline The rule command is used to configure the VLAN mapping rules of the profile. If a profile is applied on an interface, the switch tests the incoming packets according the rules of the profile. If the packets match a rule, the action of the rule will be taken. The action may be adding or replacing the outer-VID. Optional, you can specify the priority of the new outer-TAG or specify the packets new inner-VID. If no specified, the priority of the new outer-TAG is the incoming port default priority and the inner-VID will not be modified.

The test order depends on the rule's sequence number of the profile and stopped when first matched. If no specifies the sequence number, it will be allocated automatically. The sequence number begins from 10 and the increment is 10. Multiple different types of profiles could be configured onto one interface.

The maximum rule number in a profile is 128.

Example This example shows how to configure rules for VLAN mapping profile 10.

```
Switch(config)#vlan mapping profile 10
Switch(config-vlan-map)# rule 10 match src-ip 100.1.1.0/24 dot1q-tunnel
outer-vid 100
Switch(config-vlan-map)# rule 20 match dst-ip 200.1.1.0/24 dot1q-tunnel
outer-vid 200
Switch(config-vlan-map)#exit
```

This example shows how to remove previous configured VLAN mapping rules.

```
Switch(config)#vlan mapping profile 10
Switch(config-vlan-map)# no rule 10
Switch(config-vlan-map)# no rule 20
Switch(config-vlan-map)#exit
```

You can verify your settings by entering the **show vlan mapping profile** command.

15-3 show vlan mapping profile

Use show vlan mapping profile command to show previous configured VLAN mapping profile information

show vlan mapping profile [*ID* **]**

Syntax Description	
ID	(Optional) Specifies the ID of the VLAN mapping profile. If nothing specified, shows all configured VLAN mapping profile.

Default N/A

Command Mode EXEC mode

Usage Guideline Use the **show vlan mapping profile** command to show previous configured VLAN mapping profile information.

Example This example shows all VLAN mapping profile information.:

```
Switch# show vlan mapping profile
VLAN mapping profile:1  type:ip
rule 10 match src-ip 100.1.1.0/24, dot1q-tunnel outer-vid 100
rule 20 match dst-ip 200.1.1.0/24, dot1q-tunnel outer-vid 200
Total Entries: 2
VLAN mapping profile:2 type:ethernet
rule 10 match src-mac 00-00-00-00-00-01, translate outer-vid 40
Total Entries: 1
```

15-4 switchport vlan mapping profile

Use switchport vlan mapping profile command to apply the VLAN mapping rules of profile to specified interface. Use no switchport vlan-mapping profile command to remove the application.

switchport vlan mapping profile *ID*

no switchport vlan mapping profile *ID*

Syntax Description	
ID	Specifies the VLAN mapping profile ID

Default None

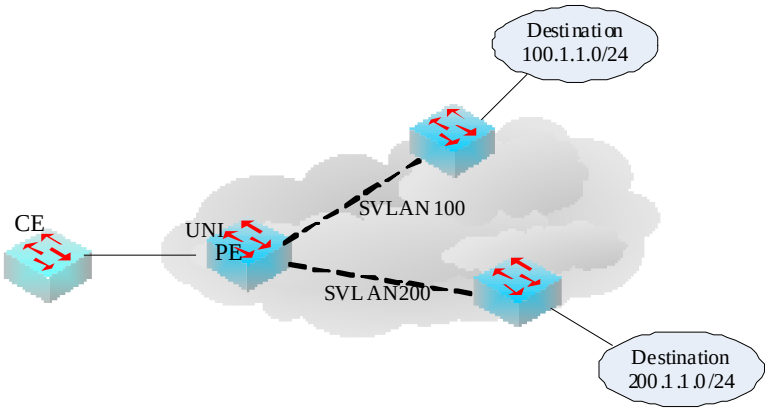
Command Mode Interface configuration mode

Usage Guideline Use switchport vlan mapping profile command to apply the VLAN mapping profile to specified interface. The interface can be a physical port or a link aggregation group which is set to the UNI role.

If a profile is applied on an interface, the switch tests the incoming packets according the rules of the profile. If the packets match a rule, the action of the rule will be taken. And the switch stops the testing of the profile.

Setting the port mode to the NNI role will lead to its VLAN mapping profile configuration is cleaned.

Example The follows example shows how to configure a VLAN mapping profile and apply it to UNI port 1.



The customer packets that go to 100.1.1.0/24 will be added S-VLAN 100 and the packets that go to 200.1.1.0/24 will be added S-VLAN 200.

```
Switch(config)# vlan mapping profile 1 type ip
Switch(config-vlan-map)# rule 10 match dst-ip 100.1.1.0/24 dot1q-tunnel
outer-vid 100
Switch(config-vlan-map)# rule 20 match dst-ip 200.1.1.0/24 dot1q-tunnel
outer-vid 200
Switch(config-vlan-map)#exit
Switch(config)# interface Gigabitethernet 1
Switch(config-if)#switchport vlan mapping profile 1
Switch(config-if)#exit
```

You can verify your settings by entering the **show qinq ports** command.

Virtual Private Wire Service (VPWS) Commands

16-1 xconnect

Use the **xconnect** command to enable the VPWS service on the interface. Use the **no** form of this command to cancel the VPWS service.

xconnect *VC-ID IP-ADDRESS* **encapsulation mpls [{raw| tagged}] [mtu 0-65535]**

no xconnect

Syntax Description	
VC-ID	Specifies the PW (pseudo-wire) service instance ID. It is used to uniquely identify the VPWS (Virtual Private Wire Service) and it must be unique at both PEs (Provider Edge). The range is 1-4294967295.
IP-ADDRESS	Specifies the peer LSR ID that is used to identify the other end PE.
raw	(Optional) Specifies the PW type is Ethernet-raw mode. For this type, the s-tag is never sent over the PW.
tagged	Specifies the PW type is Ethernet-tag mode. For this type, the s-tag shall be sent over the PW. By default, the PW type is Ethernet-tag mode.
mtu	(Optional) Specifies the local CE-PE link MTU that will be advertised to remote peer. If specifies the MTU to 0, the LDP will not advertise the local MTU. The MTU must be the same at both local and remote, otherwise the PW will not setup. If no MTU is specified, the default value of 1500 will be used. Note: you must ensure the specified MTU is same as the real MTU of the CE-PE link.

Default No VPWS on interface.

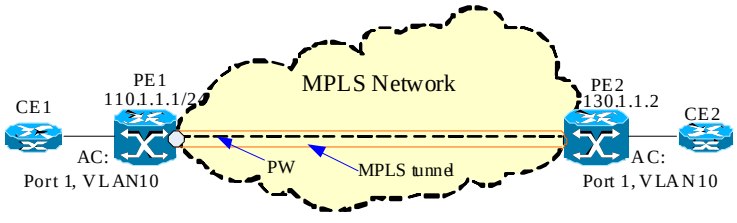
Command Mode Interface configuration mode.

Usage Guideline This command can be used to create a port-based or port VLAN-based VPWS service.

If creating the VPWS on a physical port, the service is a port-based and this Ethernet port is the AC. If creating the VPWS on a VLAN sub-interface of a port interface, the service is the port VLAN-based and this VLAN sub-interface of the port interface is the AC.

The interface that is specified used as AC cannot be Layer 3 interface.

Example The follows example shows how to configure a VPWS:



The AC from CE (Customer Edge Bridge) to PE is the VLAN 10 of port 1. Assume the MPLS interfaces of PEs are VLAN 20 and the VC-ID is 2. For

making the VLAN 10 packets from CE one can be transmitted to the other end through the MPLS network, user shall configure PE1 and PE2 as follows:

Configuring PE 1:

```
Switch(config)#interface vlan 20
Switch(config-if)#mpls ip
Switch(config-if)#mpls label protocol ldp
Switch(config-if)#exit
Switch(config)#mpls ip
Switch(config)#mpls label protocol ldp
Switch(config-mpls-router)#ldp router-id 110.1.1.1
Switch(config-mpls-router)#exit
Switch(config)#interface GigabitEthernet 1
Switch(config-if)#encapsulation dot1q 10
Switch(config-subif)#xconnect 2 130.1.1.2 encapsulation mpls
```

Configuring PE 2:

```
Switch(config)#interface vlan 20
Switch(config-if)#mpls ip
Switch(config-if)#mpls label protocol ldp
Switch(config-if)#exit
Switch(config)#mpls ip
Switch(config)#mpls label protocol ldp
Switch(config-mpls-router)#ldp router-id 130.1.1.2
Switch(config-mpls-router)#exit
Switch(config)#interface GigabitEthernet 1
Switch(config-if)#encapsulation dot1q 10
Switch(config-subif)#xconnect 2 110.1.1.1 encapsulation mpls
```

16-2 xconnect backup

Use the **xconnect backup** command to enable the PW redundancy of VPWS service on the interface. Use the **no xconnect backup** command to cancel the PW redundancy of VPWS service.

xconnect backup *VC-ID IP-ADDRESS*

no xconnect backup

Syntax Description	
VC-ID	Specifies the PW (pseudo-wire) service instance ID. It is used to uniquely identify the VPWS (Virtual Private Wire Service) and it must be unique at both PEs (Provider Edge). The range is 1-4294967295.
IP-ADDRESS	Specifies the peer LSR ID that is used to identify the other end PE.

Default

No PW redundancy of VPWS on interface.

Command Mode

Interface configuration mode.

Usage Guideline

This command can be used to enable PW redundancy of a VPWS service. It will create a backup pseudowire service. Before this command is executed, VPWS service i.e. primary pseudowire must be existed. The backup pseudowire will have same PW type and MTU with primary pseudowire.

There should be one primary pseudowire and one backup pseudowire set up for PW redundancy of VPWS service. In a normal situation, the primary pseudowire is link up and the backup pseudowire is link standby. The packet forwarding in the VPWS service will work in the primary pseudowire. But when LDP hello procedure or other situations found primary pseudowire link down happens, backup pseudowire will be changed to link up to take packet forwarding in the VPWS service. After primary pseudowire is recovered to link up again, backup pseudowire will be back to link standby, and the packet forwarding in the VPWS service will be back to primary pseudowire again.

Example

The follows example shows how to configure PW redundancy for a VPWS, which will add a backup PW to another PE.

Configuring PE:

```
Switch(config)#interface vlan 20
Switch(config-if)#mpls ip
Switch(config-if)#mpls label protocol ldp
Switch(config-if)#exit
Switch(config)#mpls ip
Switch(config)#mpls label protocol ldp
Switch(config-mpls-router)#ldp router-id 110.1.1.1
Switch(config-mpls-router)#exit
Switch(config)#interface GigabitEthernet 1
Switch(config-if)#encapsulation dot1q 10
Switch(config-subif)#xconnect 2 130.1.1.2 encapsulation mpls
Switch(config-subif)#xconnect backup 2 120.1.1.2
```

16-3 show mpls l2transport vc

Use this command to display the VPWS VC information.

show mpls l2transport vc [*VC-ID*] [detail]

Syntax Description	
VC-ID	Show the specified PW ID only.
detail	Show the detailed PW information.

Default N/A

Command Mode EXEC mode

Usage Guideline None

Example Show information of all VC:

```
Switch# show mpls l2transport vc
VC ID      Peer            Local AC              Type    Oper Status
 ---------- -------------- -------------------- ------  -----------
 1          150.1.1.4      Eth1/VLAN2          Raw     Up
 2          130.1.1.2      Eth1/VLAN3          Tagged  Down

Total Entries: 2
```

Show detailed information of VC 1:

```
Switch# show mpls l2transport vc 1 detail
 VC ID: 1, Peer IP Address: 150.1.1.4, Operate Status: Up
   Local AC: Eth1/VLAN2, Status: Up
   Remote AC Status: Up
   MPLS VC Labels: Local 16, Remote 16
   Outbound Tunnel label: 100
   MTU: Local 1500, Remote 1500
   Group ID: Local 0, Remote 0
   Signaling Protocol: LDP
   VC Statistics:
     RX Bytes: 0, RX Packets: 0
     TX Bytes: 0, TX Packets: 0

 Total Entries: 1
```

Show detailed information of VC 3 belonged to PW redundancy:

```
Switch# show mpls l2transport vc 3 detail
VC ID: 3, Peer IP Address: 140.1.1.2, Operate Status: Up, Primary
  Local AC: Eth1/VLAN4, Status: Up
  Remote AC Status: Up
  MPLS VC Labels: Local 17, Remote 17
  Outbound Tunnel label: 101
  MTU: Local 1500, Remote 1500
  Group ID: Local 0, Remote 0
  Signaling Protocol: LDP
  VC Statistics:
    RX Bytes: 0, RX Packets: 0
    TX Bytes: 0, TX Packets: 0

VC ID: 3, Peer IP Address: 160.1.1.2, Operate Status: Up, Backup
  Local AC: Eth1/VLAN4, Status: Standby
  Remote AC Status: Up
  MPLS VC Labels: Local 18, Remote 18
  Outbound Tunnel label: 102
  MTU: Local 1500, Remote 1500
  Group ID: Local 0, Remote 0
  Signaling Protocol: LDP
  VC Statistics:
    RX Bytes: 0, RX Packets: 0
    TX Bytes: 0, TX Packets: 0

 Total Entries: 2
```

Virtual Private LAN Service (VPLS) Commands

17-1 vpls

Use the **vpls** command in global configuration mode to create a VPLS and enter VPLS configuration mode. Use the **no vpls** command in global configuration mode to delete a VPLS.

vpls *VPLS-NAME*

no vpls *VPLS-NAME*

Syntax Description	
VPLS-NAME	Specifies VPLS name. The name range is 1 – 32 characters.

Default No VPLS.

Command Mode Global configuration mode.

Usage Guideline This command is used to create a VPLS and enter VPLS configuration mode. If that VPLS has been existed, directly enter VPLS configuration mode. VPLS name is used to locally identify a unique VPLS in a device.

Example The following example shows how to create a VPLS named “vpls100” and enter VPLS configuration mode:

```
switch(config)#vpls vpls100
switch(config-vpls)#
```

The following example shows how to delete a VPLS named “vpls100”:

```
switch(config)#no vpls vpls100
switch(config)#
```

17-2 vpls-id

Use the **vpls-id** command in VPLS configuration mode to set VPLS ID of a VPLS.

vpls-id *VPLS-ID*

Syntax Description	
VPLS-ID	Specifies VPLS ID of a VPLS. The value range is 1-4294967295. VPLS ID is used as VC ID of the pseudowires in the VPLS, which do not have specified VC ID.

Default VPLS ID is zero.

Command Mode VPLS configuration mode.

Usage Guideline This command is used to set VPLS ID of a VPLS in VPLS configuration mode. Each VPLS in a device should have a local unique VPLS ID.

Example The following example shows how to set the VPLS ID of a VPLS to 100.

```
switch(config-vpls)#vpls-id 100
switch(config-vpls)#
```

17-3 service-type

Use the **service-type** command in VPLS configuration mode to set the type of emulated service in a VPLS.

service-type {raw | tagged}

Syntax Description	
raw	Specifies the service type is Ethernet-raw mode in a VPLS. It means the encapsulation of all pseudowires in the VPLS is Ethernet-raw mode.
tagged	Specifies the service type is Ethernet-tagged mode in a VPLS. It means the encapsulation of all pseudowires in the VPLS is Ethernet-tagged mode.

Default Ethernet-tagged mode.

Command Mode VPLS configuration mode.

Usage Guideline This command is used to set the type of emulated service in a VPLS in VPLS configuration mode. All pseduowires of a VPLS should have same encapsulation as the type of emulated service in the VPLS. The service type of a VPLS can be modified only when there is no pseudowire existed in this VPLS.

Example The following example shows how to set the service type of a VPLS to Ethernet-raw mode.

```
switch(config-vpls)#service-type raw
switch(config-vpls)#
```

17-4 mtu

Use the **mtu** command in VPLS configuration mode to set the local AC link MTU of a VPLS.

mtu <*VALUE 0-65535***>**

Syntax Description	
<VALUE 0-65535>	Specifies local AC link MTU of a VPLS that will be advertised to remote peers in this VPLS. MTU must be same at both local and remote. Otherwise, the related pseudowires will not be setup with remote peers. If a user specifies MTU to 0, local MTU will not be advertised to remote peers in the VPLS. **Note:** a user must ensure the specified MTU is same as the real MTU of local AC link.

Default 1500

Command Mode VPLS configuration mode

Usage Guideline This command is used to set local AC link MTU of a VPLS in VPLS configuration mode. Local AC link MTU of a VPLS can be modified only when there is no pseudowire existed in this VPLS.

Example The follow example shows how to set local AC link MTU of a VPLS to 1000:

```
switch(config-vpls)#mtu 1000
switch(config-vpls)#
```

17-5 mac-limit

Use the **mac-limit** command in VPLS configuration mode to set MAC address learning limitation of a VPLS.

mac-limit *VALUE*

Syntax Description	
VALUE	Specifies the limited number of learned MAC addresses in a VPLS. The maximum value of limited number of learned MAC addresses is project dependent setting. If a user specifies 0, there is no MAC address learning limitation in this VPLS. For the DGS-3620, the maximum number is 32767.

Default 0.

Command Mode VPLS configuration mode.

Usage Guideline This command is used to set MAC address learning limitation of a VPLS in VPLS configuration mode. After a user set a non-zero MAC address learning limitation, when the situation of over MAC address learning limitation happens, the packets with unlearned source MAC address in the VPLS will be dropped.

Example The follow example shows how to set MAC address learning limitation of a VPLS to 4096.

```
switch(config-vpls)#mac-limit 4096
switch(config-vpls)#
```

17-6 peer

Use the **peer** command in VPLS configuration mode to create a peer i.e. a pseudowire in a VPLS. Use the **no peer** command in VPLS configuration mode to delete a peer in a VPLS.

peer *IP-ADDRESS* **[***VC-ID***] [{network | spoke}]**

no peer *IP-ADDRESS* **[***VC-ID***]**

Syntax Description	
IP-ADDRESS	Specifies the LSR ID that is used to identify the PE which the peer belongs to.
VC-ID	Optional, specifies the pseudowire id. The range is 1-4294967295. It is used with IP-ADDRESS to uniquely identify a peer i.e. a pseudowire for a VPLS. If no specifies, the pseudowire id is set by VPLS ID of this VPLS.
network	Specifies a peer is used as a network pseudowire. The packets from other network pseudowires in a VPLS must not be forwarded to this pseudowire, and the packets from this pseudowire must not be forwarded to other network pseudowires in the VPLS. It is the "split horizon" rule.
spoke	Specifies a peer is used as a spoke pseudowire (in H-VPLS topology). The packets from other pseudowires in a VPLS can be forwarded to this pseudowire, and the packets from this pseudowire can be forwarded to other pseudowires in the VPLS.

Default VC-ID is set by VPLS ID of this VPLS, and it is a network pseudowire.

Command Mode VPLS configuration mode.

Usage Guideline This command is used to create a peer i.e. a pseudowire in a VPLS in VPLS configuration mode. The no peer command is used to delete a peer or a backup peer in a VPLS in VPLS configuration mode.

Example The following example shows how to create a peer i.e. a pseudowire, for which the IP ADDRESS is 2.2.2.2, and VC ID is set by VPLS ID, it is a network pseudowire.

```
switch(config-vpls)#peer 2.2.2.2
switch(config-vpls)#
```

The following example shows how to create a peer, for which the IP ADDRESS is 2.2.2.2, and VC ID is 100, it is a spoke pseudowire in H-VPLS topology.

```
switch(config-vpls)#peer 2.2.2.2 100 spoke
switch(config-vpls)#
```

The following example shows how to delete a peer of a VPLS, for which the IP ADDRESS is 2.2.2.2, and VC ID is 100

```
switch(config-vpls)#no peer 2.2.2.2 100
switch(config-vpls)#
```

The follow example shows how to delete all peers of a VPLS, for which the IP ADDRESS is 2.2.2.2

```
switch(config-vpls)#no peer 2.2.2.2
switch(config-vpls)#
```

17-7 peer backup

Use the **peer backup** command in VPLS configuration mode to create a backup peer i.e. a backup pseudowire for PW redundancy of H-VPLS.

peer backup *IP-ADDRESS* **[***VC-ID***]**

Syntax Description	
IP-ADDRESS	Specifies the LSR ID that is used to identify the PE which the peer belongs to.
VC-ID	Optional, specifies the pseudowire id. The range is 1-4294967295. It is used with IP-ADDRESS to uniquely identify a peer i.e. a pseudowire for a VPLS. If no specifies, the pseudowire id is set by VPLS ID of this VPLS.

Default VC-ID is set by VPLS ID of this VPLS.

Command Mode VPLS configuration mode.

Usage Guideline This command is used to create a backup peer i.e. a backup pseudowire for PW redundancy of H-VPLS in VPLS configuration mode. For PW redundancy of H-VPLS, the device will act as MTU-s, and there should be one primary pseudowire and one backup pseudowire set up.

In a normal situation, the primary pseudowire is link up and the backup pseudowire is link standby. The packet forwarding between MTU-s and PE will work in the primary pseudowire, but when LDP hello procedure or other situations find primary pseudowire link down occurs, backup pseudowire will be changed to link up to take packet forwarding between MTU-s and PE. After primary pseudowire is recovered to link up again, backup pseudowire will be back to link standby, and the packet forwarding between MTU-s and PE will be back to primary pseudowire again.

When backup pseudowire is changed from link standby to link up, MAC withdraw message with NULL-MAC list will be sent from MTU-s to PE via backup pseudowire to clear old MAC addresses. When primary pseduoware is recovered to link up and backup pseudowire is changed from link up to link standby, MAC withdraw message with NULL-MAC list will be sent from MTU-s to PE via primary pseudowire to clear old MAC addresses.

Example The following example shows how to create a backup peer i.e. a pseudowire, which IP ADDRESS is 2.2.2.2, and VC ID is set by VPLS ID.

```
switch(config-vpls)#peer backup 2.2.2.2
switch(config-vpls)#
```

The following example shows how to create a backup peer, which IP ADDRESS is 2.2.2.2, and VC ID is 100.

```
switch(config-vpls)#peer backup 2.2.2.2 100
switch(config-vpls)#
```

17-8 xconnect vpls

Use the **xconnect vpls** command in interface configuration mode to create a local AC in a VPLS. Use the **no xconnect vpls** command in interface configuration mode to delete a local AC in a VPLS.

xconnect vpls *VPLS-NAME*

no xconnect vpls *VPLS-NAME*

Syntax Description	
VPLS-NAME	Specifies VPLS name. The name range is 1 – 32 characters.

Default N/A

Command Mode Interface configuration mode (Ethernet interface or Ethernet VLAN interface)

Usage Guideline This command is used to create a local AC in a VPLS in interface configuration mode.

A local AC could be an Ethernet-based AC which is created in Ethernet interface or an Ethernet VLAN-based AC which is created in Ethernet VLAN interface. All local ACs in a VPLS should have same AC type.

Example The following example shows how to create a local AC, which is Ethernet-based AC and Ethernet port is 1, into a VPLS which name is “vpls100”.

```
switch(config)#interface GigabitEthernet 1
switch(config-if)#xconnect vpls vpls100
switch(config-if)#
```

The following example shows how to create a local AC, which is Ethernet VLAN-based AC and Ethernet port is 1 and VLAN is 100, into a VPLS which name is “vpls100”.

```
switch(config)#interface GigabitEthernet 1
switch(config)#encapsulation dot1q 100
switch(config-subif)#xconnect vpls vpls100
switch(config-subif)#
```

The following example shows how to delete a local AC, which is Ethernet-based AC and Ethernet port is 1, from a VPLS which name is “vpls100”.

```
switch(config)#interface GigabitEthernet 1
switch(config-if)#no xconnect vpls vpls100
switch(config-if)#
```

The following example shows how to delete a local AC, which is Ethernet VLAN-based AC and Ethernet port is 1 and VLAN is 100, from a VPLS which name is “vpls100”.

```
switch(config)#interface GigabitEthernet 1
switch(config)#encapsulation dot1q 100
switch(config-subif)#no xconnect vpls vpls100
switch(config-subif)#
```

17-9 show vpls

Use the **show vpls** command in EXEC mode to show VPLS information.

show vpls [*VPLS-NAME***] [detail]**

Syntax Description	
VPLS-NAME	Optional, specifies VPLS name. The name range is 1 – 32 characters.
detail	Optional, specifies detail VPLS information.

Default N/A

Command Mode EXEC mode

Usage Guideline This command is used to show VPLS (detail) information.

Example The following example shows how to show all VPLS information.

```
switch#show vpls

VPLS Name                        VPLS ID     Peers/ACs  Oper Status
 -------------------------------  ----------  ---------  -----------
 vpls100                         100         3/1        Up
 vpls101                         101         3/1        Up
 vpls102                         102         3/1        Up
 vpls103                         103         3/1        Up
 vpls104                         104         3/1        Up
 vpls105                         105         3/1        Up
 vpls106                         106         3/1        Up
 vpls107                         107         3/1        Down

Total Entries: 8

switch#
```

The following example shows how to show VPLS information for a VPLS.

```
switch#show vpls vpls100

VPLS Name                        VPLS ID     Peers/ACs  Oper Status
 -------------------------------  ----------  ---------  -----------
 vpls100                         100         3/1        Up

Total Entries: 1

switch#
```

The following example shows how to show all VPLS detail information.

```
switch#show vpls detail

VPLS Name: vpls100, Operate Status: Up
     VPLS ID: 100, Service Type: Tagged, MTU: 1500, MAC Limit: 0
     Peers via Pseudowires:
       VC ID       Peer             Type     Oper Status
       ----------  ---------------  -------  -----------
       100         3.3.3.3          Network  Down
       100         1.1.1.1          Network  Up
       100         5.5.5.5          Spoke    Down
     Local ACs:
       Local AC           Oper Status
       -----------------  -----------
       Eth17/VLAN100      Up

 VPLS Name: vpls101, Operate Status: Up
     VPLS ID: 101, Service Type: Tagged, MTU: 1500, MAC Limit: 0
     Peers via Pseudowires:
       VC ID       Peer             Type     Oper Status
       ----------  ---------------  -------  -----------
       101         3.3.3.3          Network  Down
       101         1.1.1.1          Network  Up
       101         5.5.5.5          Spoke    Down
     Local ACs:
       Local AC           Oper Status
       -----------------  -----------
       Eth17/VLAN101      Up

Total Entries: 2

switch#
```

The following example shows how to show VPLS detail information for a VPLS.

```
switch#show vpls vpls100 detail

VPLS Name: vpls100, Operate Status: Up
     VPLS ID: 100, Service Type: Tagged, MTU: 1500, MAC Limit: 0
     Peers via Pseudowires:
       VC ID       Peer             Type     Oper Status
       ----------  ---------------  -------  -----------
       100         3.3.3.3          Network  Down
       100         1.1.1.1          Network  Up
       100         5.5.5.5          Spoke    Down
     Local ACs:
       Local AC           Oper Status
       -----------------  -----------
       Eth17/VLAN100      Up

Total Entries: 1

switch#
```

The following example shows how to show VPLS detail information for a VPLS with PW redundancy.

```
switch#show vpls vpls102 detail

VPLS Name: vpls102, Operate Status: Up
     VPLS ID: 102, Service Type: Tagged, MTU: 1500, MAC Limit: 0
     Peers via Pseudowires:
       VC ID       Peer             Type     Oper Status
       ----------  ---------------  -------  -----------
       100         1.1.1.1          Primary  Up
       100         2.2.2.2          Backup   Standby
     Local ACs:
       Local AC           Oper Status
       -----------------  -----------
       Eth17/VLAN102      Up

Total Entries: 1

switch#
```

17-10 show mac-address-table vpls

Use the **show mac-address-table vpls** command in EXEC mode to show VPLS MAC address information.

show mac-address-table vpls [*VPLS-NAME* **[{peer** *IP-ADDRESS* **[***VC-ID***] | ac interface** *INTERFACE-ID* **[vlan** *VLAN-ID***]}]] [address** *MAC-ADDR***]**

Syntax Description	
VPLS-NAME	Optional, specifies VPLS name. The name range is 1 – 32 characters.
peer	Optional, specifies a peer in a VPLS.
IP-ADDRESS	Optional, specifies the LSR ID that is used to identify the PE which the peer is belonging to.
VC-ID	Optional, specifies the pseudowire id. The range is 1-4294967295.
ac	Optional, specifies a local AC in a VPLS.
interface *INTERFACE-ID*	Optional, specifies Ethernet interface of a local AC.
vlan *VLAN-ID*	Optional, specifies a local AC is Ethernet VLAN-based AC and related VLAN ID. If no specifies, a local AC is Ethernet-based AC.
address *MAC-ADDR*	Optional, specifies the MAC address need to be shown.

Default N/A

Command Mode EXEC mode

Usage Guideline This command is used to show VPLS MAC address information. A user can select to show a specified VPLS MAC address, or the VPLS MAC addresses on a specified VPLS peer, or the VPLS MAC addresses on a specified VPLS AC, or the VPLS MAC addresses on a specified VPLS, or all VPLS MAC addresses.

Example The following example shows how to show all VPLS MAC address information.

```
switch#show mac-address-table vpls

VPLS Name                        MAC Address        Peer (VC ID/IP) or AC
-------------------------------- ----------------- ----------------------
vpls100                          00-08-A1-79-9A-DF   101/1.1.1.1
vpls100                          00-08-A1-79-9A-E0   101/1.1.1.1
vpls100                          00-08-A1-79-9A-E1   101/1.1.1.1
vpls100                          00-08-A1-79-9A-E2   101/1.1.1.1
vpls100                          00-08-A1-79-9A-E3   101/1.1.1.1
vpls100                          00-08-A1-79-9A-E4   101/1.1.1.1
vpls100                          00-08-A1-79-9A-E5   101/1.1.1.1
vpls100                          00-08-A1-79-9A-E6   101/1.1.1.1

Total Entries: 8

switch#
```

The following example shows how to show the VPLS MAC addresses for a VPLS which name is “vpls100”.

```
switch#show mac-address-table vpls vpls100

VPLS Name                        MAC Address        Peer (VC ID/IP) or AC
-------------------------------- ----------------- ----------------------
vpls100                          00-08-A1-79-9A-DF   101/1.1.1.1
vpls100                          00-08-A1-79-9A-E0   101/1.1.1.1
vpls100                          00-08-A1-79-9A-E1   101/1.1.1.1
vpls100                          00-08-A1-79-9A-E2   101/1.1.1.1
vpls100                          00-08-A1-79-9A-E3   101/1.1.1.1
vpls100                          00-08-A1-79-9A-E4   101/1.1.1.1
vpls100                          00-08-A1-79-9A-E5   101/1.1.1.1
vpls100                          00-08-A1-79-9A-E6   101/1.1.1.1

Total Entries: 8

switch#
```

The following example shows how to show the VPLS MAC addresses for a peer of a VPLS.

```
switch#show mac-address-table vpls vpls100 peer 1.1.1.1

VPLS Name                        MAC Address        Peer (VC ID/IP) or AC
-------------------------------- ----------------- ----------------------
vpls100                          00-08-A1-79-9A-DF  101/1.1.1.1
vpls100                          00-08-A1-79-9A-E0  101/1.1.1.1
vpls100                          00-08-A1-79-9A-E1  101/1.1.1.1
vpls100                          00-08-A1-79-9A-E2  101/1.1.1.1
vpls100                          00-08-A1-79-9A-E3  101/1.1.1.1
vpls100                          00-08-A1-79-9A-E4  101/1.1.1.1
vpls100                          00-08-A1-79-9A-E5  101/1.1.1.1
vpls100                          00-08-A1-79-9A-E6  101/1.1.1.1

Total Entries: 8

switch#
```

The following example shows how to show the VPLS MAC addresses for a local AC of a VPLS.

```
switch#show mac-address-table vpls vpls100 ac interface gigabitEthernet 21
vlan 101

VPLS Name                        MAC Address         Peer (VC ID/IP) or AC
-------------------------------- ----------------- ----------------------
vpls100                          00-08-A1-79-9A-DF   Eth21/VLAN101
vpls100                          00-08-A1-79-9A-E0   Eth21/VLAN101
vpls100                          00-08-A1-79-9A-E1   Eth21/VLAN101
vpls100                          00-08-A1-79-9A-E2   Eth21/VLAN101
vpls100                          00-08-A1-79-9A-E3   Eth21/VLAN101
vpls100                          00-08-A1-79-9A-E4   Eth21/VLAN101
vpls100                          00-08-A1-79-9A-E5   Eth21/VLAN101
vpls100                          00-08-A1-79-9A-E6   Eth21/VLAN101

Total Entries: 8

switch#
```

The following example shows how to show a specified VPLS MAC addresses in a VPLS which name is “vpls100”.

```
switch#show mac-address-table vpls vpls100 address 00:08:A1:79:9A:DF

VPLS Name                        MAC Address         Peer (VC ID/IP) or AC
-------------------------------- ----------------- ----------------------
vpls100                          00-08-A1-79-9A-DF  Eth21/VLAN101

Total Entries: 1

switch#
```

The following example shows how to show a specified VPLS MAC addresses in all VPLS.

```
switch#show mac address-table vpls address 00:08:A1:79:9A:DF

VPLS Name                        MAC Address         Peer (VC ID/IP) or AC
-------------------------------- ----------------- ----------------------
vpls100                          00-08-A1-79-9A-DF   Eth21/VLAN101

Total Entries: 1

switch#
```

17-11 clear mac-address-table vpls

Use the **clear mac-address-table vpls** command in EXEC mode to clear VPLS MAC address.

clear mac-address-table vpls dynamic [*VPLS-NAME* **[{peer** *IP-ADDRESS* **[***VC-ID***] | ac interface** *INTERFACE-ID* **[vlan** *VLAN-ID***] | address** *MAC-ADDR***}]]**

Syntax Description	
VPLS-NAME	Optional, specifies VPLS name. The name range is 1 – 32 characters.
peer	Optional, specifies a peer in a VPLS.
IP-ADDRESS	Optional, specifies the LSR ID that is used to identify the PE which the peer is belonging to.
VC-ID	Optional, specifies the pseudowire id. The range is 1-4294967295.
ac	Optional, specifies a local AC in a VPLS.
interface *INTERFACE-ID*	Optional, specifies Ethernet interface of a local AC.
vlan *VLAN-ID*	Optional, specifies a local AC is Ethernet VLAN-based AC and related VLAN ID. If no specifies, a local AC is Ethernet-based AC.
address *MAC-ADDR*	Optional, specifies the MAC address need to be cleared.

Default N/A

Command Mode EXEC mode

Usage Guideline This command is used to clear VPLS MAC address. A user can select to clear a specified VPLS MAC address, or the VPLS MAC addresses on a specified VPLS peer, or the VPLS MAC addresses on a specified VPLS AC, or the VPLS MAC addresses on a specified VPLS, or all VPLS MAC addresses.

Example The following example shows how to clear all VPLS MAC addresses.

```
switch#clear mac-address-table vpls dynamic
switch#
```

The following example shows how to clear VPLS MAC addresses for a VPLS.

```
switch#clear mac-address-table vpls dynamic vpls100
switch#
```

The following example shows how to clear VPLS MAC address for a peer of a VPLS.

```
switch#clear mac-address-table vpls dynamic vpls100 peer 1.1.1.1
switch#
```

The following example shows how to clear VPLS MAC address for a local AC of a VPLS.

```
switch#clear mac-address-table vpls dynamic vpls100 ac interface
gigabitEthernet 1 vlan 100
switch#
```

The following example shows how to clear one VPLS MAC address.

```
switch#clear mac-address-table vpls dynamic vpls100 address
00:11:22:33:44:55
switch#
```

17-12 show mpls l2transport vc

Use the **show mpls l2transport vc** command in EXEC mode to show VC information for VPWS and VPLS.

show mpls l2transport vc [*VC-ID***] [detail]**

Syntax Description	
VC-ID	Optional, specifies the pseudowire id. The range is 1-4294967295.
detail	Optional, specifies detail VC information.

Default N/A

Command Mode EXEC mode

Usage Guideline This command is used to show VC (detail) information for VPWS and VPLS.

Example To show all VC information including VPWS and VPLS.

```
switch#show mpls l2transport vc
VC ID       Peer            Local AC              Type    Oper Status
 ---------- -------------- -------------------- ------  -----------
 1          150.1.1.4      Eth1/VLAN2           Raw     Up
 2          130.1.1.2      Eth1/VLAN3           Tagged  Down
 3          140.1.1.2      vpls100              Tagged  Up
 4          160.1.1.2      vpls100              Tagged  Standby

Total Entries: 4
```

The following example shows how to show detail VC information for a VPLS.

```
switch#show mpls l2transport vc 5 detail
VC ID: 5, Peer IP Address: 120.1.1.2, Operate Status: Up
   Local AC: vpls101, Status: Up
   Remote AC Status: Up
   MPLS VC Labels: Local 19, Remote 19
   Outbound Tunnel label: 103
   MTU: Local 1500, Remote 1500
   Group ID: Local 0, Remote 0
   Signaling Protocol: LDP
   VC Statistics:
     RX Bytes: 0, RX Packets: 0
     TX Bytes: 0, TX Packets: 0

 Total Entries: 1
```

Virtual Routing and Forwarding Lite (VRF Lite) Commands

18-1 address-family ipv4 vrf

Use this command to enter VRF address family configuration mode. Use the **no** form of this command to disable VRF address family configuration mode.

address-family ipv4 vrf *VRF-NAME*

no address-family ipv4 vrf *VRF-NAME*

Syntax Description	
VRF-NAME	Specifies the name of VRF

Default By default, no VRF address family is specified.

Command Mode Router configuration mode

Usage Guideline This command is used for configuring routing instances such as BGP or RIP that use IPv4 address prefixes. After executing this command, the address family configuration mode will be entered and a new routing instance may be created with this command. For example, in RIP, with this command, a new RIP routing instance will be created. Then use the command **show ip rip vrf** to check the settings.
If the **no** form of this command is executed, the related routing instance will be removed and the command line will exit address family mode.

Example To create a new RIP routing instance of VRF VPN-A:

```
Switch# configure terminal
Switch(config)# ip vrf VPN-A
Switch(config-vrf)# exit
Switch(config)# interface vlan 1
Switch(config-if)# ip vrf forwarding VPN-A
Switch(config-if)# end
Switch# config ipif System ipaddress 10.1.1.1/24 state enable
Switch# configure terminal
Switch(config)# router rip
Switch(config-router)# address-family ipv4 vrf VPN-A
Switch(config-router-af)#
```

To disable the address family of the VRF VPN-A:

```
Switch# configure terminal
Switch(config)# router rip
Switch(config-router)# no address-family ipv4 vrf VPN-A
Switch(config-router)#
```

18-2 exit-address-family

Use this command to exit address family configuration mode.

exit-address-family

Syntax Description None.

Default None.

Command Mode Address family configuration mode

Usage Guideline This command is used to exit address family configuration mode.

Example To exit address family configuration mode:

```
Switch# configure terminal
Switch(config)# router rip
Switch(config-router)# address-family ipv4 vrf VPN-A
Switch(config-router-af)#network 10.1.1.0
Switch(config-router-af)#exit-address-family
Switch(config-router)#
```

18-3 import map

Use this command to set import route map of one VRF. Use the **no** form of this command to delete the import route map.

import map *ROUTE-MAP*

no import map

Syntax Description	
ROUTE-MAP	Specifies the name of import route map of the VRF.

Default By default, no import route map is specified to a VRF instance.

Command Mode VRF configuration mode

Usage Guideline This command is used to set the import route map of one VRF. This is used by BGP to distribute VPN routing information. One VRF only has one import route map. The new import route map will overwrite the value set before.

Use the command **show ip vrf** to check the settings.

Example To create a VRF VPN-A and set its import route map:

```
Switch# configure terminal
Switch(config)# ip vrf VPN-A
Switch(config-vrf)# import map rmap1
Switch(config-vrf)#
```

18-4 ip vrf

Use this command to create a new VRF instance. Use the **no** form of this command to delete one VRF instance.

ip vrf *VRF-NAME*

no ip vrf *VRF-NAME*

Syntax Description	
VRF-NAME	Specifies the name of the VRF.

Default By default, no VRF instance is specified.

Command Mode Global configuration mode

Usage Guideline This command is used to create a new VRF instance and enter VRF configuration mode. After a new VRF instance is created, a new VRF routing table will be created. With the **no** form of this command, one VRF will be deleted. The related VRF routing table will be deleted at the same time. And all routing instances based on this VRF will be destroyed too. All IP interfaces associated to this VRF will be restored to global routing instance. In the other words, all configurations based on this VRF will be removed.

There is a limitation about the max number of VRF instances and it is 127 for this switch.

Use the command **show ip vrf** and s**how ip route vrf** to check the settings.

Example To create and delete a VRF instance:

```
Switch# configure terminal
Switch(config)# ip vrf VPN-A
Switch(config-vrf)#exit
Switch(config)# no ip vrf VPN-A
Switch(config)#
```

18-5 ip vrf forwarding

Use this command to associate one interface to a VRF instance. Use the **no** form of this command to restore one interface to global routing instance.

ip vrf forwarding *VRF-NAME*

no ip vrf forwarding *VRF-NAME*

Syntax Description	
VRF-NAME	Specifies the name of the VRF.

Default By default, no interface is associated to a VRF instance.

Command Mode Interface configuration mode

Usage Guideline This command is used to associate an interface to one VRF instance. After one interface is associated to one VRF instance with this command, its IP address will be restored to unspecified. User needs to set its IP address before use it.

By associating interfaces to different VRF, the interfaces in different VRF can be configured with same IP address. The IP address space in one VRF is individual and can overlap among different VRFs.

Use the command **show ip vrf** to check the settings.

Example To associate VLAN 100 interface to VRF VPN-A:

```
Switch# configure terminal
Switch(config)# interface vlan 100
Switch(config-if)# ip vrf forwarding VPN-A
Switch(config-if)# end
Switch# config ipif vlan100 ipaddress 100.1.1.1/24 state enable
```

18-6 maximum routes

Use this command to limit the maximum routes within the VRF. Use the **no** form of this command to remove the limit.

maximum routes *LIMIT* **{***WARN-THRESHOLD* **|** *WARNING-ONLY***}**

no maximum routes

Syntax Description	
LIMIT	Specifies the maximum number of routes within the VRF. Its range is 1 to *MAX_ROUTES*. The *MAX_ROUTES* is 12288.
WARN-THRESHOLD	(Optional) Specifies the warning threshold percent of limit. Warning message will be printed when the routes number reach the threshold and no more routes can be written into hardware. Its range is 1% to 100%.
WARNING-ONLY	(Optional) When the routes number reaches the limit, one warning message will be printed. But more routes can still be written into hardware.

Default By default, no limit is defined to a VRF instance.

Command Mode VRF configuration mode.

Usage Guideline This command is used to limit how many routes can be allowed within the VRF. Please note this limit only apply to the active route. If user only wants to get a warning, set the warning-only.

Use the command **show ip vrf details** *VRF-NAME* to check the settings.

Example To set VRF VPN-A's routes limit to 100:

```
Switch# configure terminal
Switch(config)# ip vrf VPN-A
Switch(config-vrf)# maximum routes 100 warning-only
Switch(config-vrf)#
```

18-7 rd

Use this command to set the route distinguisher of one VRF.

rd *ROUTE-DISTINGUISHER*

Syntax Description	
ROUTE-DISTINGUISHER	Specifies VRF's route distinguisher, witch is used to prepend an 8-bytes value to an IPv4 prefix to create a VPN-IPv4 prefix.

Default By default, no route distinguisher is set for one VRF.

Command Mode VRF configuration mode.

Usage Guideline This command is used to set VRF's route distinguisher to form unique VPN-IPv4 prefix. One VRF has only one route distinguisher and cannot be changed if it has been set to one value.

Use the command **show ip vrf** to check the settings.

Example To create an VRF instance VPN-A and set its route distinguisher:

```
Switch# configure terminal
Switch(config)# ip vrf VPN-A
Switch(config-vrf)# rd 100:1
Switch(config-vrf)#
```

18-8 route-target

Use this command to add one route target of a VRF. Use the no form of this command to remove one route target.

route-target {import | export | both} *ROUTE-TARGET*

no route-target {import | export | both} *ROUTE-TARGET*

Syntax Description	
import	(Optional) Specifies to add import route target to import routing information from the target VPN extended community.
export	(Optional) Specifies to add export route target to export routing information to the target VPN extended community.
both	(Optional) Specifies to add both import route target and export route target.
ROUTE-TARGET	Specifies the value of route target.

Default By default, no route target is specified for one VRF.

Command Mode VRF configuration mode

Usage Guideline This command is used to add a route target to one VRF. One VRF can have multiple route targets.

Use the command **show ip vrf** to check the settings.

Example To create an VRF instance VPN-A and add import and export target:

```
Switch# configure terminal
Switch(config)# ip vrf VPN-A
Switch(config-vrf)# route-target import 100:1
Switch(config-vrf)# route-target export 100:1
```

18-9 show ip vrf

Use this command to show VRF settings.

show ip vrf [{details | interfaces}] [*VRF-NAME*]

Syntax Description	
details	(Optional)Specifies to show detail information about one or more VRFs.
interfaces	(Optional)Specifies to show interfaces associated with one or more VRFs.
VRF-NAME	(Optional)Specifies to show information associated with one VRF.
N/A	Show brief information about all VRF instances.

Default None.

Command Mode Privileged mode

Usage Guideline This command is used to check the settings of VRF instances.

Example To check current VRF settings:

```
Switch# show ip vrf

VRF Name                RD                      Interfaces
----------------------- ----------------------- -----------------------
VPN-A                   100:1                   ip100
VPN-B                   Not Set
```

To check detail information about VRF VPN-A

```
Switch# show ip vrf details VPN-A

VRF VPN-A; Default RD: 100:1
  Interfaces:
    ip100
  Export VPN Route-target Communities:
    RT:100:1
  Import VPN Route-target Communities:
    RT:100:1
  Import Route-map: rmap1
  Route Warning Limit 5, Current Count 0
```

To check interfaces associated with VRFs:

```
Switch# show ip vrf interfaces

Interfaces   IP Address         VRF
------------ ------------------ ------------
ip100        100.1.1.1/24       VPN-A
```

Virtual Router Redundancy Protocol (VRRP) Commands

19-1 vrrp authentication

Use this command to enable VRRP authentication and set the password on an interface. Use the **no** form of this command to remove the authentication.

vrrp authentication *STRING*

no vrrp authentication

Syntax Description	
STRING	Specifies the plaintext authentication password (8 characters).

Default By default no authentication is configured.

Command Mode Interface configuration mode

Usage Guideline This command is used to enable VRRP authentication on an interface. The authentication is applied to all virtual routers on this interface.
The devices in the same VRRP group must have the same authentication password.

Use the command **show vrrp** to verify your settings.

Example Following example is to configure one interface's VRRP authentication:

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# vrrp authentication test
```

19-2 vrrp critical-ip

Use this command to set the critical IP address of a virtual router. Use the **no** form of this command to remove the critical IP address.

vrrp *VRID* **critical-ip** *IP-ADDRESS*

no vrrp *VRID* **critical-ip**

Syntax Description	
VRID	Specifies the virtual router identifier. The valid range is from 1 to 255.
IP-ADDRESS	Specifies the critical IP address.

Default By default no critical IP address is configured.

Command Mode Interface configuration mode

Usage Guideline This command is used to set the critical IP address for one virtual router. If the critical IP is configured on one virtual router, the virtual router can not be active when the critical IP address in unreachable. The critical IP address must an valid host address and must belong to one existing interface on switch.

Use command **show vrrp** to verify your settings.

Example Following example is to set critical IP address of virtual router 1 on System interface:

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# vrrp 1 critical-ip 192.168.100.1
```

19-3 vrrp ip

Use this command to create a VRRP router. Use the **no** form of this command to remove a VRRP router.

vrrp *VRID* **ip** *IP-ADDRESS*

no vrrp *VRID*

Syntax Description	
VRID	Specifies the virtual router identifier that identifies the VRRP group. The valid range is from 1 to 255.
IP-ADDRESS	Specifies the IP address for the virtual router.

Default No virtual group is created on the interface.

Command Mode Interface configuration mode

Usage Guideline This command creates a virtual router and specifies its IP address. All routers in the same VRRP group must be configured with the same virtual router ID and IP address.
A virtual router group is represented by a virtual router ID. The IP address of the virtual router is the default router configured on hosts. The virtual router's IP address can be a real address configured on the routers, or an unused IP address. If the virtual router address is a real IP address, the router that has this IP address is the IP address owner.
A master will be elected in a group of routers that supports the same virtual routers. Others are the backup routers. The master is responsible for forwarding the packets that are sent to the virtual router.
The limitation about the number of supported virtual router groups is project dependent.

Use the command **show vrrp** to verify your settings.

Example Following example is to create a VRRP virtual router on an interface:

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# vrrp 1 ip 10.1.1.100
```

To remove the VRRP virtual router:

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# no vrrp 1
```

19-4 vrrp preempt

Use this command to allow a router to take over the master role if it has a better priority than the current master. Use the **no** form of the command to restore to the default setting.

vrrp *VRID* **preempt**

no vrrp *VRID* **preempt**

Syntax Description	
VRID	Specifies the virtual router identifier. The valid range is from 1 to 255.

Default By default preempt mode is enabled.

Command Mode Interface configuration mode

Usage Guideline In preempt mode, a router will take over the master role if it has a better priority than the current master. To reduce unnecessary changes to the role in an unstable network, the router will delay the process of taking over the master role for the specified period of time.
In non-preempt mode, the master will not be preempted unless the incoming router is the IP address owner of the virtual router.

Use the command **show vrrp** to verify your settings.

Example In the following example, the user configures the router for VRRP group 7 to preempt the current master router when its priority of 200 is higher than that of the current master router:

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# vrrp 7 preempt
```

In the following example, to the user configures the router to disable the preempt function of the virtual router:

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# no vrrp 7 preempt
```

19-5 vrrp priority

Use this command in the interface configuration mode to set the priority of a virtual router. Use the **no** form of this command to restore to the default priority.

vrrp *VRID* **priority** *PRIORITY*

no vrrp *VRID* **priority**

Syntax Description	
VRID	Specifies the virtual router identifier. The valid range is from 1 to 255.
PRIORITY	Specifies the priority of the virtual router. A higher value means a higher priority. The valid range is from 1 to 254.

Default The default value of priority of virtual router is 100.

Command Mode Interface configuration mode.

Usage Guideline The master of a virtual router is elected based on the priority setting. The router that owns the virtual router IP address has the highest priority to be elected.
The router with the highest priority will become the master, and other routers with a lower priority will then act as the backup for the virtual router. Each router should be configured with different priority values. If there are multiple routers with the same highest priority value, the router with the highest numbers in its IP address will become the master.
The router that is the IP address owner of the VRRP group is always the master of the VRRP group.

Use the command **show vrrp** to verify your settings.

Example In the following example, the user configures the priority of VRRP group 7 to be 200 on interface vlan1:

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# vrrp 7 priority 200
```

In the following example, the user resets the priority of VRRP group 7 to the default value on interface vlan1:

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# no vrrp 7 priority
```

19-6 vrrp timers advertise

Use this command to configure the interval between successive VRRP advertisements by the master router. Use the **no** form of this command to restore to the default value.

vrrp *VRID* **timers advertise** *INTERVAL*

no vrrp *VRID* **timers advertise**

Syntax Description	
VRID	Specifies the virtual router identifier. The valid range is from 1 to 255.
INTERVAL	Specifies the time interval between successive advertisements by the master router. The unit of the interval is second.The valid value is from 1 to 255.

Default The default value of advertisement interval is 1 second.

Command Mode Interface configuration mode.

Usage Guideline The maser will constantly send the VRRP advertisements to communicate the related information of the current master virtual router.
The **vrrp timers advertise** command configures the interval between advertisement packets and the time before other routers declare the master router as down. All routers in a VRRP group must use the same timer values.

Use the command **show vrrp** to verify your settings.

Example In the following example, the user configures the router to send advertisements for VRRP 7 every 10 seconds on interface vlan1:

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# vrrp 7 timers advertise 10
```

In the following example, the user configures the advertisement interval to use the default settings:

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# no vrrp 7 timers advertise
```

19-7 show vrrp

Use this command to view the VRRP status.

show vrrp [interface *IPIF_NAME* **[group** *VRID***]] [brief]**

Syntax Description	
interface *IPIF_NAME*	(Optional) Only show information about the virtual routers that belong to specified interface.
group *VRID*	(Optional) Only show the detail information about the specified virtual router. The valid range is from 1 to 255.
brief	(Optional) Show brief information.

Default None

Command Mode Privileged mode

Usage Guideline Use this command to show the VRRP related setting and status.

Example The following example show brief information about all virtual routers:

```
Switch# show vrrp brief
Interface       Grp Pri Own Pre State   Master addr     Group addr
System          1   255  Y   Y  Master  10.1.1.1        10.1.1.1
System          2   100      Y  Master  10.1.1.1        10.1.1.101
Ip100           1   50       Y  Init    100.1.1.1       100.1.1.100
```

The follow example show brief information about the virtual routers belong to ip100 interface:

```
Switch# show vrrp interface ip100 brief
Interface       Grp Pri Own Pre State   Master addr     Group addr
Ip100           1   50       Y  Init    100.1.1.1       100.1.1.100
```

The following example show brief information about the group 1 on System interface:

```
Switch# show vrrp interface System group 1 brief
Interface       Grp Pri Own Pre State   Master addr     Group addr
System          1   255  Y   Y  Master  10.1.1.1        10.1.1.1
```

Field	Description
Interface	Interface name the virtual routers belong to.
Grp	Group ID, the identifier of virtual router, as specified with the **vrrp ip** command.
Pri	The priority of virtual router, as specified with the **vrrp priority** command.

Own	"Y" represents IP address owner.
Pre	The preempt mode of virtual router, as specified with the **vrrp preempt** command. "Y" represents the preempt mode is enabled.
State	State of this virtual router, which could be Master, Backup or Init
Master addr	The IP address of the interface that the Master virtual router belongs to.
Group addr	The IP address of virtual router, as specified with the **vrrp ip** command.

The following example show detail information about all virtual routers:

```
Switch# show vrrp
System – Group 1
  State is Master
  Virtual IP Address is 10.1.1.1
  Virtual MAC Address is 00-00-5E-00-01-01
  Advertisement Interval is 1 sec
  Preemption is Enabled
  Priority is 255
  Master Router is 10.1.1.1

System – Group 2
  State is Master
  Virtual IP Address is 10.1.1.101
  Virtual MAC Address is 00-00-5E-00-01-02
  Advertisement Interval is 1 sec
  Preemption is Enabled
  Priority is 100
  Master Router is 10.1.1.1

ip100 - Group 1
  State is Init
  Virtual IP Address is 100.1.1.100
  Virtual MAC Address is 00-00-5E-00-01-01
  Advertisement Interval is 1 sec
  Preemption is Enabled
  Priority is 100
  Authentication is enabled
  Authentication Text is 12345678
  Master Router is 100.1.1.1
```

The following example show detail information about groups on System interface:

```
Switch# show vrrp interface System
System – Group 1
  State is Master
  Virtual IP Address is 10.1.1.1
  Virtual MAC Address is 00-00-5E-00-01-01
  Advertisement Interval is 1 sec
  Preemption is Enabled
  Priority is 255
  Master Router is 10.1.1.1

System – Group 2
  State is Master
  Virtual IP Address is 10.1.1.101
  Virtual MAC Address is 00-00-5E-00-01-02
  Advertisement Interval is 1 sec
  Preemption is Enabled
  Priority is 100
  Master Router is 10.1.1.1
```

The following example show detail information about group 1 on System interface:

```
Switch# show vrrp interface System group 1
System – Group 1
  State is Master
  Virtual IP Address is 10.1.1.1
  Virtual MAC Address is 00-00-5E-00-01-01
  Advertisement Interval is 1 sec
  Preemption is Enabled
  Priority is 255
  Master IP Router is 10.1.1.1
```

19-8 debug vrrp

Use this command to turn on VRRP debug. Use the **no** form of the command to turn off VRRP debug.

debug vrrp

no debug vrrp

Syntax Description None.

Default By default VRRP debug is turned off.

Command Mode Privileged mode

Usage Guideline Use this command to turn on or turn off all VRRP debug switches, including VRRP error prompt, VRRP event, VRRP message and status.

Example The following example turn on all VRRP debug switches:

```
Switch# debug vrrp
Switch#
VR 1 at interface System switch to Master
VR 2 at interface System switch to Master
Send out an ADV msg at VR 1 at interface System priority 255
Send out an ADV msg at VR 2 at interface System priority 100
```

Field	Description
VR	VRRP virtual router.
ADV	VRRP advertisement message.

19-9 debug vrrp errors

Use this command to turn on VRRP error prompt debug switch. Use the **no** form of the command to turn off VRRP error prompt debug switch.

debug vrrp errors

no debug vrrp errors

Syntax Description None.

Default By default the VRRP error prompt debug switch is turned off.

Command Mode Privileged mode.

Usage Guideline Use this command to turn on or turn off VRRP error prompt debug switch.

Example The following example turn on VRRP error prompt debug switch:

```
Switch# debug vrrp errors
Switch#
Received an ADV msg with incorrect checksum on VR 1 at interface System
Received an ADV msg with incorrect checksum on VR 1 at interface System
Received an ADV msg with incorrect checksum on VR 1 at interface System
```

19-10 debug vrrp events

Use this command to turn on VRRP event debug switch. Use the **no** form of the command to turn off VRRP event debug switch.

debug vrrp events

no debug vrrp events

Syntax Description	None
Default	By default the VRRP event debug switch is turned off.
Command Mode	Privileged mode
Usage Guideline	Use this command to turn on or turn off VRRP event debug switch.
Example	The following example turn on VRRP event debug switch:

```
Switch# debug vrrp events
Switch#
interface ip100 link up
interface ip100 link down
Master received a higher priority ADV msg at VR 2 at interface System
Master received a higher priority ADV msg at VR 2 at interface System
Authentication type mismatch on VR 1 at interface System
```

19-11 debug vrrp packets

Use this command to turn on VRRP packet debug switch. Use the **no** form of the command to turn off VRRP packet debug switch.

debug vrrp packets

no debug vrrp packets

Syntax Description	None
Default	By default the VRRP packet debug switch is turned off.
Command Mode	Privileged mode
Usage Guideline	Use this command to turn on or turn off VRRP packet debug switch.
Example	The following example turn on VRRP packet debug switch:

```
Switch# debug vrrp packets
Switch#
Received an ADV msg at VR 2 on interface System
Received an ADV msg at VR 2 on interface System
Received an ADV msg at VR 2 on interface System
Send out an ADV msg at VR 1 at interface System priority 255
Send out an ADV msg at VR 1 at interface System priority 255
Send out an ADV msg at VR 1 at interface System priority 255
```

19-12 debug vrrp state

Use this command to turn on VRRP state debug switch. Use the **no** form of the command to turn off VRRP state debug switch.

debug vrrp state

no debug vrrp state

Syntax Description None.

Default By default the VRRP state debug switch is turned off.

Command Mode Privileged mode.

Usage Guideline Use this command to turn on or turn off all VRRP state debug switch.

Example The following example turn on VRRP state debug switch:

```
Switch# debug vrrp state
Switch#
VR 1 at interface System switch to Master
VR 2 at interface System switch to Master
VR 1 at interface ip100 switch to Init
```

19-13 debug vrrp log

Use this command to turn on log of VRRP. Use the **no** form of the command to turn off log of VRRP.

debug vrrp log

no debug vrrp log

Syntax Description None.

Default By default the log of VRRP is turned off.

Command Mode Privileged mode

Usage Guideline Use this command to turn on or turn off the log of VRRP.
When log of VRRP is turned on and there are some VRRP change event, some log will be recorded.

Example The following example turn on the log of VRRP:

```
Switch# debug vrrp log
Switch#
```

List of Commands (Alphabetical)